Access Integration Services

Software User's Guide Version 3.2

SC30-3988-00

Access Integration Services

Software User's Guide Version 3.2

SC30-3988-00

Note
Before using this document, read the general information under “Notices” on page xxi.

First Edition (November 1998)

This edition applies to Version 3.2 of the IBM Access Integration Services and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers’ comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

Department CGF
Design & Information Development
IBM Corporation
P.O. Box 12195
RESEARCH TRIANGLE PARK NC 27709
USA

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Notice to Users of Online Versions of This Book

For online versions of this book, you are authorized to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine-readable documentation.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking	IBM	PS/2
AIX	Micro Channel	RS/6000
AIXwindows	NetView	System/370
APPN	AS/400	Nways
VTAM	BookManager	

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This manual contains the information that you will need to use the router user interface for configuration and operation of the Access Integration Services base code installed on your IBM 2212. With the help of this manual, you should be able to perform the following processes and operations:

- Configure, monitor, and use the Access Integration Services base code.
- Configure, monitor, and use the interfaces and Link Layer software supported by your IBM 2212.

This manual contains the information you will need to configure bridging and routing functions on an IBM 2212. The manual describes all of the features and functions that are in the software. A specific IBM 2212 might not support all of the features and functions described. If a feature or function is device-specific, a notice in the relevant chapter or section indicates that restriction.

This manual supports the IBM 2212 and refers to this product as either “the router” or “the device”. The examples in the manual represent the configuration of an IBM 2212 but the actual output you see may vary. Use the examples as a guideline to what you might see while configuring your device.

Who Should Read This Manual

This manual is intended for persons who install and manage computer networks. Although experience with computer networking hardware and software is helpful, you do not need programming experience to use the protocol software.

To get additional information: Changes may be made to the documentation after the books are printed. If additional information is available or if changes are required after the books have been printed, the changes will be in a file (named README) on diskette 1 of the configuration program diskettes. You can view the file with an ASCII text editor.

About the Software

IBM Access Integration Services is the software that supports the IBM 2212 (licensed program number 5639-F73). This software has these components:

- The base code, which consists of:
  - The code that provides the routing, bridging, data link switching, and SNMP agent functions for the device.
  - The router user interface, which allows you to configure, monitor, and use the Access Integration Services base code installed on the device. The router user interface is accessed locally through an ASCII terminal or emulator attached to the service port, or remotely through a Telnet session or modem-attached device.

  The base code is installed at the factory on the 2212.
- The Configuration Program for IBM Access Integration Services (referred to in this book as the *Configuration Program*) is a graphical user interface that enables you to configure the device from a stand-alone workstation. The Configuration Program includes error checking and online help information.

The Configuration Program is not pre-loaded at the factory; it is shipped separately from the device as part of the software order.

You can also obtain the Configuration Program for IBM Access Integration Services from the IBM Networking Technical Support home page. See *Configuration Program User's Guide for Multiprotocol and Access Services Products,* GC30-3830, for the server address and directories.

Conventions Used in This Manual

The following conventions are used in this manual to show command syntax and program responses:

1. The abbreviated form of a command is underlined as shown in the following example:

   ```
   reload
   ```

   In this example, you can enter either the whole command (reload) or its abbreviation (rel).

2. Keyword choices for a parameter are enclosed in brackets and separated by the word or. For example:

   ```
   command [keyword1 or keyword2]
   ```

   Choose one of the keywords as a value for the parameter.

3. Three periods following an option mean that you enter additional data (for example, a variable) after the option. For example:

   ```
   time host ...
   ```

   In this example, you enter the IP address of the host in place of the periods, as explained in the description of the command.

4. In information displayed in response to a command, defaults for an option are enclosed in brackets immediately following the option. For example:

   ```
   Media (UTP/STP) [UTP]
   ```

   In this example, the media defaults to UTP unless you specify STP.

5. Keyboard key combinations are indicated in text in the following ways:
   - **Ctrl-P**
   - **Ctrl -**

   The key combination **Ctrl -** indicates that you should press the Ctrl key and the hyphen simultaneously. In certain circumstances, this key combination changes the command line prompt.

6. Names of keyboard keys are indicated like this: **Enter**

7. Variables (that is, names used to represent data that you define) are denoted by italics. For example:

   ```
   File Name: filename.ext
   ```

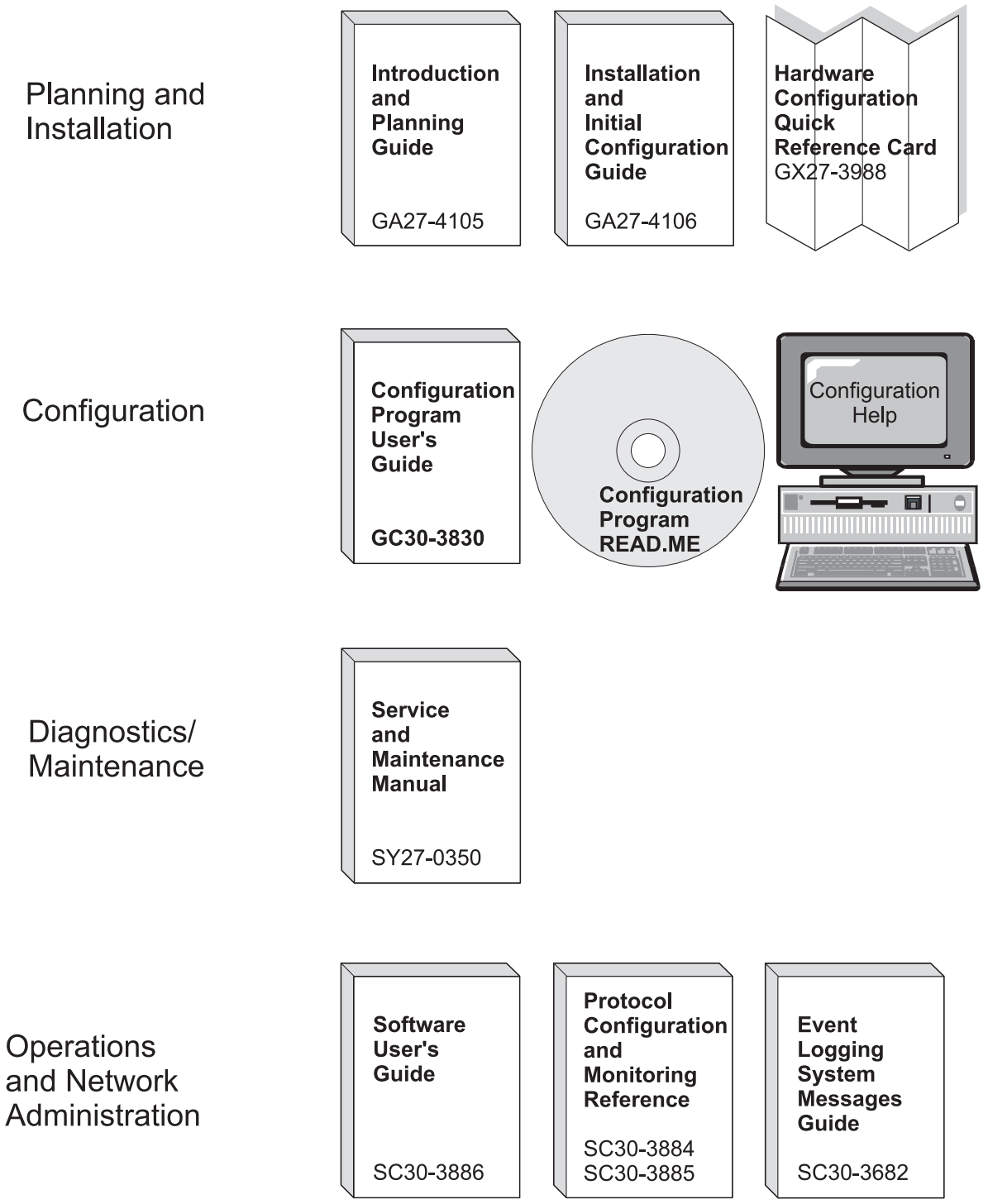

Figure 1. Common Tasks and the IBM 2212 Library

Library Overview

The following list shows the books in the IBM 2212 library, arranged according to tasks.

Information updates and corrections: To keep you informed of engineering changes, clarifications, and fixes that were implemented after the books were printed, refer to the IBM 2212 home pages at:

```
   http://www.networking.ibm.com/216/216prod.html
and
   http://www.networking.ibm.com/216/216lib.html
```

Planning

GA27-4105
IBM 2212 Access Utility Introduction and Planning Guide

This book is shipped with the IBM 2212. It explains how to prepare for installation and perform an initial configuration.

Installation

GA27-4106
IBM 2212 Access Utility Installation and Initial Configuration Guide

This booklet is shipped with the IBM 2212. It explains how to install the IBM 2212 and verify its installation.

GX27-3988
2216 Nways Multiaccess Connector Hardware Configuration Quick Reference

This reference card is used for entering and saving hardware configuration information used to determine the correct state of an IBM 2212.

Diagnostics and Maintenance

SY27-0350
2216 Nways Multiaccess Connector Service and Maintenance Manual

This book is shipped with the IBM 2212 It provides instructions for diagnosing problems with and repairing the IBM 2212.

Operations and Network Management

The following list shows the books that support the Nways Multiprotocol Access Services program.

SC30-3886
Nways Multiprotocol Access Services Software User's Guide

This book explains how to:

- Configure, monitor, and use the Nways Multiprotocol Access Services software.
- Use the Nways Multiprotocol Access Services command-line router user interface to configure and monitor the network interfaces and link-layer protocols shipped with the IBM 2212.

SC30-3884
Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1

SC30-3885
Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2

These books describe how to access and use the Nways Multiprotocol Access Services command-line user interface to configure and monitor the routing protocol software shipped with the product.

They include information about each of the protocols that the devices support.

SC30-3682
Nways Event Logging System Messages Guide

This book contains a listing of the error codes that can occur, along with descriptions and recommended actions to correct the errors.

Configuration

GC30-3830
Configuration Program User's Guide

This book discusses how to use the Nways Multiprotocol Access Services Configuration Program.

Safety

SD21-0030
Caution: Safety Information—Read This First

This book, shipped with the IBM 2212, provides translations of caution and danger notices applicable to the installation and maintenance of a IBM 2212.

Marketing

URL: **http://www.networking.ibm.com/216/216prod.html**

This IBM Web page provides product information through the World Wide Web.

Summary of Changes for the IBM 2212 Software Library

The IBM 2212 is a new product; however, it uses common software. The following list applies to changes in the software that were made in Version 3.2.

- **New functions:**
  - IP Version 6
    - TCP6, UDP6, Telnet, PING-6 and traceroute-6, ICMPv6, and IPsec
    - Neighbor discovery protocol (NDP) for host auto-configuration
    - Static routes, RIPng, Protocol Independent Multicast-Dense Mode (PIM-DM), and Multicast Listener Discovery (MLD)
    - Configured or automatic tunneling of IPv6 packets over IPv4 networks
  - Resource ReSerVation Protocol (RSVP)
    - Signalling mechanisms that enable applications on IPv4 networks to reserve network resources to achieve a desired quality of service for packet delivery
  - Thin Server Support
    - Acts as boot server for network stations
    - Servers supported include Network Station Manager (NSM) R2.5 and 3.0 on OS/400 and NSM R3.0 for NFS servers such as Windows NT, OS/390, AIX, and VM

- Binary Synchronous Relay (BRLY) support for BSC interfaces

  Binary Synchronous Relay (BRLY) support for tunneling Bisync Synchronous (BSC) transmissions over a IPv4 network to a partner 2210 or 2212 router

- **Enhanced functions:**
  - Base Services
    - Event Logging System (ELS) enhancements to capture, format, and offload large volumes of ELS messages
    - Support for maintaining multiple, compressed dump files
    - Timed configuration change support from the configuration tool that is persistent across reloads and restarts
    - Packet trace support for PPP, Frame Relay, and V.34 interfaces.
  - Bridging support for a multiaccess bridge port for source route bridging over Frame Relay. The multiaccess port incorporates many DLCIs in a single bridge port for improved scalability.
  - DIALs
    - DIALs support for functions supported by Microsoft Dial-Up Network Clients
      - Support for Callback Control Protocol (CBCP)
      - Support for Microsoft Point-to-Point Encryption (MPPE) and Microsoft PPP CHAP (MS-CHAP)
    - Virtual connections to suspend and resume dial-up connections when Shiva Password Authentication Protocol (SPAP) is used
  - IP items
    - IP precedence/TOS filter enhancements
    - Policy-based routing
    - Configuration of the IP MTU by interface
    - OSPF Enhancements to allow for easier migration of IBM 6611 router networks
    - BGP-4 support for policies per neighbor and additional attributes for path selection
    - DVMRPv3 support
    - IGMP prune and grafting support
  - ISDN support for callback based on the caller ID and call blocking
  - L2TP support for the L2TP client model which allows the 2212 to create an L2TP tunnel between itself and another router. The tunnel can be used for any traffic entering the 2212. The L2TP Network Server (LNS) function has also been enhanced to initiate outgoing calls to the L2TP Network Access Concentrator (LAC).
  - Network Dispatcher items
    - Support for stateless UDP applications
    - New protocol advisors for Network News Transfer Protocol (NNTP), Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), and Telnet
    - While you are balancing TN3270 servers, one of the TN3270 servers may be in the same 2212 as the Network Dispatcher function
  - Support for PPP authentication using an ACE/Server
  - Security Enhancements
    - IPsec tunnel-in-tunnel support for creating up to two nested levels of security associations

- IPsec ESP NULL algorithm support
- IPsec support for setting the *don't fragment* bit and propogation of Path MTU
- Improved dynamic reconfiguration for IPsec

– Mixed media multi-link PPP support for bundling PPP leased line, ISDN, V.25bis, and V.34 connections

– APPN enhancements

- APPN SDLC Secondary multipoint support
- Configuration of the APPN transmission group (TG) number for all link station types
- Support for the APPN Ping (APING) command in Talk 5
- New trace options

– TN3270 Enhancements

Note: These TN3270 enhancements will not be available in the initial release of V3.2, but will be available on the 2212 Web server by 12/31/98.

- TN3270 LU pooling support that allows SNA LUs to be grouped into named pools
- TN3270 IP address to LU name mapping
- Self-Defining Dependent LUs (SDDLU) and Dynamically Defined Dependent LUs (DDDLU) support
- Multiple TCP port support

– DLSw enhancements

- Support for duplicate MAC addresses
- Support to delay polling of SDLC devices until contacted by the remote SDLC device

– X.25 enhancements

- Configuration support for a defining a range of PVCs
- Support for up to 2500 PVCs

– Frame Relay support for switched virtual circuits

– IPXWAN support on Frame Relay permanent virtual circuits (PVCs), including support for numbered RIP, unnumbered RIP, and static routing

• **Clarifications and corrections**

The technical changes and additions are indicated by a vertical line (|) to the left of the change.

Summary of Changes

Part 1. Understanding and Using the Software

Chapter 1. Getting Started

This chapter shows you how to get started with using the following components related to the IBM 2212 Access Utility (2212) and the Access Integration Services:

- Router console terminals
- Router software (Access Integration Services)
- Router software user interface

The information in this chapter is divided into the following sections:

- "Before You Begin"
- "Accessing the Software Using Local and Remote Consoles"
- "Discussing the User Interface System" on page 6

Before You Begin

Before you begin, refer to the following checklist to verify that your router is installed correctly.

HAVE YOU...

- Installed all necessary hardware?
- Connected the console terminal (video terminal) to the router?

  Attention: If you are using a service port-attached terminal to configure or monitor your IBM 2212 and your service terminal is unreadable, you need to change some parameters in your configuration.

  Refer to your hardware documentation.
- Connected your router to the network using the correct network interfaces and cables?
- Run all necessary hardware diagnostics?

For more information on any of these procedures, refer to the *IBM 2212 Access Utility Installation and Initial Configuration Guide*.

Migrating to the Current Release

Refer to the *IBM 2212 Access Utility Service and Maintenance Manual* for information about migrating to a new code level.

Accessing the Software Using Local and Remote Consoles

The router console lets you use the router user interface to monitor and change the function of the router's networking software (Access Integration Services). The router supports local and remote consoles.

Local Consoles

Local consoles are either directly connected by an EIA 232 (RS-232) cable, or connected via modems to the router. You may need to use a local console during

the initial software installation. After the initial setup connection, you can connect using Telnet, as long as IP forwarding has been enabled. (Refer to *Protocol Configuration and Monitoring Reference* for more information on enabling IP forwarding.)

When the configured router is started for the first time, a boot message appears on the screen, followed by the OPerator's CONsole or OPCON prompt (*). The * prompt indicates that the router is ready to accept OPCON commands.

You will need to use an ASCII terminal attached to the 2212 service port to initially configure it.

Important: Garbage, random characters, reverse question marks, or the inability to connect your terminal to the 2212 service port can have many causes. The following list contains some of those causes:

- The most common cause of garbage or random characters on the service console is that the baud rate is not synchronized with the IBM 2212.

  If the 2212 is set to a specific baud rate, the terminal or terminal emulator must be set to the same baud rate.

  Refer to your hardware documentation for more information.
- Defective terminal or device (ac) grounds.
- Defective, incorrectly shielded, or incorrectly grounded EIA 232 (RS-232) cable between the terminal and the IBM 2212.
- Defective terminal or terminal emulator.
- Defective IBM 2212 system board.
- High ambient electromagnetic interference (EMI) levels.
- Power line disturbances.

Once the 2212 is initially configured, you will not need a local console for router operation, as long as IP is enabled.

The router software automatically handles console activity. When upgrading the software, you might have to use the local console. For information on attaching and configuring local consoles, refer to the *IBM 2212 Access Utility Installation and Initial Configuration Guide*.

Remote Consoles

Remote consoles attach to the router using a standard remote terminal protocol. Remote consoles provide the same function as local consoles, except that a local console must be used for initial configuration. You can use no more than two remote consoles at the same time on a router. You can connect remote consoles to the router through a Telnet connection. You have the option to disable this feature.

Telnet Connections

The router supports both Telnet Client and Server. The remote console on the router acts as a Telnet server. The router acts as a Telnet client when connecting from the router to either another router or a host using the **telnet** command in the OPCON (*) process.

Remote Login Names and Passwords

During a remote login, the router prompts you for a login name and password. You can display the login name when logged in to the router from a remote console by using a router **status** command.

Logging In Remotely or Locally

Logging in to a local console is the same as logging in to a remote console except that you must connect to the router by starting Telnet on your host system. To log in remotely, begin at step 1. To log in locally, begin at step 3.

To log in from a remote console:

1. Connect to the router by starting Telnet on your host system. Your host system is the system to which remote terminals are connected.
2. Supply the router's name or Internet Protocol (IP) address.

   To use router names, your network must have a name server. Issue either the router name or the IP address as shown in the following example:

   ```
   % telnet brandenburg
   ```

   or

   ```
   % telnet 128.185.132.43
   ```

   At this point, it makes no difference whether you have logged in remotely or locally.
3. If you are prompted, enter your login name and password.

   ```
   login:
   Password:
   ```

   It is possible that there is a login and no password. The password controls access to the router. If a password has not been set, press the **Enter** key at the `Password:` prompt. Logins are not set automatically. For security, you can set up user names and passwords using the **add user** command in the CONFIG process. For additional information, see the **add user** configuration command, on page82. Remember to reload to activate any changes.

   Note: If you do not enter a login name and valid password within 1 minute of the initial prompt, or if you enter an incorrect password three times in succession, the router drops the Telnet connection.
4. Press the **Enter** key to display the asterisk (*) prompt.

   You may have to press the **Enter** key more than once or press **Ctrl-P** to obtain the * prompt.

   Once at this level, you can begin to enter commands from the keyboard. Press the **Backspace** key to delete the last character typed in on the command line. Press the **Delete** key or **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See "Command History for GWCON and CONFIG Command Line" on page 24 for information on how to access previously entered commands.

   You can also use local Telnet commands on your Telnet client to close the Telnet connection.

   Note: If you use a VT100 terminal, do not press the **Backspace** key, because it inserts invisible characters. Use the **Delete** key.

5. Exit the router as described in “Exiting the Router”.

Reloading or Restarting the Router

Use the **reload** command to reboot the device and load a new copy of the code into memory.

For example:

```
* reload

The configuration has been changed, save it? (Yes or [No]  or Abort)

Are you sure you want to reload the gateway? (Yes or [No]): yes
```

Use the **restart** command to invoke a new configuration. For example, to change a configuration parameter that is not dynamically configurable, you can make and save the change, then restart the device.

Restart does dot reload the code, it simply invokes the new configuration. As a result, restart is much faster than reload.

For example:

```
* restart

The configuration has been changed, save it? (Yes or [No] . . . or Abort)
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Exiting the Router

Return to the * prompt and close the Telnet connection. For example:

```
IP Config> exit
Config> Ctrl-P
* logout

%
```

You can also use local Telnet commands on your Telnet client to close the Telnet connection.

Discussing the User Interface System

The software (Access Integration Services) is a multitasking system that schedules use of the CPU among various processes and hardware devices. The router software:

- Provides timing and memory management, and supports both local and remote operator consoles from which you can view and modify the router’s operational parameters.
- Consists of functional modules that include various user interface processes, all network interface drivers, and all protocol forwarders purchased with the router.

Understanding the First-Level User Interface

The user interface to the software consists of the main menu (process) and several subsidiary menus (processes). These menus are related to the multiple levels of processes in the software.

The first level of processes consists of the OPCON and CONFIG-ONLY processes. In most cases, you will use the OPCON process to access the second level to configure or operate the base services, features, interfaces, and protocols you will run on your IBM 2212.

The second level of processes consists of the processes listed by the **status** command. You use the talk *pid* command to access the second-level processes. There are processes that you cannot use in the software. See Table 1 on page 12 for an overview of the processes.

Figure 2 shows the processes and how they fit within the structure of the router software.

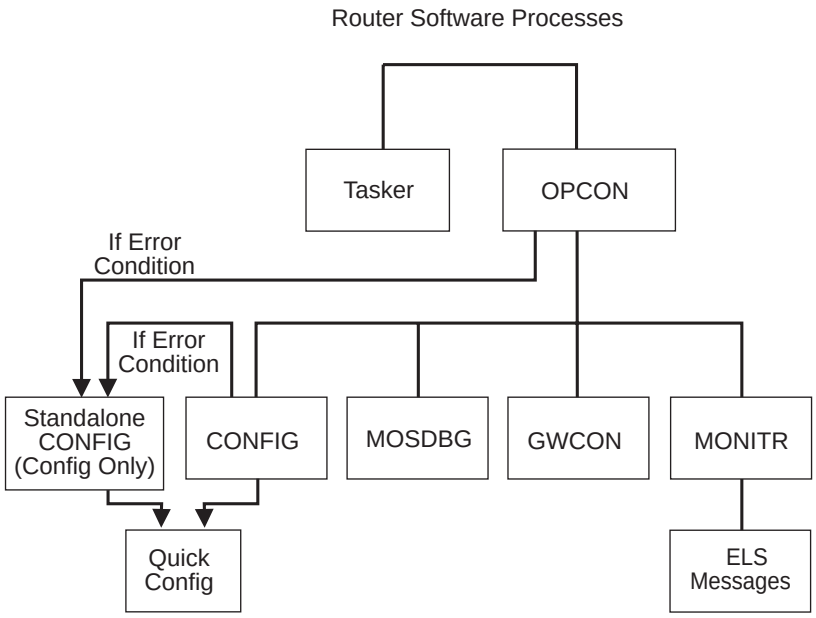

Figure 2. Access Integration Services

Figure 3 on page 8 is an example of the relationship between the various process levels.

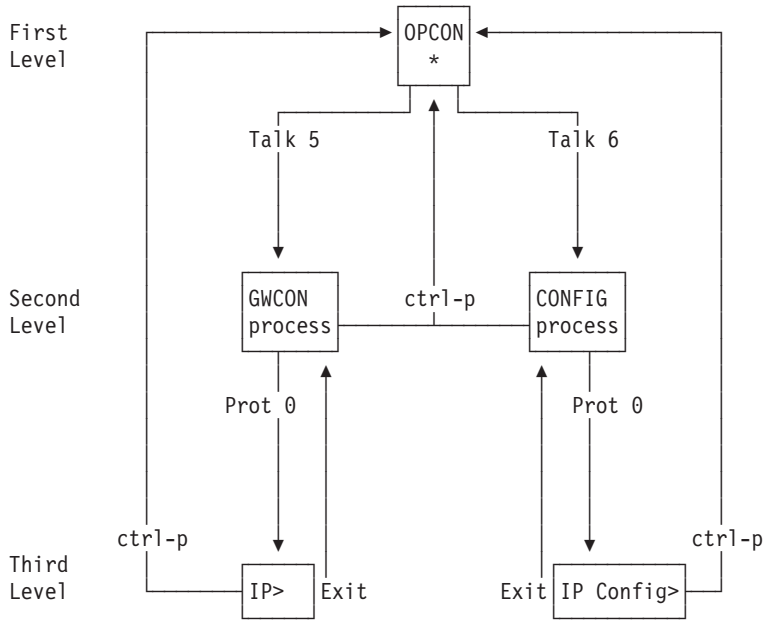

Figure 3. Relationship of Processes and Commands

Note: Also shown in Figure 3 are the various commands to access each process level and return from each process level.

See “Chapter 3. The OPCON Process” on page 27 for more information about OPCON, and “Config-Only Mode” on page 66 for more information about CONFIG-ONLY.

The ROPCON process handles processing from remote consoles and is essentially the same as the OPCON process.

If an error condition exists where the bootstrap code cannot load the code from the hardfile or compact FLASH you are taken to the Service Recovery interface (SVC> prompt). When you are at this interface, only the operating system has been loaded, but not all the operational code. See “Chapter 7. Using the Service Recovery Function” on page 55 for more information.

Quick Configuration Process

Quick Configuration, or Quick Config, allows you to quickly configure portions of the router without dealing with the specific operating system commands. When you initially load or restart the router with no configuration, you enter Config-Only and you can access Quick Config menus from that process. If the router has devices configured and the devices do not have any protocols configured, the router automatically starts Config-Only and then enters Quick Config.

You can also enter Quick Config from the CONFIG process using the **qconfig** command.

System Security

Multiple users with login permissions can be added using the **add user** command. See “Configuring User Access” on page 67 for details on security issues and for information on the **set password** and **add user** commands.

Chapter 2. Using the Software

This chapter describes how to use the software. It consists of:

Entering Commands

When typing a command, remember the following:

- Type only enough sequential letters of the command to make it unique among the available commands. For example, to execute the **reload** command you must enter **rel** as a minimum. The minimum number of required characters are underlined in the command syntax chapters.
- Commands are not case-sensitive.
- Sometimes, only the first letter of the command (and subsequent options) is required to execute the command. For example, typing **s** at the * prompt followed by pressing the **Enter** key causes the **status** command to be executed.

Connecting to a Process

When you start the router, the console displays a boot message. The OPCON prompt (*) then appears on the screen indicating that you are in the OPCON process and you can begin entering OPCON commands. This is the command prompt from which you communicate with different processes.

To connect your console to a process:

1. Find out the process ID (PID) number of a process by entering the **status** command at the * prompt.

   The **status** command displays information about the router processes, such as the process IDs (PIDs), process names and status of the process. Issuing the **status** command is shown in the following example:

```
* status
Pid  Name      Status TTY  Comments
1    COpCn1    RDY    TTY0
2    Monitr    DET     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELScon    DET     --
8    ROpCn1    IDL    TTY1 128.185.210.125
9    ROpCn2    IDL    TTY2
```

2. Use the **talk** *pid* command, where *pid* is the number of the process to which you want to connect. (For more information about these and other OPCON commands, refer to "Chapter 3. The OPCON Process" on page 27.)

   Note: Not every process listed has a user interface (for example, the **talk 3** process). The **talk 4** command is for use by IBM service representatives.

Identifying Prompts

Each process uses a different prompt. You can tell which process your console is connected to by looking at the prompt. (If the prompt does not appear when you enter the **talk** *pid* command, press the **Return** key a few times.)

The following list shows the prompts for the five main processes:

Table 1. Processes, Their Purpose, and Commands to Access

Process	Level and Purpose	Command to Access	Input Prompt
OPCON	Level 1 - access to all secondary levels	**Ctrl-P**	asterisk (*)
CONFIG	Level 2 - base services configuration and access to configuration third level	**talk 6**	Config >
GWCON	Level 2 - base services operation and monitoring and access to operations and monitoring on third level	**talk 5**	plus sign (+)
MONITR	level 2 - message display	**talk 2**	(none)
ELSCon	level 2 - direct monitoring and access to ELS console	**talk 7**	ELS Secondary Console>
MOSDBG	level 2 - diagnostic environment	**talk 4**	db>
DIAGS	level 2 - run hardware diagnostics	**diags**	
Note: Only enter the **talk 4** command under the direction of a service representative.			

At the OPCON prompt level, you can begin to enter commands from the keyboard. Use the **Backspace** key to delete the last character typed in on the command line. Use **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See “Command History for GWCON and CONFIG Command Line” on page 24 for information on how to access previously entered commands.

Getting Help

At the command prompts, you can obtain help in the form of a listing of the commands available at that level. To do this, type **?** (the **help** command), and then press **Enter**. Use **?** to list the commands that are available from the current level. You can usually enter a **?** after a specific command name to list its options. For example, the following information appears if you enter **?** at the * prompt:

```
*?

DIAGS hardware diagnostics
DIVERT output from process
FLUSH output from process
HALT output from process
INTERCEPT character is
LOGOUT
MEMORY statistics
RELOAD
RESTART

STATUS of process(es)
TALK to process
TELNET to IP-Address
```

Exiting a Lower Level Environment

The multiple-level nature of the software places you in secondary, tertiary, and even lower level environments as you configure or operate the 2212. To return to the next higher level, enter the **exit** command. To get to the secondary level, continue entering **exit** until you receive the secondary level prompt (either `Config>` or `+`).

For example, to exit the IP protocol configuration process:

```
IP config> exit
Config>
```

If you need to get to the primary level (OPCON), enter the intercept character (**Ctrl P** by default).

Getting Back to OPCON

To get back to the OPCON prompt (*), press **Ctrl-P**. You must always return to OPCON before you can communicate with another process. For example, if you are connected to the GWCON process and you want to connect to the CONFIG process, you must press **Ctrl-P** to return to OPCON first. The **Ctrl-P** key combination is the default *intercept character*.

If you use the intercept character from a third-level or lower level process to return to the * prompt, the next time you use the **talk** command, you will reenter the third level process. This link goes away when the router is re-initialized.

Some Configuration Suggestions

Configuring a 2212 is different depending on whether you are configuring for the first time, creating a configuration based on an existing configuration, or just updating a configuration. Use the following sections as a guide to the best procedure to use, depending on your needs.

Creating a First Configuration

This procedure assumes that you have no other 2212 that contains a configuration similar to the one for the 2212 you are configuring. The procedure also assumes that you have just taken the 2212 out of the box. Although this procedure specifies an order, you can perform the actual configuration (after step 3) in any order.

To configure a IBM 2212 for the first time:

1. Examine the 2212 you are configuring to determine which interfaces you need to configure. Note these for later use.
2. Connect to the 2212 as described in “Accessing the Software Using Local and Remote Consoles” on page 3.
3. Initially configure a port on the 2212 and at least an internal IP address for the device using Quick Config as described in “Quick Configuration” on page 66 or “Appendix A. Quick Configuration Reference” on page 571. Configure the minimum needed to allow you to Telnet into the device.
4. Configure any base services, such as boot options. Access the configuration process as described in “Accessing the Configuration Process, CONFIG (Talk 6)” on page 16.

5. Configure the interfaces. Access the interface configuration process as described in “Accessing the Network Interface Configuration Process” on page 18 .
6. Configure any required features. Access the feature configuration process as described in “Accessing Feature Configuration and Operating Processes” on page 21 .
7. Configure any protocols that will run through this device. Access the protocol configuration process as described in “Accessing Protocol Configuration and Operating Processes” on page 22.

   Note: At the very least, you will configure IP in this step.
8. Restart the router as described in “Reloading or Restarting the Router” on page 6 .

Basing a Configuration on an Existing Configuration

This section describes how to:

- Base a configuration on the configuration in an operating 2212
- Permanently update the configuration in a 2212
- Temporarily update the configuration of a 2212 while the 2212 is operating

Basing on an Existing Configuration

If you already have a 2212 that has the same interfaces, features, and protocols that you want to configure on a new 2212, you can save time by basing the configuration on the existing 2212. You can perform this type of configuration either using the command line interface or by using the configuration program that comes with the 2212. In both cases, the procedures assume that the 2212 is not in your production network.

To base a configuration on an existing configuration using the command line interface:

1. Obtain a copy of the configuration you want to use.
   a. Enter **talk 6** at the OPCON (*) prompt.
   b. Enter **boot** at the `Config>` prompt.
   c. Enter the **tftp put configuration** *file* command at the `Boot config>` prompt. See “Chapter 5. Using BOOT Config to Perform Change Management” on page 41 for more information.
2. Connect to the 2212 that you are configuring.
3. Load the configuration you obtained in step 1 into the 2212 using TFTP GET. See “Chapter 5. Using BOOT Config to Perform Change Management” on page 41.
4. Update the configuration.
5. Write the configuration. See “Chapter 8. The Configuration Process (CONFIG - Talk 6) and Commands” on page 65.
6. Reload the 2212.

To base a configuration on an existing configuration using the configuration program:

1. Start the configuration program.

2. Retrieve the configuration from the 2212 on which you want to base the new configuration.
3. Make the changes you need for the new configuration. These changes include addresses, the host names, users, and other items.
4. Save the configuration with a different name from the name that you used to retrieve the configuration.
5. Send the configuration to the 2212 you are configuring.
6. Reload the 2212.

For more about using the configuration program, see *Configuration Program User's Guide for Multiprotocol and Access Services Products* GC30-3830.

Permanently Updating a Configuration

To permanently update a configuration:

1. Access the 2212 you are updating as described in "Accessing the Software Using Local and Remote Consoles" on page 3. You will see the * prompt.
2. Enter the **talk 6** command to access the configuration process.
3. Enter the appropriate commands to access the third-level process that configures the areas that you are changing.
4. Enter **exit** as many times as needed to return to the configuration process.
5. Write the configuration. See "Chapter 8. The Configuration Process (CONFIG - Talk 6) and Commands" on page 65.
6. Reload the 2212.

Temporarily Updating a Configuration

The ability to temporarily update a configuration allows you to make changes to some of the operating characteristics of a 2212 until you can make permanent updates to the configuration. This enables you to implement changes immediately to resolve problems or improve performance and avoid an outage during a peak period. You can then make permanent updates to the configuration and schedule an outage so you can restart or reload to pick up the change.

To temporarily update a configuration:

1. Access the 2212 you are updating as described in "Accessing the Software Using Local and Remote Consoles" on page 3. You will see the * prompt.
2. Enter the **talk 5** command to access the operating/monitoring process.

   Note: Not all interface types, protocols, or features allow you to make temporary config changes via talk 5 commands.
3. Enter the appropriate commands to access the third-level process that monitors the areas that you are changing.
4. Enter **exit** as many times as needed to return to the operating/monitoring process.
5. Enter **Ctrl-P** to return to the * prompt.
6. Exit the router as described in "Exiting the Router" on page 6

Accessing the Second-Level Processes

All interfaces, features, and protocols have commands that you use to access the following processes:

- The configuration process to initially configure and enable the interface, feature, or protocol, as well as perform later configuration changes.
- The operating/monitoring process to display information about each interface, feature, or protocol, to make temporary configuration changes, or to activate configuration changes.

You can also configure or operate some base system services through the second-level processes. The commands to perform these functions are described starting in “Chapter 8. The Configuration Process (CONFIG - Talk 6) and Commands” on page 65.

The next sections describe the procedures for accessing the second-level processes.

Accessing the Configuration Process, CONFIG (Talk 6)

Each protocol configuration process is accessed through the router’s CONFIG process. CONFIG is the second-level process of the router user interface that lets you communicate with third-level processes. Protocol processes are examples of third-level processes.

The CONFIG command interface is made up of levels that are called modes. Protocol configuration command interfaces are modes of the CONFIG interface. Each protocol configuration interface has its own prompt. For example, the prompt for the TCP/IP protocol command interface is `IP config>`.

The next sections describe these procedures in more detail.

Entering the CONFIG Process

To enter the CONFIG command process from OPCON and obtain the CONFIG prompt, enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Return** key again.

Quick Configuration Process: Quick Configuration, or Quick Config, allows you to quickly configure portions of the router without dealing with the specific operating system commands. You enter the Quick Config menus from the CONFIG process using the **qconfig** command (see “Quick Configuration” on page 66).

Restarting or Reloading the Router

Changes that you make to the protocol parameters through CONFIG do not take effect until you either activate the interface or reset the interface or protocol that contains any dynamic changes or the router software.

Note: You can also use the **write** command to save the changes on the hardfile or compact flash.

Accessing the Operating/Monitoring Process, GWCON (Talk 5)

To view information about the interfaces, features, or protocols or to change parameters while running, you must access and use the operating (monitoring) process. Operating command interfaces are modes of the GWCON interface. Within the GWCON mode, each interface, feature, or protocol interface has its own prompt. For example, the prompt for the TCP/IP protocol is `IP>`.

Note: Any parameters you change in this process will not remain active across any event that causes the 2212 to reload the operational code, such as a power outage or entering the **reload** command.

The next sections describe these procedures in more detail.

Entering the GWCON Command Process

To enter the GWCON process from OPCON and obtain the GWCON prompt, enter the **talk** command and the PID for GWCON. For example:

```
* talk 5
```

The GWCON prompt (+) then displays on the console. If the prompt does not appear, press **Return** again.

Accessing the Secondary ELS Console Process, ELSCon (Talk 7)

The Secondary ELS Console provides convenient access to GWCON `talk 5` ELS without disrupting the current state of GWCON. You may be in the middle of a **ping** in `talk 5`, or deep inside a `talk 5` menu structure, and want to control ELS without disrupting the current state of GWCON. `Talk 7` serves this purpose.

In the following example, another ELS event is displayed while performing a **ping** command.

Note: The intercept character (Ctrl-P by default) is used to obtain the OPCON prompt (*).

```
*talk 5
+protocol ip
IP>ping 10.0.0.9
PING 10.0.0.2 -> 10.0.0.9: 56 data bytes, ttl=64, every 1 sec.

*talk 7

ELS Secondary Console>display event ip.7
Complete
ELS Secondary Console>
*talk 2
00:20:48   IP.007: 10.0.0.2 -> 10.0.0.9
00:20:49   IP.007: 10.0.0.2 -> 10.0.0.9
```

Accessing the Third-Level Processes

After accessing the second level, you must enter commands on the third level to configure or operate the interfaces, features, and protocols in your IBM 2212. The following sections describe how to access the third level processes.

Accessing Network Interface Configuration and Operating Processes

This section describes how to get started with accessing the network interface configuration and operating processes. Accessing these processes lets you change and monitor software-configurable parameters for network interfaces used in your router.

Accessing the Network Interface Configuration Process

Use the following procedure to access the router's configuration process. This process gives you access to a specific interface's *configuration* process.

1. At the OPCON prompt, enter the OPCON **talk** command and the PID for CONFIG. (For more details about this command, refer to "Chapter 3. The OPCON Process" on page 27.)

   ```
   * talk 6
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter **CONFIG**, press **Return** again.

   Use the **add device** command to create a network interface. The **add device** command automatically assigns the interface number and supports the following types of devices (Enter **add device ?** to get a list of the supported device types):

   a. Multi-port adapters

      When you specify a multi-port adapter device name with the **add device** command, you are prompted for the adapter's slot number and the port number on the adapter that you want to use for the interface.

      If you want to use multiple ports on an adapter, you must enter the add device command multiple times and specify a different port number each time.

      ```
      Config>add dev e1-2port-isdn
      Device Slot #(1-4) [1]? 3
      Device Port Range (1-2) [1]?
        Adding 2-port ISDN Primary E1 device in slot 3 port 1 as interfaces #4.
      Use "net 4" to configure 8-port ISDN Primary E1 parameters.
      ```

   b. Single-port adapters

      When you specify a single-port adapter device name with the **add device** command, you are prompted for the adapter's slot number.

      The following example adds an interface for the ISDN basic adapter:

      ```
      Config>add dev e1-1port-isdn
      Device Slot #(1-4) [1]? 3
      Adding ISDN Basic device in slot 3  port 1 as interface #4
      Use "net 4" to configure 1-port ISDN Primary E1 parameters
      ```

   c. Dial circuits

      The following example adds a dial circuit interface:

      ```
      Config> add device dial-circuit
      Enter the number of PPP Dial Circuit interfaces [1]?
      Adding device as interface 8
      Base net for this circuit[0]?4
      ```

```
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 8" command to configure circuit parameters
```

d. The following example adds a dial-in circuit:

```
Config>add device dial-in
Enter the number of dial-in interfaces [1]?
Adding device as interface 5
Base net for this circuit [0]? 5
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 5" command to configure circuit parameters
```

e. Multilink PPP

The following example adds a multilink PPP interface:

```
Config>add device multilink-ppp
Enter the number of Multilink PPP interfaces [1]?
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
```

Notes:

a. When you create interfaces for serial adapters or dial circuits, the default data-link type is PPP. However, you can use the **set data-link** command to change the data-link type. Refer to Table 2 on page 20 for the data-link types supported on serial ports and dial circuits, and to the description of the **set data-link** command on page 100.

2. At the Config> prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured, as follows:

```
Config>li dev
Ifc 0     WAN PPP
Ifc 1     WAN PPP
Ifc 2     WAN PPP
Ifc 3     WAN PPP
Ifc 4     1-port IBM Token Ring              Slot: 5   Port: 1
Ifc 5     2-port IBM Token Ring              Slot: 1   Port: 1
Ifc 6     2-port IBM Token Ring              Slot: 1   Port: 2
Ifc 7     2-port IBM Token Ring              Slot: 2   Port: 1
Ifc 8     2-port IBM Token Ring              Slot: 2   Port: 2
Ifc 9     2-port 10/100 Ethernet             Slot: 3   Port: 1
Ifc 10    2-port 10/100 Ethernet             Slot: 3   Port: 2
Ifc 11    ISDN Basic                         Slot: 4   Port: 1
```

3. Record the interface numbers.
4. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

```
Config> network 1
```

The appropriate configuration prompt (such as TKR Config> for token-ring), now displays on the console.

Note: Not all network interfaces are user-configurable. For interfaces that cannot be configured, you receive the message:

```
That network is not configurable
```

Displaying the Interface Configuration: From the same interface configuration prompts, you can list configuration information specific to that selected interface by using the **list** command. For example:

```
TKR Config> list

Token-Ring configuration:

PACKET SIZE (INFO FIELD): 4472
Speed:                    16 Mb/sec
```

```
Media:                    Shielded

RIF Aging Timer:          120     Source Routing:          Enabled
MAC Address:              000000000000
```

Configuring the Network Interface: Refer to the specific chapters in this guide for complete information on configuring your IBM 2212's network interfaces.

Table 2 lists network architectures and the supported interfaces for each architecture.

Table 2. Network Architecture and the Supported Interfaces

Network Architecture	Supported Interfaces
802.5 Token-Ring	2-Port Token-Ring • 1-port Token-Ring PMC • 2-port Token-Ring CPCI
Ethernet	• 1-port 10/100-Mbps Ethernet PMC • 2-Port 10/100 Mbps Ethernet CPCI
ISDN	• 2-Port Basic Rate Interface (BRI) • 2-Port ISDN-PRI (T1/J1)* • 2-Port ISDN-PRI (E1)* • 1-Port ISDN-PRI (T1/J1) * • 1-Port ISDN-PRI (E1) * **Note:** The interfaces marked with an asterisk (*) can be used either as ISDN or channelized interfaces.
Point-to-Point	integrated WAN ports, 4-port WAN adapter, dial circuit interfaces
Frame Relay	integrated WAN ports, 4-port WAN adapter, dial circuit interfaces
X.25	integrated WAN ports, 4-port WAN adapter, dial circuit interfaces
SDLC Relay	integrated WAN ports, 4-port WAN adapter
Bisync	integrated WAN ports, 4-port WAN adapter
SDLC	integrated WAN ports, 4-port WAN adapter, dial circuit interfaces
V.25bis	integrated WAN ports, 4-port WAN adapter
V.34	integrated WAN ports, 4-port WAN adapter
Dial-Out	Supports DIALs and Telnet dial-out over V.34 base interfaces
Dial-In	A PPP dial circuit interface that has configuration parameters defaulted to support DIALs
Multilink PPP (MP)	Supported on any PPP link
L2TP	Supports virtual PPP DIALs connections through the Layer 2 Tunneling Protocol (L2TP).

Notes:

1. PPP dial circuit interfaces can use ISDN, a V.34 network, or V.25bis as the base network interface.
2. FR dial circuit interfaces can use an ISDN or a V.25bis network as the base network interface.
3. Dial-Out circuit interfaces use a V.34 network as the base network interface.
4. Dial-In circuit interfaces can use an ISDN or V.34 network as the base network interface.
5. SDLC dial circuits use V.25bis as the base network interface.

6. X.25 uses the ISDN BRI D-channel as the base network interface.

Accessing the Network Interface Console Process

To monitor information related to a specific interface, access the interface console process by using the following procedure:

1. At the OPCON prompt, enter the OPCON **talk** command and the PID for GWCON. For example:

   ```
   * talk 5
   ```

2. The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.
3. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

   ```
   +configuration

   Access Integration Services
   2212-AIS Feature 3763 V3.2 Mod 0 PTF 0 RPQ 0 AIS.EH5   cc_156c
   Num Name  Protocol
   3   ARP    Address Resolution
   7   IPX    NetWare IPX
   11  SNMP   Simple Network Management Protocol
   23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
   24  HST    TCP/IP Host Services
   25  LNM    LAN Network Manager

   Num Name  Feature
   2   MCF    MAC Filtering
   7   CMPRS  Data Compression Subsystem
   9   DIALs  Dial-in Access to LANs
   10  AUTH   Authentication

   11 Total Networks:
   Net  Interface   MAC/Data-Link        Hardware                      State
   0    PPP/0       Point to Point       SCC Serial Line               Up
   1    PPP/1       Point to Point       SCC Serial Line               Down
   2    PPP/2       Point to Point       SCC Serial Line               Down
   3    PPP/3       Point to Point       SCC Serial Line               Down
   4    TKR/0       Token-Ring/802.5     IBM Token Ring                Up
   5    TKR/1       Token-Ring/802.5     IBM Token Ring                Not present
   6    TKR/2       Token-Ring/802.5     IBM Token Ring                Not present
   7    TKR/3       Token-Ring/802.5     IBM Token Ring                Up
   8    TKR/4       Token-Ring/802.5     IBM Token Ring                Up
   9    Eth/0       Ethernet/IEEE 802.3  10/100 Ethernet               Up
   10   Eth/1       Ethernet/IEEE 802.3  10/100 Ethernet               Down
   ```

4. Enter the GWCON **network** command and the number of the interface you want to monitor. For example:

   ```
   + network 11
   X.25>
   ```

   In this example, the X.25 console prompt is displayed on the console. You can then view information about the X.25 interface by entering the X.25 console commands.

Monitoring the Network Interface: Refer to the specific chapters in this manual for complete information on monitoring your 2212's network interfaces.

Accessing Feature Configuration and Operating Processes

To help you access the Access Integration Services feature configuration and operating processes, this section outlines both of these procedures.

Accessing the Feature Processes

Use the **feature** command from the CONFIG process to access configuration commands for specific Access Integration Services features outside of the protocol and network interface configuration processes.

Use the **feature** command from the GWCON process to access console commands for specific features that are outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to display a listing of the features available for your software release. For example:

```
Config> feature ?

WRS
BRS
MCF
TSF
Feature name or number [1] ?
```

To access a particular feature's configuration or operating prompt, enter the **feature** command at the Config> or + (GWCON) prompt, respectively, followed by the feature number or short name. For example:

```
Config> feature mcf

MAC filtering user configuration

Filter Config>
```

Table 9 on page 91 lists the available feature numbers and names.

Once you access the configuration or operating prompt for a feature, you can begin entering specific commands for the feature. To return to the previous prompt level, enter the **exit** command at the feature's prompt.

Accessing Protocol Configuration and Operating Processes

This section describes how to access the protocol configuration and operating processes.

Entering a Protocol Configuration Process

To enter the desired protocol configuration process from the CONFIG> prompt:

1. At the CONFIG> prompt, enter the **list configuration** command to see the numbers and names of the protocols purchased in your copy of the software. See page 93 for sample output of the **list configuration** command.
2. From the Config> prompt, enter the **protocol** command with the number or short name (for example, IP, IPX, and ARP) of the protocol you want to configure. The protocol number and short name is obtained from the **list configuration** command display. In the following example, the command has been entered for accessing the IP protocol configuration process:

   ```
   Config> protocol IP
   ```

   or

   ```
   Config> protocol 0
   ```

The protocol configuration prompt then displays on the console. The following example shows the IP protocol configuration prompt:

```
IP config>
```

You can now begin entering the protocol's configuration commands. See the corresponding protocol section of the *Protocol Configuration and Monitoring Reference* for more information on specific protocol configuration commands.

In summary, the **protocol** command lets you enter the configuration process for the protocol software installed in your router. The **protocol** command enters a protocol's command process. After entering the protocol command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol.

Entering a Protocol Operating Process

To enter a protocol console process from the GWCON prompt:

1. At the GWCON prompt, enter the **configuration** command to see the protocols and networks configured for the router. For example:

```
+configuration

Access Integration Services
2212-AIS Feature 3763 V3.2 Mod 0 PTF 0 RPQ 0 AIS.EH5   cc_156c
Num Name  Protocol
3   ARP    Address Resolution
7   IPX    NetWare IPX
11  SNMP   Simple Network Management Protocol
23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
24  HST    TCP/IP Host Services
25  LNM    LAN Network Manager

Num Name  Feature
2   MCF    MAC Filtering
7   CMPRS  Data Compression Subsystem
9   DIALs  Dial-in Access to LANs
10  AUTH   Authentication

11 Total Networks:
Net  Interface   MAC/Data-Link        Hardware                      State
0    PPP/0       Point to Point       SCC Serial Line               Up
1    PPP/1       Point to Point       SCC Serial Line               Down
2    PPP/2       Point to Point       SCC Serial Line               Down
3    PPP/3       Point to Point       SCC Serial Line               Down
4    TKR/0       Token-Ring/802.5     IBM Token Ring                Up
5    TKR/1       Token-Ring/802.5     IBM Token Ring                Not present
6    TKR/2       Token-Ring/802.5     IBM Token Ring                Not present
7    TKR/3       Token-Ring/802.5     IBM Token Ring                Up
8    TKR/4       Token-Ring/802.5     IBM Token Ring                Up
9    Eth/0       Ethernet/IEEE 802.3  10/100 Ethernet               Up
10   Eth/1       Ethernet/IEEE 802.3  10/100 Ethernet               Down
```

2. Enter the GWCON **protocol** command with the protocol number or short name of the desired protocol displayed in the configuration information.

   In the following example, the command has been entered for accessing the IP protocol console process.

```
+ protocol 0
```

   or

```
+ protocol IP
```

The protocol console prompt then displays on the console. This example shows the IP protocol console prompt:

```
IP>
```

You can now begin entering the protocol's commands. See the corresponding protocol section of the *Protocol Configuration and Monitoring Reference* for more information on specific protocol console commands.

Command History for GWCON and CONFIG Command Line

The Command History contains up to the last 50 commands entered by the user in GWCON (Talk 5) or CONFIG (Talk 6) command line menus.

Backward and Forward retrieve keys can be used to recall previously entered commands. In addition, a facility is provided to enable the advanced user to repeat a particular series of commands.

Repeating a Command in the Command History

By pressing **Ctrl-B** (backward) or **Ctrl-F** (forward) at any command line prompt in a GWCON or CONFIG menu, the current command line is replaced by the previous or next command in the Command History. The Command History is common to both GWCON and CONFIG. That is, a command entered while in a GWCON menu can be retrieved from within CONFIG and a command entered while in a CONFIG menu can be retrieved from within GWCON.

The Command History contains the most recently entered commands, up to a maximum of the last 50 commands. If only three commands have been entered since a restart, pressing **Ctrl-F** or **Ctrl-B** circles through only those three commands. If no commands have been entered thus far, **Ctrl-F** or **Ctrl-B** results in a "bell", the same bell you see when trying to backspace beyond the beginning of a line of text.

Note: A command aborted by pressing **Ctrl-U** will not be entered into the Command History.

To enter two similar commands:

```
display sub les
display sub lec
```

Enter:

`display sub les`, then press **Enter**

Ctrl-B for Backward, and the current line is replaced with-

`display sub les`

Press **Backspace** and replace "s" with "c" to get

`display sub lec` and then press **Enter**

Repeating a Series of Commands in the Command History

There is an additional feature for advanced users to facilitate repeating a particular series of GWCON or CONFIG commands. C1, C2,...,Cn in the Command History is referred to as a *repeat sequence*. This feature may be more convenient than simply using **Ctrl-B** and **Ctrl-F** when you must repeat a given task that requires multiple

commands. Enter **Ctrl-R** (repeat) to set the start of the *repeat sequence* at command C1. Enter **Ctrl-N** (next) successively to retrieve the next command(s) in the repeat sequence. Commands are not automatically entered, but are placed on the current command line allowing you to modify or enter the command.

To produce the desired behavior of a repeat sequence, the first command retrieved using the first **Ctrl-N** (next) depends on the manner in which the start of the repeat sequence was set using **Ctrl-R** (repeat).

Setting the start of the repeat sequence with **Ctrl-R** can be done in two ways:

1. When C1 is initially entered
2. When C1 is retrieved from the Command History with **Ctrl-B** or **Ctrl-F**.

Starting a Repeat Sequence As Commands Are Entered

If you enter **Ctrl-R** as command C1 is being keyed in, and then enter commands C2, C3... Cn. **Ctrl-N** will successively bring commands C1, C2, ... Cn, C1, C2, ... Cn, C1, ... to the command line.

In Example 1, the start of the repeat sequence is set as the first command is keyed in. The user knows ahead of time that the same commands to be entered in GWCON need to be repeated in CONFIG.

Example 1

1. As the first command in the sequence is keyed in, use **Ctrl-R** (repeat) to set the start of the repeat sequence.

   ```
   *talk 5
   +event Ctrl-R
   ```

   then press **Enter** to set the start of the repeat sequence.
2. Continue typing the subsequent commands in the sequence:

   ```
   Event Logging System user console
     ELS>display sub les
     ELS>display sub lec
     ELS>exit
     +
   ```
3. To enter these same commands in CONFIG, press

   Ctrl-P (the default OPCON intercept character) and go to CONFIG.

   ```
   +-press Ctrl-P-
   *talk 6
   Config>Ctrl-N for NEXT to retrieve the start of
           this sequence-
   Config>event Enter
   Event Logging System user configuration
   ELS config>Ctrl-N for NEXT to retrieve the next
              command in sequence-
   ELS config>display sub les Enter
   ELS config>Ctrl-N for NEXT to retrieve the next
              command in sequence-
   ELS config>display sub lec Enter
   ELS config>Ctrl-N for NEXT to retrieve the next
              command in sequence-
   ELS config>exit Enter
   Config>
   ```

Starting a Repeat Sequence After All Commands Are Entered

On the other hand, if you first enter C1, C2, ... Cn, and retrieve C1 via **Ctrl-B** or **Ctrl-F**. Entering **Ctrl-R**, entering **Ctrl-N** successively brings commands C2,..., Cn, C1, C2,..., Cn, C1,...,Cn to the command line (see Example 2). The first occurrence of C1 is bypassed since C1 is already available on the command line at the time it was retrieved, and does not need to be recalled again by the first **Ctrl-N**.

In Example 2, all the commands are entered and then the first command in the sequence to be repeated is retrieved. A sequence of commands has been entered in GWCON, and the same sequence needs to be repeated in CONFIG.

Example 2

1. Enter the following commands in GWCON:

```
*talk 5
+event
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

2. To enter these same commands in CONFIG, press **Ctrl-P** (the default OPCON intercept character) and go to CONFIG.

```
+Ctrl-P-
*talk 6
Config>Ctrl-B four times to retrieve the start of
        the four command sequence in this example-
Config>event
Config>event Ctrl-R for REPEAT to set the start of
             the repeat sequence-
 Config>event Enter
 Event Logging System user configuration
 ELS config>Ctrl-N for NEXT to retrieve the next
             command in sequence-
 ELS config>display sub les Enter
 ELS config>Ctrl-N for NEXT to retrieve the next
             command in sequence-
 ELS config>display sub lec Enter
 ELS config>Ctrl-N for NEXT to retrieve the next
             command in sequence-
 ELS config>exit Enter
 Config>
```

If the OPCON **intercept** command described in “Chapter 3. The OPCON Process” on page 27 has been used to redefine the OPCON intercept character from the default character **Ctrl-P** to one of the Command History control characters, **Ctrl-B**, **Ctrl-F**, **Ctrl-R**, or **Ctrl-N**, the OPCON intercept character will take priority. For example, if the intercept character has been changed to **Ctrl-F**, then **Ctrl-F** will not retrieve Forward in the Command History, but will instead place the user back at the OPCON prompt (*).

Chapter 3. The OPCON Process

The Operator Console process (OPCON) is the root-level process of the router software user interface. The main function of OPCON is to control which processes are connected to consoles. Using OPCON commands, you can:

- Manipulate the output from a process
- Change the intercept character
- Display information about router memory usage
- Restart the router software
- Reload the router software (reboot)
- Telnet to other routers or hosts
- Display status information about all router processes
- Communicate with processes at the secondary level
- Escape to the MOS system debugging tool

Chapter 4. Using OPCON

This chapter describes the OPCON interface configuration and operational commands. It includes the following sections:

- "Accessing the OPCON Process"
- "OPCON Commands"

Accessing the OPCON Process

When the router starts for the first time, a boot message appears on the console. Then the OPCON prompt (*) appears on the console, indicating that the OPCON process is active and ready to accept commands.

The OPCON process allows you to configure, change, and monitor all of the router's operating parameters. While in the OPCON process, the router is forwarding data traffic. When the router is booted and enters OPCON, a copyright logo and an asterisk (*) prompt appears on the locally attached console terminal. This is the OPCON (OPerator's CONsole) prompt, the main user interface that allows access to second-level processes.

Some changes to the router's operating parameters made while in OPCON take effect immediately without requiring reinitializing of the router. If the changes do not take effect, use the **reloadrestart**command at the * prompt.

At the * prompt, an extensive set of commands enables you to check the status of various internal software processes, monitor the performance of the router's interfaces and packet forwarders, and configure various operational parameters.

OPCON Commands

This section describes the OPCON commands. Each command includes a description, syntax requirements, and an example. The OPCON commands are summarized in Table 3. To use them, access the OPCON process and enter the appropriate command at the OPCON prompt (*).

Table 3. OPCON Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Diags	Displays device status and the contents of the hardware test log and the hardware error log.
Divert	Sends the output from a process to a console or other terminal.
Flush	Discards the output from a process.
Halt	Suspends the output from a process.
Intercept	Sets the OPCON default intercept character.
Logout	Logs out a remote console.
Memory	Reports the router's memory usage.
Reload	Reloads the router software.
Restart	Restarts (but does not reload) the router software.
Status	Shows information about all router processes.

Table 3. OPCON Commands (continued)

Command	Function
Talk	Connects to another router process and enables the use of its commands.
Telnet	Connects to another router.

Diags

Use the **diags** command to display the Diagnostic Main Menu. The diagnostic menus allow you to enable, disable and test hardware adapters or ports. Diagnostic menus have on-screen help for the various options and status information that is available.

You can use the “b” (back) key to return to any previous menu. Use the “e” (exit) key to exit the diagnostics and return to the OPCON command prompt.

See the *Service and Maintenance Manual* for the 2212 for more information on diagnostic support.

Syntax:

diags

Divert

Use the **divert** command to send the output from a specified process to a specified terminal. This command allows you to divert the output of several processes to the same terminal to simultaneously view the output. The **divert** command is commonly used to redirect MONITR output messages to a specific terminal. The router allows only certain processes to be redirected.

After entering the command, enter the PID and tty# (number of the output terminal). To obtain these values, use the OPCON status command. The terminal number can be the number of either the local console (tty0) or one of the remote consoles (tty1, tty2). The following example shows Event Logging System messages generated by the MONITR process (2) being sent to a remote console *tty1* (1).

Event messages are displayed immediately even though you may be in the middle of typing a command. The display and keyboard have separate buffers to prevent command confusion. The following example shows the MONITR process connected to TTY1 after executing the **divert 2 1** command. If you want to stop the output, enter **halt 2**. The **halt** command is described in “Halt” on page 31.

Syntax:

divert *pid tty#*

Example: `divert 2 1`

```
Copyright Notices:
Copyright IBM Corp. 1994, 1997
MOS Operator Control


* divert 2 1

* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW    TTY0 gzs
2    Monitr    IDL    TTY0
```

```
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCN1    IDL    TTY1
9    ROpCN2    RDY    TTY2 jlg@128.185.40.40
```

Flush

Use the **flush** command to clear the output buffers of the MONITR process. This command is generally used before displaying the contents of the MONITR's FIFO buffer to prevent messages from scrolling off the screen. Accumulated messages are discarded.

The router allows only certain processes to be redirected. To obtain the *pid* and *tty#*, use the OPCON **status** command. In the following example, after executing the **flush 2** command, the output of the MONITR process is sent to the SNK (it has been flushed).

Syntax:

flush *pid*

Example: `flush 2`

```
* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW    TTY0 gzs
2    Monitr    IDL    SNK
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCN1    IDL    TTY1
9    ROpCN2    RDY    TTY2 jlg@128.185.40.40
```

Halt

Use the **halt** command to suspend all subsequent output from a specified process until the **divert**, **flush**, or **talk** OPCON command is issued to the process. The router cannot redirect all processes. **Halt** is the default state for output from a process. To obtain the PID for this command, use the OPCON **status** command. In the following example, after executing the **halt 2** command, the MONITR process is no longer connected to TTY1. Event messages no longer appear.

Syntax:

halt *pid*

Example: `halt 2`

```
* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW    TTY0 gzs
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCN1    IDL    TTY1
9    ROpCN2    RDY    TTY2 jlg@128.185.40.40
```

Intercept

Use the **intercept** command to change the OPCON intercept character. The intercept character is what you enter from other processes to get back to the OPCON process. The default intercept key combination is **Ctrl-P**.

The intercept character ***must*** be a control character. Enter the ^ (shift 6) character followed by the letter character you want for the intercept character.

Note: Do not set the intercept character to the return key or to a printable character. If you change the OPCON intercept character from the default, **Ctrl-P**, to one of the Command History control characters, **Ctrl-B**, **Ctrl-F**, **Ctrl-R**, or **Ctrl-N**, the OPCON intercept character will take priority.

For example, if you change the intercept character to **Ctrl-F**, then **Ctrl-F** will not retrieve Forward in the Command History, but will instead return to the OPCON prompt (*). See “Command History for GWCON and CONFIG Command Line” on page 24 for information on how to access previously entered GWCON or CONFIG commands.

Syntax:

intercept *character*

Example: `intercept ^u`

From this example, the intercept character is now **Ctrl-U**.

Logout

Use the **logout** command to terminate the current session for the user who enters the logout command. If the console login is enabled, this command will require the next user to log in using an authorized userid/password combination. If the console login is not enabled, the OPCON prompt appears again.

Syntax:

logout

Memory

Use the **memory** command to obtain and display information about the router’s global heap memory usage. The display helps you to determine if the router is being utilized efficiently. For an example of memory utilization, see Figure 4 on page 33 .

See “Memory” on page 120 for memory usage via talk 5.

Syntax:

memory

Example:

```
memory
Number of bytes:  Busy = 319544, Idle = 1936, Free = 1592
```

Busy Specifies the number of bytes currently allocated.

Idle Specifies the number of bytes previously allocated but freed and available for reuse.

Free Specifies the number of bytes that were never allocated from the initial free storage area.

Note: The sum of the Idle and Free memory equals the total available heap memory.

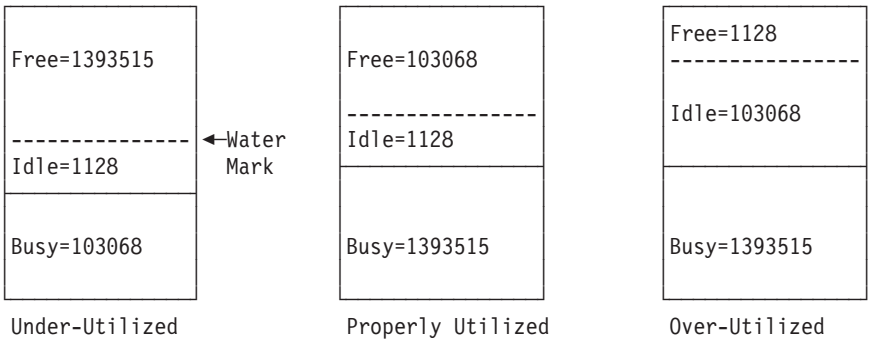

Figure 4. Memory Utilization

Reload

Use the **reload** command to reboot the router by loading in a new copy of the router software. When you use this command from a remote console, you install a new software load without going to the router. This command executes the same functions as pressing the reset button except that the router will not dump (if so configured). Before the reload takes effect, you are prompted to confirm the reload. You are also prompted if you have not saved the configuration changes.

Syntax:

reload

Example:

```
reload
Are you sure you want to reload the gateway (Yes or No)?
```

Restart

Use the **restart** command to activate a new configuration. Unlike reload, which loads new code into memory, restart simply activates a saved configuration. It is much faster than reload.

If you have made configuration changes that have not been saved , before restart takes effect, you are prompted to save them. You are also prompted to confirm the command. After you reinitialize the software, a bus reset occurs. This causes the connected network interfaces to self-test, all routing tables to clear, and any packets in the router to drop. Before the restart takes effect, you are prompted to confirm the restart.

Note: If you use this command from a remote console, your Telnet session will be lost because all router processes are being restarted.

Syntax:

restart

Example:

```
restart
Are you sure you want to restart the gateway (Yes or No)? Yes

Copyright Notices:
Copyright IBM Corp. 1994, 1997
MOS Operator Control
*
```

Status

Use the **status** command to display information about all router processes. By entering the PID after the **status** command, you can look at the status of only the desired process. The following example shows the total status display.

Syntax:

status *pid*

Example: status

```
Pid  Name      Status TTY  Comments

1    COpCN1    IOW    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    IOW     --
6    Config    IOW    TTY1
7    ELSCon    DET     --
8    ROpCN1    IOW    TTY1 128.185.46.101
9    ROpCN2    RDY    TTY2 128.185.46.104
```

Pid Specifies the PID. This is the process to talk to or from OPCON, or it can be an argument to the STATUS command to request status information about a specific process.

Name Specifies the process name. It usually corresponds to the name of the program that is running in the process.

Status

Specifies one of the following:

- **IDL** Specifies that the process is idle and waiting for completion of some external event, such as asynchronous I/O.
- **RDY** Specifies that the process is ready to run and is waiting to use the CPU.
- **IOW** Specifies that the process is waiting for synchronous I/O, usually its expected standard input, to complete.
- **DET** Specifies that the process has output ready to be displayed and it is either waiting to be attached to a display console or waiting to have its output diverted to a specified console.
- **FZN** Specifies that the process is frozen due to an error. This usually means the process is trying to use a device which is faulty or incorrectly configured.

TTY*n* Specifies the output terminal, if any, to which the process is currently connected.

TTY0 Local console

TTY1 or TTY2
Telnet consoles.

SNK Process has been flushed.

Two dashes (--)
Process has been halted.

Comments
Specifies the user's login IP address provided during login when a user is logged in using Telnet (ROpCon).

Talk

Use the **talk** command to connect to other router processes, such as GWCON, MONITR, or CONFIG. After connecting to a new process, you can send specific commands to and receive output from that process. You cannot talk to the TASKER or OPCON process. See "Command History for GWCON and CONFIG Command Line" on page 24 for information on how to access previously entered GWCON or CONFIG commands.

To obtain the PID, use the OPCON **status** command. Once you are connected to the second-level process, such as CONFIG, use the intercept character, **Ctrl-P**, to return to the * prompt.

Syntax:

talk *pid*

Example: `talk 5`

When using third-level processes, such as IP Config or IP, use the **exit** command to return to the second level.

Telnet

Use the **telnet** command to remotely attach to another router or to a remote host. The only optional parameter is the terminal type that you want to emulate.

You can use the **telnet** command with IPv4 or with IPv6 addresses.

A router has a maximum of five Telnet sessions: two servers (inbound to the router), and three clients (outbound from the router).

Note: To use Telnet in a pure bridging environment, enable Host Services.

Syntax:

telnet *ip-address terminal-type*

Example 1: `telnet 128.185.10.30` or `telnet 128.185.10.30 23` or `telnet 128.185.10.30 vt100`

```
Trying 128.185.10.30  ...
Connected to 128.185.10.30
Escape character is '^]'
```

Example 2: `telnet 1:9::10`

```
Trying 1:9::10  ...
Connected to 1:9::10
Escape character is '^]'
```

When telneting to a non-existent IP address, the router displays:

```
Trying 128.185.10.30  ...
```

To enter the Telnet command mode, type the escape character-sequence, which is **Ctrl-]**, at any prompt.

```
telnet>
```

If you Telnet into a router,

- Press ← **Backspace** to delete the last character typed on the command line.

  Note: When using a VT100 terminal, do not press ← **Backspace** because it inserts invisible characters. Press **Delete** to delete the last character.
- Press **Ctrl-U** at the `telnet>` prompt to delete the whole command line entry so that you can reenter a command.

The Telnet command mode consists of the following subcommands:

close Close current connection

display
Display operating parameters

mode Try to enter line-by-line or character-at-a-time mode

open Connect to a site

quit Exit Telnet

send Transmit special characters (’send ?’ for more)

set Set operating parameters (’set ?’ for more)

status Print status information

toggle Toggle operating parameters (’toggle ?’ for more)

z Suspend Telnet

? Print help information

The **status** and **send** subcommands have one of two responses depending on whether or not the user is connected to another host. For example:

Connected to a host:

```
   telnet>    status
Connected to 128.185.10.30    Operating in character-at-a-time mode.    Escape character is ^].

   telnet>    send ayt
```

Note: The send command currently supports only ayt.

Not connected to a host:

```
   telnet>    status
   Need to be connected first.

   telnet>    send ayt

   Need to be connected first.
```

Use the **close** subcommand to close a connection to a remote host and terminate the Telnet session. Use the **quit** subcommand to exit the **telnet** command mode, close a connection, and terminate a Telnet session.

```
telnet>    close
```

or

```
telnet>    quit

logout
*
```

Part 2. Understanding, Configuring, and Using Base Services

Chapter 5. Using BOOT Config to Perform Change Management

This chapter describes how to use the Boot/Dump Configuration process. This chapter includes the following sections:

Understanding Change Management

Change management is the handling of software and configuration data for an IBM 2212. This involves:

1. Moving code and configuration data to and from the IBM 2212
2. Moving code and configuration data on the IBM 2212 persistent storage device, which is is a hard file or compact flash.
3. Selecting and activating specific combinations of software and configuration.

The change management functions are available by entering the **boot** command at the `Boot config>` prompt (talk 6), or the service recovery interfaceshould the box be in a condition where the hard file or compact FLASH does not contain viable software (that is, you cannot access talk 6).

The IBM 2212 code and configuration data storage resource is divided into areas called "system banks" (banks for short), each containing a single version of the operational code and any other files pertinent to that release of the code. Up to four configuration files are associated with each bank's software.

The general change management model of the IBM 2212 is to introduce new code and/or configuration data to the system while the system runs at its present level and then activate the changed code or configuration data set later. If for some reason the new code or configuration does not function as expected, you have the ability to revert to the previous version of the configuration.

Using the Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol that runs over the Internet UDP protocol. This implementation provides multiple, simultaneous TFTP file transfers between an IBM 2212's non-volatile configuration memory, image bank, and remote hosts.

TFTP allows you to:

- Get a configuration file from a server to an IBM 2212
- Put a configuration file from an IBM 2212 to a server
- Get load modules from a server to an IBM 2212
- Put load modules from an IBM 2212 to a server

Using BOOT Config

TFTP transfers involve a *client* node and a *server* node. The client node generates a TFTP Get or Put request onto the network. The IBM 2212 acts as a client node by generating TFTP requests from the IBM 2212 console using the `Boot config>` process **tftp** command.

The client can transfer a copy of a configuration file or image file stored in the image bank of a server.

The server is any device (for example, a personal computer or workstation) that receives and services the TFTP requests. When the IBM 2212 acts as a server, transfers are transparent to the user. Use the ELS subsystem TFTP message log to view the transfer in progress.

Loading an Image at a Specific Time

There may be occasions when you may want to load a device on a specific day and time when you will be unavailable. You can configure the device to perform a timed load using the **timedload activate** command. Other commands allow you to view a device's scheduled load information or cancel a scheduled load. See "Change Management Configuration Commands" on page 43 for information on these commands.

Chapter 6. Configuring Change Management

This chapter describe the Change management configuration commands. It includes the following sections:

- "Accessing the Change Management Configuration Environment"
- "Change Management Configuration Commands"

Accessing the Change Management Configuration Environment

To enter the change management configuration command environment, use the CONFIG **boot** command. When the router's software is initially loaded, it is running in the OPCON process, signified by the * prompt. From the * prompt:

1. Enter **talk 6**.
2. At the `Config>` prompt, type **boot**.

To return to the CONFIG process, type **exit**.

Change Management Configuration Commands

This section describes the Change Management Configuration commands. Each command includes a description, syntax requirements, and an example. Table 4 summarizes the Change Management Configuration commands.

After accessing the Change Management Configuration environment, enter the configuration commands at the `Boot config>` prompt.

Table 4. Change Management Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds an optional description to a configuration file.
Copy	Copies boot files and configuration files to or from banks.
Describe	Displays information about the stored loadfile images.
Disable	Turns off various change management functions.
Enable	Turns on various change management functions.
Erase	Erases a stored image or a configuration file.
List	Displays information about configuration files and scheduled load information.
Lock	Prevents the device from overwriting the selected configuration with any other configuration.
Set	Selects code bank and configuration to be used.
TFTP	Initiates TFTP file transfers between the IBM 2212 and remote servers.
Timedload	Schedules a load into the device on a specific day and time, cancels a scheduled load, or displays scheduled load information.
Unlock	Removes the lock from a configuration allowing the configuration to be updated by the device.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Add

Use the **add** command to add an optional description to a configuration file.

Syntax:

add configuration *file description*

load *image description*

Example: Boot config> **add**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 01:52 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970 00:30 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |

+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A]
Select the source configuration:  (1, 2, 3, 4): [1] 3
Enter the description of the file: () New config for today

Attempting to set description for bank A configuration 3.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:58 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        | New config for today           | 09 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 01:05 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |

+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.
```

Copy

Use the **copy** command to copy configuration files and load images to and from banks.

Syntax:

copy configuration *file*

load *image*

Example: Boot config>**copy load**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 01:26 |
```

```
| CONFIG 2 - AVAIL   *    | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL        |                                | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL        |                                | 01 Jan 1970 01:52 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL        |                                | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL        |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL        |                                | 01 Jan 1970 00:37 |
| CONFIG 4 - ACTIVE  *    |                                | 01 Jan 1970 00:24 |

+-------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A] b
Select the destination bank:  (A, B): [B] a
Copy SW load image from: bank B
                      to: bank A.


Operation completed successfully.
```

Example: Boot config>**copy configuration**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - CORRUPT         |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL        | test config for pubs           | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *    | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL        |                                | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL        |                                | 01 Jan 1970 01:52 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL        |                                | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL        |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL        |                                | 01 Jan 1970 00:37 |
| CONFIG 4 - ACTIVE  *    |                                | 01 Jan 1970 00:24 |

+-------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A]
Select the source configuration:  (1, 2, 3, 4): [1]
Select the destination bank:  (A, B): [B]

Select the destination configuration:  (1, 2, 3, 4): [1]
Copy SW configuration from: bank A, configuration 1
                         to: bank B, configuration 1.
/hd0/sys0/CONFIG0 --> /hd0/sys1/CONFIG0

Operation completed successfully.
```

If the copy fails you may receive one of the following messages:

Error: Active bank cannot be overwritten or erased.
: You attempted to copy a configuration into the bank currently in use by the IBM 2212.

Error: File copy failed.
: This condition occurs when the copy operation fails for reasons other than copying to the active configuration. The most common cause is specifying the same source and destination configurations. When you list (see “List” on page 48) the configurations, CORRUPT appears next to the bank that is damaged.

Describe

Use the **describe** command to display information about a stored image.

Syntax: describe

Example: Boot config>**describe**

```
+------------------------+------------------------+
|         BANK A         |         BANK B         |
| Product ID -   2212-AIS | Product ID -   2212-AIS |
| Version   3 Release   2 | Version   3 Release   2 |
| Maint.    0 PTF       0 | Maint.    0 PTF       0 |
| Feat.  3763 RPQ       0 | Feat.  3763 RPQ       0 |
| Date  21 Jul 1998 07:22 | Date  14 Jul 1998 07:33 |
| Build           cc_156c | Build           cc_155b |
+------------------------+------------------------+
```

Disable

Use the **disable** command to turn off various change management functions.

Syntax:

disable auto-boot

auto-boot

Disabling auto-boot causes the router boot sequence to stop at the service recovery interface, without running the router operational code. The default auto-boot mode is “enabled”.

Example:

```
Boot config>disable auto-boot
Auto-boot mode is now disabled
```

Enable

Use the **enable** command to turn on various change management functions.

Syntax:

enable auto-boot

auto-boot

Enabling auto-boot causes the router boot to the router operational code without stopping at the service recovery interface. The default auto-boot mode is “enabled”

Erase

Use the **erase** command to erase a stored image or a configuration file

Syntax:.

erase configuration [file]

load [image]

config or load

Erases a configuration file or a load image. Enter the config number to be erased after the **erase** command.

Example: Boot config>**erase load**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - CORRUPT        |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
```

```
| CONFIG 3 - NONE        |                                | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |

+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the bank to erase:  (A, B): [A] a
Erase SW load image from bank A.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |

+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.
```

Example: Boot config>**erase configuration**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 01:26 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 01:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |

+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A]
Select the configuration to erase:  (1, 2, 3, 4): [1] 3
Erase SW configuration file from bank A, configuration 3.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                |                   |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
```

```
+-----------------------+--------------------------------+------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.
```

Notice that the list command displays **NONE** by bank A, config 3.

If the erasure fails, a message indicating the failure appears on the console with the banks that failed.

List

Use the **list** command to display information about which load images and configuration files are available and active. This command may also be used to display boot options and scheduled load information.

Syntax:

list

Example: Boot config>**list**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+-----------------------+--------------------------------+-----------------+
  * - Last Used Config      L - Config File is Locked
  Auto-boot mode is enabled.


 Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank A.
The configuration is CONFIG 1 in bank A.
Boot config>
```

The possible file status descriptors are:

ACTIVE
: The file is currently loaded and is running on the 2212

AVAIL This is a valid file that can be made ACTIVE.

CORRUPT
: The file was damaged or not loaded into the 2212 completely. The file must be replaced.

LOCAL
: The file will be used only on the next reload or reset. After the file is used, it will be placed in AVAIL state.

PENDING
: This file will be loaded on the next reload, reset, or power-up of the 2212.

Lock

Use the **lock** command to prevent the device from overwriting the selected configuration with any other configuration.

Syntax:

lock

Example: Boot config>**lock**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Auto-boot mode is enabled.  Fast-boot
mode is disabled.Select the source bank:  (A, B): [A]

Select the source configuration:  (1, 2, 3, 4): [1] 4
Attempting to lock bank A and configuration 4.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL   L   |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.
```

Note: Note that bank A config 4 is marked with an “L.”

Set

Use the **set** command to select the code bank, the configuration to use, and the duration of use. The valid durations are:

once The configuration is active for the next boot only.

always
The configuration is active for all subsequent boots until changed again.

Syntax:

set

Example: Boot config>**set**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A] b

Select the source configuration:  (1, 2, 3, 4): [1] 4
Select the duration to use for booting:  (once, always): [always]
Set SW to boot using bank B and configuration 4, always.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

   Auto-boot mode is enabled.
```

TFTP

Use the **tftp** command to initiate TFTP file transfers between the 2212 and remote servers.

Note: When you unzip an image, you will see multiple files ending in ".ld". Use the **tftp get load modules** command to get multiple load modules.

Syntax:

tftp get	config
	load modules
tftp put	config
	load modules

Note for Dynamic Loading of Software: All of the load modules in the specified directory will be retrieved as part of the load going into the bank.

Example: Boot config>**tftp get load modules**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:14 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote modules directory: : (/u/bin) /usr/2212load/
Select the destination bank:  (A, B): [A] a
  TFTP SW load image
  get:   /usr/2212load/LML.ld
  from:  192.9.200.1
  to:    bank A.

Operation completed successfully.
```

Notes:
When putting files to a server:

1. Make sure that the files on the target server have the appropriate permissions that would allow anyone to write to those files. If not, the put operation will fail.

Timedload

Use the **timedload** command to schedule a load on a device, cancel a scheduled load, or view scheduled load information.

This command allows you to load the device outside peak network traffic periods when support personnel may not be present.

Note: You may also use the Configuration Program to schedule a reload for a device, which is not affected by reloads or power outages. These circumstances would normally cause the reload to be lost. See the chapter "Using the Configuration Program" in *Configuration Program User's Guide* for details.

Syntax:

timedload activate
deactivate
view

activate
Schedules a load on the device. You will be prompted for information for a time-activated load similar to the **tftp get load** and **tftp get config** commands. See "TFTP" on page 50 for information about the parameters.

Time of day to load the device
Specifies the date and time to load the device. Specify the value as *YYYYMMDDHHMM*, where:

YYYY is the four-digit year

Note: If the current month on the device is December, the year data must be the current year or the following year. Otherwise, if the current month on the device is January through November, the year data must be the current year.

MM is the two digit month.

MM Valid Values: 01 to 12 with 01 representing January.

DD is the two-digit day of the month.

DD Valid Values: 01 to 31, depending on the value of MM.

HH is the two-digit hour in 24-hour time.

HH Valid Values: 00 to 23

MM is the two-digit minute of the hour.

MM Valid Values: 00 to 59

The following are examples of scheduling a load from different sources.

Example 1. Load modules and configuration source is a remote host:

```
Boot config>timedload activate

+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |

+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Time Activated Load Processing...

Select the bank to use:  (A, B): [A] a
Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] yes

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote modules directory: : (/u/bin) /usr/601bin/205img
The destination bank is bank A
TFTP SW load image
  get:   /usr/601bin/205img/
  from:  192.9.200.1
  to:    bank A.
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'

Operation completed successfully.

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] yes

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (config.dat) /tftpboot/192.9.200.6.config
The destination bank is bank A
Select the destination configuration:  (1, 2, 3, 4): [1] 1
TFTP SW configuration file
  get:   /tftpboot/192.9.200.6.config
  from:  192.9.200.1
  to:    bank A, configuration 1.
tftp: connect to '192.9.200.1'
```

```
Operation completed successfully.

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>
```

Example 2. Load modules and configuration source is a bank:

```
Boot config>timedload activate

+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:39 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Time Activated Load Processing...

Select the bank to use:  (A, B): [A] a
Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] no

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] no

Select the configuration to use:  (1, 2, 3, 4): [1] 1

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>
```

deactivate

Cancels a scheduled load.

Example 1: Deactivate the time activated load

```
Boot config>timedload deactivate
Deactivate Load Timer Processing...

Do you want to deactivate the load timer? (Yes, No, Quit): [No] yes
The load timer has been deactivated.
Boot config>
```

view Displays scheduled load information.

```
Boot Config> timedload view
Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank A.
The configuration is CONFIG 1 in bank A.
Boot config>
```

Unlock

Use the **unlock** command to allow the device to overwrite the selected configuration that was previously locked.

Syntax:

unlock

Example: Boot config>**unlock**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
```

```
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL    L  |                                 | 01 Jan 1970 00:26 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A]

Select the source configuration:  (1, 2, 3, 4): [1] 4
Attempting to unlock bank A and configuration 4.

Operation completed successfully.
Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE        |                                 | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL       |                                 | 01 Jan 1970 00:14 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                 | 01 Jan 1970 00:24 |

+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

  Auto-boot mode is enabled.
```

Note: Note that bank A config 4 is no longer marked with an “L.”

Chapter 7. Using the Service Recovery Function

This chapter describes the service recovery function. It includes the following sections:

- "Accessing the Service Recovery Function"
- "Service Recovery Commands"

Accessing the Service Recovery Function

When powering on, the 2212 runs some diagnostic routines, loads boot code, and then runs the operational code. The operational code resides on the 2212's compact FLASH or hard file. If the system determines that the hard file or compact FLASH is unusable, you will need to recover it. A hard file or compact FLASH failure automatically places you at the service recovery function `SVC>` prompt.

If you are instructed by a service representative to use the service recovery function to update the 2212 boot code do the following to access the service recovery function:

1. Unplug and replug the 2212 to force it to reboot.
2. Watch the messages during the boot sequence. When you see,

   ```
   Jumping into OS/OPEN
   ```

   Press the space bar. You will then see the message:

   ```
   Do you wish to halt in service mode?
   ```

   If you enter **Yes**, the `SVC>` prompt is displayed. If you enter anything else, the 2212 continues booting. If you do nothing, a 5 second timer expires and booting continues.

Service Recovery Commands

This section describes the service recovery commands and tells you where to find the descriptions for these commands. This section also describes the commands unique to the service recovery function.

Table 5. Service Recovery Commands

The following commands perform change management functions for the service recovery function and are described in "Change Management Configuration Commands" on page 43:	
Command	**Function**
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds an optional description to a configuration file.
Copy	Copies boot files and configuration files to or from banks.
Describe	Displays information about the stored loadfile images.
Erase	Erases a stored image or a configuration file.
List	Displays information about configuration files and scheduled load information.

Table 5. Service Recovery Commands (continued)

Lock	Prevents the device from overwriting the selected configuration with any other configuration.
Set	Selects code bank and configuration to be used.
TFTP	Initiates TFTP file transfers between the IBM 2212 and remote servers.
Unlock	Removes the lock from a configuration allowing the configuration to be updated by the device.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.
The following Service Recovery function commands are described after this table.	
Command	**Function**
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Add	Adds the configuration description.
Baud-rate	Specifies the baud-rate of the 2212 service port.
Bootmode	Sets the bootmode.
Copy	Copies the software or configuration.
Debug	Switches to the debugger command menus.
Describe	Describes the software level information.
Dump	Sets the system dump parameters.
Erase	Erases the software or configuration.
Interface	Sets the recovery interface parmeters.
List	Lists the bank information.
Lock	Locks the configuration file.
Reboot	Reboots the 2212.
Set	Locks the configuration file
TFTP	Transfers TFTP software and configuration files.
Unlock	Unlocks the configuration file.
VPD	Specifies vital product data.
Writeboot	Writes boot code from flash memory to the hard file.
Writeos	Writes operational code from a memory bank to the hard drive.
Zmodem	Transfers zmodem software and configuration files.
The service function also supports the **diags** command which is described in “Diags” on page 30 .	

Add

Use the **add** command to add the configuration description.

Syntax:

add

Baud-rate

Use the **baud-rate** command to specify the baud-rate of the 2212 service port.

Syntax:

baud-rate

The service port speed may be configured for any of the valid values; however, the speed must match the speed configured for the ASCII terminal. See the installation instructions for more information on setting the service port speed.

Valid values:2400, 9600, 14400, 19200, 28800, 38400, 57600, or 115200 bps

Default value: 19200 bps

Bootmode

Use the **bootmode** command to program the 2212 to boot one of 3 different ways. Normally only used for service. Default is normal boot.

Syntax:

bootmode *mode*

- 1. Boot from recovery block. The recovery block is the operating system stored on the system card's FLASH. Also, the boot will stop at the service recovery interface prompt.
- 2. Boot from disk. This option causes the device to boot to the service recovery interface (SVC> prompt) and only load the operating system stored on the pending bank of the hard file or compact FLASH.
- 3. Normal boot from disk. This option causes the device to boot to the OPCON (*) prompt and to load all of the device's software.

Valid values: 1, 2, or 3

Default value: 3

Example:

```
svc>bootmode ?
Current Boot Mode:  Normal Boot from disk.
Valid boot modes are:
 1.  Boot from Recovery Block, stop at svc> prompt.
 2.  Boot from Disk, stop at svc> prompt.
 3.  Normal Boot from Disk.
Select the appropriate boot mode by number:
```

Copy

Use the **copy** command to copy the software or the configuration.

Syntax:

copy

```
svc>copy
        BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - PENDING        |                                | 10 Feb 1998 17:46 |
| CONFIG 1 - AVAIL       |                                | 10 Feb 1998 17:46 |
```

```
| CONFIG 2 - AVAIL       |                                | 09 Jan 1998 10:40 |
| CONFIG 3 - AVAIL       |                                | 06 Jan 1998 15:46 |
| CONFIG 4 - PENDING *   |                                | 02 Jan 1998 11:51 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 14 Feb 1998 15:38 |
| CONFIG 1 - AVAIL   *   |                                | 03 Feb 1998 14:43 |
| CONFIG 2 - AVAIL       |                                | 22 Jan 1998 13:43 |
| CONFIG 3 - AVAIL       |                                | 06 Jan 1998 17:25 |
| CONFIG 4 - AVAIL       |                                | 26 Jun 1998 09:48 |
+------------------------+--------------------------------+-------------------+
Load or Config? c
Enter source bank <A|B>: a
Enter source config <1-4>:3
Enter destination bank : b
Enter destination config <1-4>: 3
/hd0/sys0/CONFIG2 --> /hd0/sys1/CONFIG2
Copy configuration commmand successful!
```

Debug

Use the **debug** command to switch to the debugger command menus.

Attention: This command should only be used under the direction of service personnel.

Syntax:

debug

Describe

Use the **describe** command to view the software level information.

Syntax:

describe

```
svc>describe
+------------------------+------------------------+
|         BANK A         |         BANK B         |
| Product ID - 2212-AIS  | Product ID - 2212-AIS  |
| Version   3 Release   2| Version   3 Release   2|
| Maint.    0 PTF       0| Maint.    0 PTF       0|
| Maint.    0 PTF       0| Maint.    0 PTF       0|
| Feat.  3763 RPQ       0| Feat.  3763 RPQ       0|
| Date   8 Aug 1998 03:02| Date   8 Aug 1998 03:02|
| Build           cc_158e| Build           cc_158e|
|                   build|                   build|
+------------------------+------------------------+
```

Dump

Use the **dump** command to manipulate the 2212 dump mode. You can enable/disable, specify local/remote dump, and if remote, specify where the dump gets sent.

Syntax:

dump

Example:

```
svc>dump
This command enables or disables system dump and
selects the dump target as disk or remote host.

Dump is currently disabled.
Do you want to enable dump? y
Dump is currently enabled.
Dump Target:  Remote Host on Network.
Enter Dump Target (Disk or Network or  to keep current value):

Remote Host settings:
 IP address:  255.255.255.255
 Remote Filename:  /foo/foo
 Remote file will be compressed and "0.cmp", "1.cmp", or "2.cmp" will be
 appended to the end of the filename.

Do you want to set or change the remote dump parameters ? n
```

```
svc>dump
This command enables or disables system dump and
selects the dump target as disk or remote host.

Dump is currently enabled.
Do you want to disable dump ? y
Dump is currently disabled.
Dump Target:  Remote Host on Network.
Enter Dump Target (Disk or Network or  to keep current value):

Remote Host settings:
 IP address:  255.255.255.255
 Remote Filename:  /foo/foo
 Remote file will be compressed and "0.cmp", "1.cmp", or "2.cmp" will be
 appended to the end of the filename.

Do you want to set or change the remote dump parameters ? y
Press  to save current setting.

Enter IP address (0.0.0.0 form): 1.1.1.3
Enter remote path and filename (32 chars max):  /tmp/2212dump
Enter Remote File Compression Mode (Compressed or Uncompressed): compressed
Remote Host settings:
 IP address:  1.1.1.3
 Remote Filename:  /tmp/2212dump
 Remote file will be compressed and "0.cmp", "1.cmp", or "2.cmp" will be
 appended to the end of the filename.

Do you want to save the new network dump parameters ? y
Remote Host settings:
 IP address:  1.1.1.3
 Remote Filename:  /tmp/2212dump
 Remote file will be compressed and "0.cmp", "1.cmp", or "2.cmp" will be
 appended to the end of the filename.

You must reboot in order for these changes to take effect.
```

Erase

Use the **erase** command to erase the software or configuration.

Syntax:

erase

Interface

Use the **interface** command to configure the 2212 to have a recovery LAN interface. This is used in the event the full router is not functional, and especially in cases of hardware service, should the 2212's primary code/config storage have a problem.

Syntax:

interface

Example:

```
svc>interface
Current Interface settings:
 Device Type:  Ethernet
 Slot Number:  1
 Port Number:  1
 IP address:  1.1.1.4
 Net Mask:  255.255.255.0
Warning:  There is currently no adapter in slot 1.
Do you want to set or change the interface parameters ? y
Press  to save current setting.

Enter LAN interface type (Eth or Tkr): eth
Enter Slot Number (1-5): 1
Enter Port Number (1-2): 1
Enter IP address (0.0.0.0 form) : 1.1.1.4
Enter Netmask (0.0.0.0 form): 255.255.255.0
Current Interface settings:
 Device Type:  Ethernet
 Slot Number:  1
 Port Number:  1
 IP address:  1.1.1.4
 Net Mask:  255.255.255.0
Warning:  There is currently no adapter in slot 1.
Do you want to save the new interface parameters ? y
Current Interface settings:
 Device Type:  Ethernet
 Slot Number:  1
 Port Number:  1
 IP address:  1.1.1.4
 Net Mask:  255.255.255.0
Warning:  There is currently no adapter in slot 1.
You must reboot in order for these changes to take effect.
```

List

Use the **list** command to list the bank information

Syntax:

list

Lock

Use the **lock** command to lock the configuration file

Syntax:

lock

Reboot

Use the **reboot** command to reboot the 2212 after writing either the boot code or the operational code. The system performs all diagnostics and then loads the boot and operational code normally.

Note: Whether or not the operational code is loaded normally depends on how the bootmode is set.

Syntax:

reboot

Set

Use the **set** command to activate software and the configuration.

Syntax:

set

Example:

```
svc>set ?
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - PENDING        |                                 | 10 Feb 1998 17:46 |
| CONFIG 1 - PENDING *   |                                 | 10 Feb 1998 17:46 |
| CONFIG 2 - AVAIL       |                                 | 09 Jan 1998 10:40 |
| CONFIG 3 - AVAIL       |                                 | 06 Jan 1998 15:46 |
| CONFIG 4 - AVAIL       |                                 | 02 Jan 1998 11:51 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 03 Feb 1998 14:42 |
| CONFIG 1 - AVAIL   *   |                                 | 03 Feb 1998 14:43 |
| CONFIG 2 - AVAIL       |                                 | 22 Jan 1998 13:43 |
| CONFIG 3 - AVAIL       |                                 | 06 Jan 1998 17:25 |
| CONFIG 4 - AVAIL       |                                 | 26 Jun 1998 09:48 |
+------------------------+---------------------------------+-------------------+
Enter target bank <A|B>: a
Enter target config <1-4>:
```

TFTP

Use the **tftp** command to transfer software and/or configuration files onto the 2212.

Syntax:

tftp

Example:

```
svc>tftp ?
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - PENDING        |                                 | 10 Feb 1998 17:46 |
| CONFIG 1 - AVAIL       |                                 | 10 Feb 1998 17:46 |
| CONFIG 2 - AVAIL       |                                 | 09 Jan 1998 10:40 |
| CONFIG 3 - AVAIL       |                                 | 06 Jan 1998 15:46 |
| CONFIG 4 - PENDING *   |                                 | 02 Jan 1998 11:51 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 03 Feb 1998 14:42 |
| CONFIG 1 - AVAIL   *   |                                 | 03 Feb 1998 14:43 |
| CONFIG 2 - AVAIL       |                                 | 22 Jan 1998 13:43 |
| CONFIG 3 - AVAIL       |                                 | 06 Jan 1998 17:25 |
| CONFIG 4 - AVAIL       |                                 | 26 Jun 1998 09:48 |
+------------------------+---------------------------------+-------------------+
Load or Config?l
Specify the server IP Address:
Enter destination bank <A|B>:
```

Unlock

Use the **unlock** command to unlock the configuration file.

Syntax:

unlock

VPD

Use the **vpd** command to enter 2212 vital information.

Syntax:

vpd

Writeboot

Use the **writeboot** command to write the 2212 bootstrap code to system card boot flash from the specified software load bank. You will receive a message telling you that the write was successful. Use the **reboot** command to cause the 2212 to reboot after the system writes the code.

Syntax:

writeboot

Example:

```
SVC> writeboot
Enter bank to write boot code from (A,B) [A]? B
Boot code written successfully.
```

Writeos

Use the **writeos** to write a new version of the operating system code to the recovery block on the system card's FLASH from the specified software load bank. The system prompts you for the bank from which the code is copied. You will receive a message telling you that the write was successful. Use the **reboot** command to cause the 2212 to reboot after the system writes the code.

Syntax:

writeos

Example:

```
SVC> writeos
Enter bank to write os from (A,B) [A]? B
Operational code written successfully.
```

Zmodem

Use the **zmodem** command to transfer software and configuration files onto the 2212. The interface for transferring is designed so that you cannot overwrite any active file.

Note: When using zmodem to transfer several files ending in `.ld` (multiple load module image), you must transfer each of the modules one by one to get the entire load module image.

Syntax:

zmodem

Chapter 8. The Configuration Process (CONFIG - Talk 6) and Commands

This chapter describes the CONFIG process and includes the following sections:

What is CONFIG?

The Configuration process (CONFIG) is a second-level process of the router user interface. Using CONFIG commands, you can:

- Set or change various configuration parameters
- Add or delete an interface to the hardware configuration
- Enter the Boot CONFIG command mode
- Enter the Quick Configuration mode
- Clear, list, or update configuration information
- Enable or disable console login
- Communicate with third-level processes, including protocol environments

Note: Refer to the chapter "Migrating to a New Code Level" in *IBM 2212 Access Utility Service and Maintenance Manual* for information about migrating to a new code level.

CONFIG lets you display or change the configuration information stored in the router's nonvolatile configuration memory. Changes to system and protocol parameters do not take effect until you restart the router orreload the router software. (For more information, refer to the OPCON **reload** command in "Chapter 3. The OPCON Process" on page 27).

Note: You must enter the **write** command to save the changes in the device's flash memory.

The CONFIG command interface is made up of levels that are called modes. Each mode has its own prompt. For example, the prompt for the TCP/IP protocol is `IP config>`.

If you want to know the process and mode you are communicating with, press **Return** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access and exit the various levels in CONFIG. See Table 7 on page 75 for a list of the commands you can issue from the CONFIG process.

Config-Only Mode

Config-Only mode is entered if the configuration file that you are using is empty or no protocols are configured. Config-Only mode can also be entered manually to recover from an invalid configuration that is causing the router to crash during start-up.

Automatic Entry Into Config-Only Mode

Config-Only mode is entered if the router is booting with an empty configuration file or the configuration file contains incomplete configuration data.

The following conditions cause the router to enter Config-Only mode:

- Devices are configured but no protocols are configured.
- The configuration file is empty.

Manual Entry Into Config-Only Mode

To enter Config-Only mode, do one of the following:

- To reload or restart the router with no configuration.

  To reload or restart the router with no configuration, use the **erase** change management configuration command. Then use the **set** change management configuration command to select the empty configuration file. You can access these commands from the `Boot>` promptor from the service recovery interface.
- Reload or restart the router with no protocols configured.

  To create a configuration that has no protocols configured, use the **clear** command to clear the protocol configuration information.

Quick Configuration

Quick Configuration (Quick Config) provides a minimal set of commands that allow you to configure bridging protocols and routing protocols present in the router load. You can also configure an SNMP community with WRITE_READ_TRAP access. This is useful during initial setup because the configuration program uses SNMP SET commands to transfer the configuration.

Important: At least one network device must be configured before using quick config. To add a device, use the **add device** command at the `config(only)>` or `config>` prompt.

The following table lists the protocols supported by Quick Config.

Table 6. Quick Config Capabilities

Bridging Protocols	Routing Protocols
STB, SRT, SRB	IP, IPX, DNA IV

Quick Config complements the existing configuration process by offering a shortcut. This shortcut allows you to configure the minimum number of parameters for these bridging protocols and routing protocols without having to exit and enter the different configuration processes. The other parameters are set to selected defaults.

Situations that call for the router to be quickly configured are:

- Blank or corrupted configuration memory, such as when one of the following situations occurs:
  - The router is configured for the first time.
  - Voltage fluctuations caused corruption of the hard file.
- Demonstration purposes, for which the router needs to be quickly configured to demonstrate its capabilities.
- Bench-marking tests to get the tests going without having to learn the router's operating system commands.

Quick Config operates as follows:

- It asks a series of questions with default values.
- It offers a short-cut to the detailed configuration of the normal mode command set.

Quick Config sets a number of default parameters based upon how you answer the configuration questions. What cannot be configured with Quick Config can be configured using Config after exiting Quick Config.

You cannot delete Quick Config information from within Quick Config. However, you can correct information either by exiting and returning to Quick Config, or by entering the **reload** command as a response to some Quick Config questions.

For complete information on using the Quick Config software, see "Appendix A. Quick Configuration Reference" on page 571.

Manual Entry Into Quick Config Mode

You might want to run Quick Config manually to demonstrate the router's capabilities or to reconfigure dynamically to perform benchmark tests without having to learn the router's operating system commands.

To enter Quick Config, type **qconfig** at the `Config>` prompt.

Exiting from Quick Config Mode

To exit Quick Config, restart by entering **r** from any prompt. Follow the queries until you enter **no** and then enter **q** to quit. The router returns to either the `Config (only)>` or the `Config>` prompt.

Configuring User Access

The router configuration process allows for a maximum of 50 user names, passwords, and levels of permission. Each user needs to be assigned a password and level of permission. There are three levels of permission: *Administration, Operation,* and *Monitoring*.

For more information, see the **add user** command.

Technical Support Access

If you are the system administrator, when you add a new user for the first time, you are asked if you want to add Technical Support access. If you answer yes, Technical Support is granted the same access privileges that you have as system administrator.

The password for this account is automatically selected by the software and is known by your service representative. This password can be changed using the **change user** command; however, if you do change the password, customer service cannot provide remote support. For additional information on the use of the **change user** command, see “Change” on page 83.

Configuring Spare Interfaces

Occasionally, you may need to configure a new interface along with its bridging and routing protocols without having to restart the device. You can accomplish this by configuring a number of ***spare interfaces*** on your device. Spare interfaces are useful if:

- You are adding dial circuits to your device.

  Use spare interfaces to add new V.25bis, V.34, or ISDN dial circuits on an existing V.25bis, V.34, or ISDN interface.

To configure a spare interface:

1. Access the CONFIG process by entering **talk 6**.
2. Configure the number of spare interfaces for the device using the **set spare-interfaces** command.
3. Exit the CONFIG process by pressing **Ctrl-P**.
4. Reload the device.

Example:

```
* talk 6
Config> set spare 2
Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]) yes
```

When the device reloads, the spare interfaces are installed as null devices.

To use one of the spare interfaces:

1. Insert the new adapter into the adapter slot.
2. Access the CONFIG process by entering **talk 6**.
3. Add an interface or a dial circuit using the **add device** command, if necessary.
4. Configure the spare interface by using the **net** command to configure the interface.
5. Configure the various protocols and features using the **protocol** and **feature** commands.
6. Exit the CONFIG process by pressing **Ctrl-P**.
7. Access the GWCON process by entering **talk 5**.
8. Bring the new interface online to the network using the **activate** command.

The following example shows how to configure and activate a new dial circuit on which the IP protocol is enabled. The dial circuit and IP protocol configuration are not shown.

Example:

```
*talk 6
Config> add device dial-circuit
Config> net 6
Circuit configuration
Circuit config>

⋮
 Here you would configure the dial circuit


⋮
Circuit config> exit
Config> protocol ip
IP>


⋮
 Here you would configure the IP protocol on the dial circuit.

⋮
IP> exit
Config>
*talk 5
+activate 6
```

Restrictions for Spare Interfaces

The **activate** command cannot be used to activate a new interface on the network under the following conditions:

- You have already entered a **delete interface** command. The device must be restarted if ***any*** interface has been deleted. You cannot delete a spare interface (indicated by ***null*** in list displays).
- The spare interface is the only interface that enables a protocol or feature. The protocol or feature must already be enabled on an existing interface before it can be used by a spare interface.
- The new spare interface has a header size or trailer size greater than the sizes for other interfaces.
- There is not enough memory to allocate receive buffers for the new interface.

In these cases, you must restart the device to bring the new interface online.

You can configure the following interfaces as spare interfaces, but you cannot activate them on the network using the **activate** command:

- SDLC
- SDLC Relay
- V.25bis
- PPP Multilink master and dedicated link nets

You must restart the device to bring these interfaces online.

You can configure the following protocols on spare interfaces, but you cannot activate them on the network using the **activate** command:

- IPv6
- LNM
- OSI/DECnet V

- XTP

Note: When using the configuration program, use the following to work with spare interfaces:

1. Make the configuration changes for the spare interface on the device
2. Enter the **activate** command on the device to bring the spare interface, protocols, and features online
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

There are requirements for certain functions. These are:

APPN	To activate this protocol on a spare interface, you must first activate the interface and then configure the protocol on the activated interface.
Bandwidth Reservation (BRS)	To configure BRS on a spare interface, you must enable BRS on each network interface where Frame Relay circuits will be active before activating the spare interface. After activating the spare interface, you can then use BRS configuration commands to make changes such as adding a traffic class or assigning a protocol to a traffic class.
DECnet IV	To activate this protocol on a spare interface, you must first activate the interface and then configure the protocol on the activated interface. Use the DECnet IV **set** command to activate the configuration changes.
Frame Relay	• You cannot activate an FR dial circuit interface unless the dial circuit's base net is already active. • An activate for an FR dial circuit will fail if the frame size, MAC header, or trailer required by the spare interface is larger than other dial circuits already assigned to the base net. • If data compression is not already active in the device, data compression will not work on a spare interface defined for data compression.
BGP	Use the BGP **reset neighbor** command to activate new neighbors.
IPX	Use the **reset** command to activate static routes, static services, and filter lists on the spare interface.
PPP	• If data compression is not already active in the device, data compression does not work on a spare interface defined for data compression. • You cannot activate a spare PPP interface if the device's global buffer is too small to support a 1500-byte PPP MRU. • You cannot activate a PPP dial circuit interface unless the dial circuit's base net is already active. • An activate for a PPP dial circuit will fail if the frame size, MAC header, or trailer required by the spare interface is larger than other dial circuits already assigned to the base net.
Bridging	• Bridging was not already active. • NetBIOS filters are defined on the spare interface. • The spare interface caused a change to the bridge personality or behavior (for example, adding SR port to pure TB bridge or SR-TB conversion enabled).
IP	Use the reset IP command to bring configuration changes online for access-controls and packet-filters.

WAN Restoral/ WAN Reroute

The spare interface cannot be activated if any of the following conditions exist:

- The spare interface is configured as a WRS primary, and its configured WRS secondary is already a WRS primary or WRR primary or WRR alternate.
- The spare interface is configured as a WRS primary, and its configured WRS secondary is already actively restoring some other WRS primary.
- The spare interface is configured as a WRS secondary, and its configured WRS primary is already a WRS secondary or WRR primary or WRR alternate.
- The spare interface is configured as a WRS secondary, and its configured WRS primary is already actively being restored by some other WRS secondary.
- The spare interface is configured as a WRR primary, and its configured WRR alternate is already a WRS primary or WRS secondary or WRR primary or WRR alternate.
- The spare interface is configured as a WRR alternate, and its configured WRR primary is already a WRS primary or WRS secondary or WRR alternate.
- The spare interface is configured as a WRR alternate, and its configured WRR primary is already actively being rerouted by some other WRR alternate.

Resetting Interfaces

Occasionally, you might need to change the configuration of a network interface along with its bridging and routing protocols without restarting the device. The **reset** command allows you to disable a network interface and then enable it using new interface, bridging and routing configuration parameters.

The interface, protocols and features configuration parameters are changed using the CONFIG process (talk 6) commands. The talk 6 commands affect the contents of the configuration memory. The configuration changes are activated by issuing the GWCON process (talk 5) **reset** command.

To reset an interface:

1. Access the CONFIG process (talk 6).
2. Use the **net** command and other commands to change configuration parameters.
3. Use the **protocol** and **feature** commands to change the interface-based configuration parameters.
4. Exit the CONFIG process by pressing **Ctrl-P**.
5. Access the GWCON process (talk 5).
6. Use the **reset** command to reset the interface and the protocols and features on the interface.

Example:

```
*talk 6
Config>net 1
PPP Config>

. . . change PPP parameters . . .

PPP Config>exit
Config>protocol ipx
```

Using the CONFIG (Talk 6) Process

```
IPX Config>

. . . change IPX parameters on the PPP interface . . .

IPX Config>exit
Config>
*talk 5
+reset 1
Resetting net 1 PPP/0...successful
```

Note: When using the configuration program, do the following to make configuration changes to existing interfaces:

1. Make the configuration changes for the interface on the device
2. Enter the **reset** command to reset interface, protocol and feature parameters
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

Restrictions for Resetting Interfaces

The **reset** command cannot be used to reset a network interface if:

- You have already entered a **delete interface** command. The device must be restarted if any interface has been deleted.
- You have changed the hardware or data link type. For example, changing the data link type from PPP to Frame Relay.
- You have configured a larger MTU.
- You have configured a routing protocol or bridging on the interface, but that routing protocol or bridging is not currently active in the device.

In these situations, you must restartreload the device to activate the configuration changes.

You can change the configuration parameters of the following types of interfaces, but you cannot activate the changes using the **reset** command:

- PPP Multilink master and dedicated link nets
- ISDN
- X.25
- SDLC
- SDLC Relay
- V.25bis

You must restartedreload the device to activate these configuration changes.

You can change the configuration parameters of the following protocols and features, but you cannot activate the changes using the **reset** command:

- AppleTalk
- Vines
- OSI/DECnet V
- LNM
- XTP
- WAN Restoral
- WAN Reroute

You must restartreload the device to activate these configuration changes.

There are also requirements for certain functions. They are:

PPP dial circuits	A PPP dial circuit cannot be reset if any of the dial circuit parameters have changed.
Frame Relay dial circuits	A Frame Relay dial circuit cannot be reset if any of the dial circuit parameters have changed.
Compression	Compression requires large header and trailer sizes. Unless compression is already enabled on some other interface, it is likely that the header and trailer sizes will be too small. In this case, compression is disabled automatically on the interface and an ELS message is logged (rather than causing the entire reset interface to fail).
Bridging	• Bridging was not already active. • NetBIOS filters are defined on the interface you are resetting. • The reset interface caused a change to the bridge personality or behavior (for example, adding SR port to pure TB bridge or SR-TB conversion enabled).
BGP	Use the BGP **reset neighbor** command to activate neighbor configuration changes.
APPN	Use the **activate_new_config** command to activate configuration changes.
IPX	Use the IPX **reset** command to activate configuration changes for static routes, static services, and filter-lists.
DNA IV	Use the DNA IV **set** command to activate configuration changes.
SNMP	Use the SNMP **revert** command to activate configuration changes.

Using System Dumps

A useful tool for debugging problems with the 2212 is the system dump. The dump is a compressed snapshot that the system saves to the hard file.

To configure dumping:

1. Specify which three dump files you will save. See page 102 for more information.
2. Specify whether you want dumping re-enabled after a dump occurs. See page 101 for more information.
3. Specify the dump target as the local hard file if one is present, or specify a remote host on the network. See page 102
4. Enable dumping on the 2212. See page 90 for more information.

You can view the status of system dumping or retrieve a dump from the system. See “System View” on page 107 and “System Retrieve” on page 106, respectively.

Chapter 9. Configuring and Monitoring the CONFIG Process

This chapter describes the CONFIG process configuration and operational commands. It includes the following sections:

- "Entering and Exiting CONFIG"
- "CONFIG Commands"

Entering and Exiting CONFIG

To enter CONFIG from OPCON (*):

1. At the OPCON prompt, enter the **status** command to find the PID of CONFIG. (See page 11 for a sample output of the **status** command.)

   ```
   * status
   ```

2. Enter the OPCON **talk** command and the PID for CONFIG:

   ```
   * talk 6
   ```

The console displays the CONFIG prompt (`Config>`). Now, you can enter CONFIG commands. If the prompt does not appear, press the **Return** key again. To exit CONFIG and return to the OPCON prompt (*), enter the intercept character. (The default is **Ctrl-P** .)

CONFIG Commands

This section describes each of the CONFIG commands. Each command includes a description, syntax requirements, and an example. The CONFIG commands are summarized in Table 7.

After accessing the CONFIG environment, enter the configuration commands at the `Config>` prompt.

Table 7. CONFIG Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds an interface to the router configuration, or a user to the router.
Boot	Enters Boot CONFIG command mode.
Change	Changes a user's password or a user's parameter values associated with this interface. Also changes a slot/port of an interface.
Clear	Clears configuration information.
Delete	Deletes an interface from the router configuration or deletes a configured user. Also deletes system dump files.
Disable	Disables login from a remote console,
Enable	Enables login from a remote console, enables modem use
Event	Enters the Event Logging System configuration environment.
Feature	Provides access to configuration commands for independent router features outside the usual protocol and network interface configuration processes.
List	Displays system parameters, hardware configuration, a complete user list.
Load	Lists, adds, or deletes optional software packages.
Network	Enters the configuration environment of the specified network.

Table 7. CONFIG Command Summary (continued)

Command	Function
Patch	Modifies the router's global configuration.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Qconfig	Initiates the Quick Config process.
Set	Sets system-wide parameters for buffers, host name, inactivity timer, packet size, prompt level, number of spare interfaces, dump parameters, location, and contact person.
System Retreive	Retrieves dumps
System View	Displays the dump settings and the current dump status. Also displays a summary of the dumps.
Time	Keeps track of system time and displays it on the console.
Unpatch	Restores patch variables to default values.
Update	Updates the current version of the configuration.
Write	Writes the current configuration information to the nonvolatile memory.

Add

Use the **add** command to add an interface to the configuration, or user-access. This command also recreates device records if the configuration is inadvertently lost.

Syntax:

add
- callback . . .
- device
- isdn-address . . .
- ppp-user
- tunnel-profile
- user . . .
- v25-bis-address
- v34-address

Callback

Use the **add callback** command to add, delete, or list information for callback on ISDN.

Add	Adds a callback number to the authentication lists.
Delete	Deletes a callback number from the authentication list.
Lists	Displays the authentication list and othere related information.

device *device_type additional-config-info*

With the **add device** command, you must enter the interface device type (*device_type*). You are prompted for additional configuration parameters. This additional information varies by device and platform. Refer to "Accessing Network Interface Configuration and Operating Processes" on page 18 for additional information about device type and configuration parameters.

Note: If you are adding more than one interface, the order in which you add them is important because the router assigns a sequential interface number to the device when it is added. This interface number is an index number in the device list; it links the device with other protocol configuration information, such as the IP addresses associated with the device. (For more information, refer to the **list devices** command, "List" on page 92.)

All device and protocol configuration information related to network interfaces is stored by interface number. Any changes made to interface numbers will invalidate much of the device configuration information in the protocols.

Example:

```
add device dial-circuit
Adding device as interface 2
```

To determine which devices you can add, use the **add devices ?** command.

isdn-address *address-name network-dial-address network-subdial-address*
Adds the local and remote numbers of the ISDN end-points that will be communicating with your router.

address-name
Can be anything (such as a description of the port).

network-dial-address
The telephone number of the local or the destination port.

network-subdial-address
The additional part of the telephone number, such as an extension, that gets interpreted when the interface connects to a PBX; this parameter is optional.

Note: You can use punctuation, such as parentheses and dashes, but the punctuation is not significant (the router uses only the numbers).

```
Example: add isdn-address line 1 local
Assign network dial address [0 - 32 digits]? 1 2345 67
Assign network subdial address [0 - 19 digits]? 98765
```

ppp-user
Adds the user profile of a remote user to the local PPP user data base. You can add up to 500 users. You add a PPP user for each remote router or DIALs client that can connect to the device you are configuring. You must configure PPP users if either of the following conditions exist:

- You are using PPP authentication protocols, PPP encryption, or allowing users to use the dial-out feature. You need to configure a PPP user for either type of encryption - Encryption Control Protocol (ECP) or Microsoft Point-to-Point Encryption (MPPE); however, MPPE does not require the encryption key.
- You want the PPP user data base to be locally stored and managed by the device. If you want PPP user information to be obtained from a RADIUS, TACACS, or TACACS+ server, then you should configure the Authentication feature instead of configuring local PPP users.

Note: MPPE cannot use the RADIUS, TACACS, or TACACS+ server. For MPPE, the PPP user data base must be local.

If ECP has been enabled for the user, you are prompted for the PPP user name, password, IP address, and encryption key .

If the DIALs feature is in the software load, you are asked if this is a DIALs user.

If you are adding a user for a DIALs client, then you are prompted for the hostname, type of route, network mask, connect time, call-back information, and dial-out capability.

See “Using a Dial-In Access to LANs (DIALs) Server” in the *Using and Configuring Features* for more information.

A user profile stored locally on the device consists of the following:

Name The userid of the PPP user, used during authentication. See “PPP Authentication Protocols” on page 377.

Password
The password known to the user and the device, used during authentication. It can be up to 31 characters in length, consist of any alphanumeric character, and is case sensitive. See “PPP Authentication Protocols” on page 377 for more information.

Enter again to verify
Enter the password again for verification.

Allow inbound access
Allows inbound access to this user profile.

Valid values: yes, no

Default value: no

Will user be tunneled?
Specifies whether this dial-in user should be tunneled to an LNS destination. If you enter “yes”, you are prompted for information about the LNS.

Valid values: yes, no

Default value: no

Number of days before account expiry
The number of days before the password expires.

Valid values: 0 to 360

Default value: 180

Number of grace logins allowed
The number of login attempts allowed after the password expires.

Valid values: 0 to 100

Default value: 0

Hostname to use when connecting to this peer:
Specifies the local hostname of this LAC that is passed as identification to the LNS during tunnel setup.

Tunnel Server endpoint:
Specifies the IP address of the LNS to which this user is tunneled.

Type of Route
Either “Host Route” or “Net Route.”

A host route is generally applied for single-user access. A net route is generally applied to a network access. A net route allows you to enter a net mask.

IP Address
IP address to be assigned to a user.

A user profile-based IP address to offer to a dial-in client if requested. There are a number of ways for a 2212 to obtain an IP address for a dial-in client. See “IP Control Protocol” on page 383 for more information.

Valid values: any valid IP address

Default value: none

Net-Route Mask
Mask for a network user.

If the dial-in user is connecting to a DIALs-enabled PPP interface, the router automatically adds a temporary static route to that client for the duration of the PPP session. Typically, this static route has a net mask of 255.255.255.255 (the default value), which implies that there is a single IP host at the other end of the PPP link. However, the net mask can be overridden. If configured, this mask is used when adding the temporary route. An example of this is a small router with a single network of hosts that dials into a DIALs-enabled router. The single route to the small office router will be installed automatically based on the user profile, making it unnecessary to configure routing protocols between the two hosts and cutting down on routing traffic overhead over a potentially slow link.

Hostname
Hostname to be sent to the Proxy DHCP server for use by Dynamic DNS. See “Using a Dial-In Access to LANs (DIALs) Server” in *Using and Configuring Features* for more information.

Time-Allotted
The length of time a DIALs user can be connected. This is the total for this session, and should not be confused with an inactivity timer.

Valid Values: 0 to 71 827 788 minutes (0=unlimited)

Default Value: 0

Callback type
Call-back method, either “Roaming” or “Required.” The call-back parameters are used to specify whether the router will call back the user and what number to call back. See “Configuring PPP Callback” on page 381 for additional information.

Dial-Out
Enables dial-out.

This parameter is specific to clients using the DIALs dial-out client. Enabling dial-out for a ppp-user allows this user to access a modem-pool of dial-out circuits. See “Using a Dial-In Access to LANs (DIALs) Server” in *Using and Configuring Features* for more information.

Set encryption key

Specifies whether ECP encryption is to be enabled for this user/port.

Valid values: yes, no

Default value: no

ECP encryption key

Enter 16-character ECP encryption key.

This parameter is displayed only if PPP Encryption Control Protocol (ECP) has been enabled using the talk 6 `PPP Config>` **enable ecp** command. MPPE does not require an encryption key. This ECP encryption key is used by the PPP Encryption Control Protocol (ECP). See "Using and Configuring Encryption Protocols" in *Using and Configuring Features*.

Disable user

Allows you to disable a user-profile.

Valid values: yes, no

Default value: no

Example:

```
Config> add ppp-user
Enter name:  [ ]? pppusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No]
Number of days before account expiry[0-1000] [0]? 10
Number of grace logins allowed after an expiry[0-100] [0]? 5
IP address: [0.0.0.0]? 1.1.1.1
Set ECP encryption key for this user? (Yes, No): [No] no
Disable user ? (Yes, No): [No]

     PPP user name: pppusr01
   User IP address: 1.1.1.1
      Virtual Conn: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
   Account expires: Sun 17Feb2036 06:28:16
  Account duration: 10 days  00.00.00
   Password Expiry: <unlimited>

User 'pppusr01' has been added
```

Example:

```
Config> add ppp-user
Enter name:  [ ]? tunusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connection to this peer: []? host01
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

--more--           PPP user name: tunusr01
--more--                Endpoint: 1.1.1.1
--more--                Hostname: host01

User 'tunusr01' has been added
```

Example with ECP encryption:

```
Config>add ppp-user
Enter name:  [ ]? ppp_user2
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expiry[0-1000] [0]?
Number of grace logins allowed after an expiry[0-100] [0]?
IP address: [11.0.0.185]?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No] y
Encryption key should be 16 characters long.
Encryption Key (16 characters ) in Hex(0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex(0-9, a-f, A-F):
ECP encryption key is set.
Disable user ? (Yes, No): [No]


     PPP user name: ppp_user2
   User IP address: 11.0.0.185
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
           Callback type: disabled
          Dial-out: disabled
        Encryption: enabled
             Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'ppp_user1' has been added
```

tunnel *tunnel-name*

Gives a tunnel peer access through an IP network to the router. The peer is then authorized to initiate tunneled PPP sessions into the router. To configure a tunnel you must specify:

Name The hostname of the tunnel peer.

Hostname to use when connecting to this peer
The local hostname to use when connecting to this peer. This name is used for identification of the host on the peer.

Set shared secret
Specifies whether a shared secret is to be used.

Shared Secret
The secret shared between the LAC and LNS. It must be exactly the same on both ends of the tunnel.

Enter again to verify
Enter the shared secret again for verification.

Tunnel-Server endpoint address
The IP address of the tunnel peer (LAC or LNS).

Example:

```
Config> add tunnel
Enter name:  []? tunnel02
Enter hostname to use when connecting to this peer: []? host02
Set shared secret? (Yes, No): [No]? yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 2.2.2.22
```

```
Tunnel name: tunnel02
   Endpoint: 2.2.2.22
```

user *user_name*

Gives a user access to the router. You can authorize up to 50 users to access the router. Each *user_name* is eight characters and is case-sensitive.

When the first user is added, console login is automatically enabled. Each user added must be assigned one of the permission levels defined in Table 8.

When users are added, set login authentication to local. Otherwise a remote server must be used.

Table 8. Access Permission

Permission Level	Description
Administrator (A)	Displays configuration and user information, adds/modifies/deletes configuration and user information. The Administrator can access any router function.
Operator (O)	Views router configuration, views statistics, runs potentially disruptive tests, dynamically changes router operation, and restarts the router. Operators cannot modify the permanent router configuration. All actions can be undone with a system restart.
Monitor (M)	Views router configuration and statistics but cannot modify or disrupt the operation of the router.
Tech Support	Allows your service representative to gain access to the router if a password is forgotten. Cannot be assigned to users.

Note: To add a user, you must have administrative permission. You do not have to reinitialize the router after adding a user.

Example:

```
add user John
Enter password:
Enter password again:
Enter permission (A)dmin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password

Specifies the access password for the user. Limited to 80 alphanumeric characters and is case-sensitive.

Enter password again

Confirms the access password for the user.

Enter permission

Specifies the permission level for the user: A, O, or M (see Table 8).

v25-bis-address

Adds the local and remote numbers of the V.25bis end-points that communicate with the router. The network *address-name* can be anything, such as a description of the port. You can use any string of up to 23 printable ASCII characters. The *network-dial-address* is the telephone number of the local or destination port. For more information, see “Chapter 36. Using the V.25bis Network Interface” on page 499.

Note: You can use punctuation, such as parentheses and dashes, but the punctuation is not significant (the router uses only the numbers).

```
Example: add v25-bis-address
 remote-site baltimore 1-909-555-0983
```

Boot

Use the **boot** command to enter the Boot CONFIG command environment. For Boot CONFIG information, see “Chapter 5. Using BOOT Config to Perform Change Management” on page 41.

Syntax:

boot

Change

Use the **change** command to modify an interface in the configuration, change your own password, or change user information.

Syntax:

change

- device . . .
- password
- ppp_user . . .
- tunnel-profile

device *device_type*

With the **change device** command you can:

- Change the slot of an existing interface. (Change slot x in interface record n to y where slot y is unoccupied.)
- Change the port of an existing interface. (Change port x in interface record n to y where port y is unoccupied.)
- Swap slots of two existing interfaces. (Swap slot x and slot y in interface records with x or y.)
- Swap ports of two existing interfaces. (Swap port u and slot x in one interface record with port v and slot y in another interface record of the same hardware type.)
- Replace the slot in an existing interface with the slot in another. (Interface configuration for slot x will become interface configuration for slot y. Interface records for slot y will be deleted.)
- Replace the port of one existing interface with the port of another. (Interface configuration for slot x port u will become interface configuration for slot y port v. The interface record for slot y port v will be deleted.)

When the target slot is occupied:

1. If you select the “swap” option, the source and target slots are swapped in all the interface records in which they appear.
2. If you select the “replace” option is selected, the interface configuration for slot x will become the interface configuration for slot y. Interface records for slot y will be deleted.

When the target port is occupied:

1. If you select the “swap” option, the source and target ports can be swapped in their respective interface records if their hardware types in these interface records are identical. For example, 1-port ISDN T1/J1.
2. If you select the “replace” option, the interface configuration for slot x port u becomes the interface configuration for slot y port v. The interface record for slot y port v is deleted.

Example - Change slot 5 on interface 0 to unoccupied slot 7:

```
Config>li dev
Ifc 0     WAN PPP
Ifc 1     WAN PPP
Ifc 2     WAN PPP
Ifc 3     WAN PPP
Ifc 4     1-port IBM Token Ring             Slot: 5   Port: 1
Ifc 5     2-port IBM Token Ring             Slot: 1   Port: 1
Ifc 6     2-port IBM Token Ring             Slot: 1   Port: 2
Ifc 7     2-port IBM Token Ring             Slot: 2   Port: 1
Ifc 8     2-port IBM Token Ring             Slot: 2   Port: 2
Ifc 9     2-port 10/100 Ethernet            Slot: 3   Port: 1
Ifc 10    2-port 10/100 Ethernet            Slot: 3   Port: 2
Ifc 11    ISDN Basic                        Slot: 4   Port: 1

Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 6)[1]? 5
Change all ports on slot # 5 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8)  [1]? 4

Changed slot 5 to slot 4 in 1 intf (port) record...
Config>li dev
Ifc 0     WAN PPP
Ifc 1     WAN PPP
Ifc 2     WAN PPP
Ifc 3     WAN PPP
Ifc 4     1-port IBM Token Ring             Slot: 4   Port: 1
Ifc 5     2-port IBM Token Ring             Slot: 1   Port: 1
Ifc 6     2-port IBM Token Ring             Slot: 1   Port: 2
Ifc 7     2-port IBM Token Ring             Slot: 2   Port: 1
Ifc 8     2-port IBM Token Ring             Slot: 2   Port: 2
Ifc 9     2-port 10/100 Ethernet            Slot: 3   Port: 1
Ifc 10    2-port 10/100 Ethernet            Slot: 3   Port: 2
Ifc 11    ISDN Basic                        Slot: 5   Port: 1
```

password

Modifies the password of the user who is now logged in.

Note: To change a user password, you must have administrative permission.

Example:

```
change password
Enter current password:
Enter new password:
Enter new password again:
```

Enter current password
Specifies your current password.

Enter new password
Specifies your new password.

Enter new password again
Specifies your new password again for confirmation. If your confirmation does not match the previous new password, the old password remains in effect.

ppp_user

Changes the information for a specific PPP user.

Syntax:

change ppp_user encryption-key
parameters
password

encryption-key

Changes the encryption key for a PPP user. The following example shows the dialog for changing an encryption key.

Example - Change Encryption key:

```
Config>change ppp_user encryption-key
Enter user name:  []? leslie
Enable encryption for this user/port (y/n) [No]:y
Encryption key should be 16 characters long.
Encryption Key (16 characters ) in Hex(0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex(0-9, a-f, A-F):
User 'leslie' has been updated
Config>
```

parameters

Changes all of the ppp-user options for a user. This parameter works similar to the **add ppp_user** except that the values shown within the [ ] are the current values and the change command does not verify the changes or list them back to you when you are done. See “Add” on page 76 for details about the **add ppp_user** command.

password

Changes the password for the PPP user.

Example - Change password:

```
Config>change ppp_user password
Enter user name:  []? sam
Password:
Enter password again:
User 'sam' has been updated
Config>
```

user Modifies the user information that was previously configured with the **add user** command.

Note: To change a user, you must have administrative permission.

Example:

```
change user
User name: []
Change password? (Yes or No)
Change permission? (Yes or [No])
```

tunnel-profile

Changes the configuration for a tunnel peer.

```
Config>change tunnel-profile
Enter name:  []? lac.org
Enter hostname to use when connecting to this peer: [lns.org]?
set shared secret? (Yes, No): [No]
Tunnel-Server endpoint address: [11.0.0.1]? 11.0.0.2

profile 'lac.org' has been updated
Config>
```

Clear

Use the **clear** command to delete the router's configuration information from nonvolatile configuration memory.

Attention: Use this command only after calling your service representative.

Syntax:

clear

- all
- ap2 (AppleTalk 2)
- arp (ARP)
- asrt (Adaptive Source Route Protocol)
- appn (Advanced Peer-to-Peer Networking)
- auth (Authentication)
- bgp (Border Gateway Protocol)
- boot
- brly
- brs (Bandwidth Reservation)
- callback
- cmprs (Data Compression)
- dls (Data Link Switching)
- device
- dialer-circuit
- dial-out
- dn (DECnet)
- els (Event Logging System Information)
- fr (Frame Relay)
- gsmp (OSI)
- hdlc
- hostname
- ip (IP)
- ip-security
- ipv6
- ipx (Novell IPX)
- isdn
- l2tp
- lnm
- mcf
- named-profiles
- nat

ndp6
ndr
osi (OSI)
ospf (OSPF routing protocol)
ppp (Point-to-Point)
prompt
rip6
rsvp
sdlc
snmp
srly (SDLC Relay)
tcp/ip-host
time (Time of day information)
tsf (Thin Server)
user
v25bis
v34
vines (Banyan VINES)
wrs (WAN Restoral feature)
x25
xtp

To clear a process from nonvolatile configuration memory, enter the **clear** command and the process name. To clear all information from configuration memory, except for device information, use the **clear all** command. To clear all information, including the device information, use the **clear all** command and then the **clear device** command.

The **clear user** command clears all user information except the router console login information. This is left as enabled (if it was configured as enabled) even though the default value is “disabled”.

Notes:

1. To clear user information, you must have administrative permission.
2. There may be other items in the list, depending upon what is included in the software load.

Example: `clear els`

```
You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):
```

Note: The previous message appears for any parameter configuration you are deleting.

Delete

Use the **delete** command to remove an interface or range of interfaces from the list of devices stored in the configuration, or to remove a user. To use the **delete** command, you must have administrative permission.

Syntax:

delete interface . . .
dump-files
isdn-address
ppp_user . . .
tunnel
user . . .
v25-bis-address

dump-files
Deletes all of the system dump files from the hard file.

Note: If you enter this command and a hard file is not available, you will receive a message indicating that the drive is unavailable.

Example:

```
Config> delete dump-files
Number of existing dump files: 3
Are you sure you want to delete the dump files ? (Yes, No): [No] Yes
Dump files deleted.
```

Note: If the dump target is set to *Network*, only small dump summary files will exist on the local disk. The full dump files are sent to a remote host. If this is the case, this command will delete only the local dump summary files, not the full dump files on the remote host.

interface [*intfc#* **or** *intfc#range***]**
To delete an interface, enter the interface or network number as part of the command. (Only devices that were added with the **add device** command can be deleted.) To obtain the interface number that the router assigns, use the **list device** command.

The delete interface command deletes the device configuration and any protocol information for that interface. However, the router will continue to run the previous configuration until it is reloaded.

If deleting a base ISDN interface , all virtual interfaces running on that base net will also be deleted. So, any dial circuits configured on a base ISDN interface will be removed when the ISDN interface is deleted.

To delete a range of interfaces, specify the first and last interface in the range separated by a hyphen, as shown in the following example:

```
delete interface 13-21
```

You can also enter an interface number or range of interface numbers, when prompted.

isdn-address *address-name*
Removes a previously added ISDN address.

Note: If the *address-name* contains spaces (for example, **remote site XYZ**), you cannot enter the command on one line. Type `delete isdn-address` and press **Return**. Then enter the name when prompted.

ppp_user *user_name*
Deletes a user from the PPP user data base.

tunnel-profile
Deletes a tunnel from the tunnel profile database.

user *user_name*
Removes user access to the router for the specified user.

v25-bis-address *address-name*
Removes a previously added V25bis address.

Note: If the *address-name* contains spaces (for example, **remote site Baltimore**), you cannot enter the command on one line. Type `delete v25-bis-address` and press **Return**. Then enter the name when prompted.

Disable

Use the **disable** command to prevent being prompted for a login from a remote console

You can also use the disable command to disable an interface, memory dumping, or rebooting when a serious error occurs.

Syntax:

disable console-login
interface . . .
dump-memory . . .
reboot-system . . .

console-login
Disables the user from being prompted for a user ID and password on the physical console. The default is disabled.

interface *interface#*
Causes the specified interface to be disabled after issuing the **reload** command. The default is enabled.

dump-memory
Disables the dumping of system memory to the installed hard disk when a serious error occurs.

reboot-system
Disables the rebooting of the system when a serious error occurs. This may be desirable if the network service personnel wish to troubleshoot the error on-line. System rebooting cannot be disabled unless memory dumping is also disabled. If you attempt to disable system rebooting while memory dumping is enabled, system rebooting is aborted and the following message is displayed:

```
System reboot not disabled:  memory dumping must be disabled first
```

Enable

Use the **enable** command to allow login from a remote console,

Syntax:

enable
- console-login
- interface . . .
- dump-memory . . .
- reboot-system . . .

console-login

Enables the user to be prompted for a user ID and password on the physical console. This is useful for security situations. If you do not configure any administrative users and you enable this feature, the following message appears:

```
Warning: Console login is disabled until an
administrative user is added.
```

Attention: Before enabling console login, save the configuration with console login disabled. If login authentication is set to a remote server using Radius or Tacacs+ and the router is unable to reach the authentication server, then access to the router is denied. By disabling the console login, a lock-out situation is prevented.

interface *interface#*

Causes the interface to be enabled after issuing the **reload** command.

dump-memory

Enables the dumping of system memory to the target device specified by the **set dump target** command (described at on page 102) if a serious error occurs. This may be desirable so that the state of the unit at the time of the error can be preserved for troubleshooting later. The dump memory function cannot be enabled unless system rebooting is enabled. If you attempt to enable the dump memory function while system rebooting is disabled, the dump memory function is not enabled and the following message is displayed:

```
System memory dump function not enabled:  rebooting must be enabled first
```

If you configured system dumping to save the first 3 dump files and 3 dump files already exist, the system displays the following message when you enable dump memory:

```
*** System dump cannot be enabled until the    ***
*** existing dump files are deleted.           ***
```

Note: If the dump target is set to *Network*, only small dump summary files will exist on the local disk. The full dump files are sent to a remote host.

See the **set dump enable-mode**, **set dump save-mode**, and **set dump target** commands.

Example:

```
Config> enable dump

Current System Dump Status:
```

```
   System dump is currently disabled.
   Number of existing dump files:  0

Enable system memory dumping? [No]: Yes

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  0
```

Note: If you enter this command and the dump target is set to local hard disk but a hard file is not available, you will receive a message indicating that the drive is unavailable.

reboot-system
Enables the rebooting of the system when a serious error occurs.

Event

Use the **event** command to enter the Event Logging System (ELS) environment so that you can define the messages that will appear on the console. Refer to "Chapter 12. Using the Event Logging System (ELS)" on page 129 for information about ELS.

Syntax:

event

Feature

Use the **feature** command to access configuration commands for specific router features outside of the protocol and network interface configuration processes.

Syntax:

feature [*feature#* or *feature-short-name*]

All 2212 features have commands that are executed by:

- Accessing the configuration process to initially configure and enable the feature, as well as perform later configuration changes.
- Accessing the console process to monitor information about each feature, or make temporary configuration changes.

The procedure for accessing these processes is the same for all features. The following information describes the procedure.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access a feature's configuration prompt, enter the **feature** command followed by the feature number or short name. Table 9 lists available feature numbers and names.

Table 9. IBM 2212 Feature Numbers and Names

Feature Number	Feature Short Name	Accesses the following feature configuration process
0	WRS	WAN Restoral/Reroute
1	BRS	Bandwidth Reservation

Table 9. IBM 2212 Feature Numbers and Names (continued)

Feature Number	Feature Short Name	Accesses the following feature configuration process
2	MCF	MAC Filtering
4	VCRM	Virtual Circuit and Resource Management
7	CMPRS	Data Compression
8	NDR	Network Dispatcher
9	DIALs	Dial-In-Access to LANs
10	AUTH	Authentication
11	IPSec	IP Security feature user configuration
12	LAYER	Layer 2 Tunneling Protocol
13	NAT	Network Address Translator user configuration
14	TSF	Thin Server Function

Once you access the configuration prompt for a feature, you can begin entering specific configuration commands for the feature. To return to the CONFIG prompt, enter the **exit** command at the feature's configuration prompt.

List

Use the **list** command to display configuration information for all network interfaces, or configuration information for the router.

Syntax:

list configuration
devices
isdn-address
patches . . .
ppp_users . . .
tunnel-profile
users . . .
v25-bis-address
vpd

devices [*device* **or** *devicerange***]**

Displays the relationship between an interface number and the hardware interface. You can also use this command to check that a device was added correctly issuing the **add** command.

You can also specify a range of devices to list as shown in the following example:

```
Ifc 2     WAN PPP
Ifc 3     WAN PPP
Ifc 4     1-port IBM Token Ring              Slot: 5   Port: 1
Ifc 5     2-port IBM Token Ring              Slot: 1   Port: 1
```

Note: If you do not specify an interface number or a range of interfaces, all interfaces are displayed.

Example: list devices

```
Ifc 0 Token Ring                    Slot: 1  Port: 1
Ifc 1 Token Ring                    Slot: 1  Port: 2
Ifc 2 Token Ring                    Slot: 2  Port: 1
Ifc 3 Token Ring                    Slot: 2  Port: 2
Ifc 4 Ethernet                      Slot: 4  Port: 1
Ifc 5 Ethernet                      Slot: 4  Port: 2
Ifc 6 Ethernet                      Slot: 5  Port: 1
Ifc 7 Ethernet                      Slot: 5  Port: 2
Ifc 8 Ethernet                      Slot: 6  Port: 1
Ifc 9 Ethernet                      Slot: 6  Port: 2
Ifc 10 V.35/V.36 Frame Relay        Slot: 8  Port: 0
Ifc 11 V.35/V.36 X.25               Slot: 8  Port: 1
Ifc 12 V.35/V.36 PPP                Slot: 8  Port: 2
Ifc 13 V.35/V.36 PPP                Slot: 8  Port: 3
Ifc 14 V.35/V.36 PPP                Slot: 8  Port: 4
Ifc 15 V.35/V.36 PPP                Slot: 8  Port: 5
```

Note: The number of receive buffers noted are exceptions from the receive buffer defaults. The **set receive buffers** command is discussed under “Set” on page 100.

configuration

Displays configuration information about the router.

Example: list configuration

```
Config>list config
Hostname: [none]
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Number of spare interfaces: 0
Console inactivity timer (minutes): 0
Physical console login: disabled
System rebooting on error: disabled
System memory dump enable-mode:
   Disable System Dump following the next system dump.
System memory dump save-mode:
   Save the last 3 (most recent) compressed dump files.
System memory dumping: disabled
Contact person for this node: [none]
Location of this node: [none]

Configurable Protocols:
Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
4   DN    DNA Phase IV
6   VIN   Banyan Vines
7   IPX   NetWare IPX
8   OSI   ISO CLNP/ESIS/ISIS
9   DVM   Distance Vector Multicast Routing Protocol
10  BGP   Border Gateway Protocol
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
13  IPV6  IPV6
20  SDLC  SDLC/HDLC-Relay
22  AP2   AppleTalk Phase 2
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
24  HST   TCP/IP Host Services
25  LNM   LAN Network Manager
26  DLS   Data Link Switching
27  XTP   X.25 Transport Protocol
31  RSVP  Resource reSerVation Protocol
33  PIM6  Protocol Independant Multicast for IP6
35  NDP6  NDP6 for IPV6
36  RIP6  RIP6 for IPV6
38  BRLY  Bisync Relay

Configurable Features:
Num Name  Feature
0   WRS   WAN Restoral
1   BRS   Bandwidth Reservation
2   MCF   MAC Filtering
4   VCRM  VC & Resource Management
7   CMPRS Data Compression Subsystem
8   NDR   Network Dispatching Router
9   DIALs Dial-in Access to LANs
10  AUTH  Authentication
11  IPSec IPSecurity
12  L2TP  Layer-2-Tunneling
13  NAT   Network Address Translation
```

isdn-address

Displays the current ISDN address configurations.

```
Example: list isdn-address
Address assigned name     Network Address     Network Subdial Address
---------------------     ---------------     -----------------------
remote site XYZ            1 2345 67           98765
```

patches

Displays the values of patch variables that have been entered using the **patch** command.

Example:

```
list patches
Patched variable             Value

ping-size                    60
ping-ttl                     59
ip-default-ttl               60
ethernet-security            3
rip-static-suppress          3
```

ppp_users

Lists specific PPP user profile parameters.

Example: List of PPP users when DIALs is not in the software load

```
Config> list ppp_users
List (Name, Verb, User, Addr, Encr):

       PPP User Name: joe
     User IP Address: Interface Default
          Encryption: Not Enabled
```

Example: List of PPP users when DIALs is in the software load

```
Config> list ppp_users
List (Name, Verb, User, Addr, Call, Time, Dial, Encr):

       PPP User Name: joe
     User IP Address: Interface Default
      Net-Route Mask: 255.255.255.255
            Hostname: <undefined>
       Time-Allotted: Box Default
      Call-Back Type: Not Enabled
            Dial-Out: Not Enabled
          Encryption: Not Enabled
```

When you enter **list ppp_users**, the software will prompt you to enter one of the following:

Name List all of the names in the database.

Verb List verbose information about each user. List all information pertaining to each user profile.

User List verbose information about a single user.

Addr (address)
List IP address information for each user, including IP Address, net mask and hostname.

Call (callback)
List callback information for each user, including the type of callback and number.

Time List time allowed configured for each user.

Encr (encryption)
List whether encryption is enabled for each user.

tunnel-profile

Displays the tunnel-profile parameters.

Example:

```
Config>list tunnel-profile

Endpoint Tunnel name Hostname
11.0.0.192 lac lns

1 TUNNEL record displayed.

Config>
```

Tunnel Name
Specifies the configured name for the peer.

Server Endpoint
The IP address of the peer.

Type Specifies the type of peer connection.

Medium
Specifies the protocol that the tunnel is using.

Local Host Name
Specifies the name configured for use when connecting to the peer.

users Displays the users configured to access the system.

Example:

```
list users
USER           PERMISSION
joe            operations
mary           administrative
peter          monitor
```

v25-bis-address
Displays the current V25bis address configurations. The V25bis address configuration consists of the network address and network address name for a local port (serial line interface) or destination port. The network address is the telephone number of the local or destination port. The network address name can be anything, such as the description of the port. See “Chapter 36. Using the V.25bis Network Interface” on page 499 for more information.

```
Example:
list v25-bis-address
Address assigned name            Network Address
---------------------            ---------------
v25-1                            8982800
v25-2                            8980001
delaware                         1-666-555-4444
```

vpd Displays the hardware and software vital product data.

Load

Use the **load** command to list packages in the software load that are available but not configured, or packages that are configured in the software load. The **load** command is also used to add or delete a software package.

Syntax:

load	add package *packagename*
	delete package *packagename*
	list . . .

The software is divided into multiple load modules. These load modules are grouped into software packages. Some of these software packages are optional because, although they are shipped with the product, they are not automatically loaded.

Software packages containing encryption are available from the 2212 Web server accessible using the Internet.

To load and run optional software packages:

1. Add the package using the **load add** command.
2. Reboot. This action loads the optional software into the device's memory.
3. Configure the optional software.
4. Save the configuration.
5. Reboot the device. This action enables the software with the new configuration.

add package *packagename*
: Adds a software package to the software. The *packagename* is the name of the package of load modules you want to include in the software.

  Example: load add package appn

delete package *packagename*
: Removes a software package from the software. The *packagename* is the name of the package of load modules you want to remove from the software.

  Example: load delete package appn

list
: Lists either the packages in the software load that are available but not configured, or the packages that are configured in the software load. You can specify one of the following:

  available
  : Lists the software packages in the current software load that are not configured.

  configured
  : Lists the software packages in the current software load that are configured.

Network

Use the **network** command to enter the network interface configuration environment for supported networks. Enter the interface or network number as part of the command. (To obtain the interface number, use the CONFIG **list device** command.) The appropriate configuration prompt (for example, `TKR Config>`) will be displayed. See the network interface configuration chapters in this book for complete information on configuring your types of network interfaces.

Syntax:

network *interface#*

Notes:

1. If you change a user-configurable parameter, you must **reload** the router for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).

2. Not all network interfaces are user-configurable. For interfaces that you cannot configure, you receive the message: `That network is not configurable.`

Patch

Use the **patch** command for modifying the router's global configuration. Patch variables are recorded in nonvolatile configuration memory and take effect immediately; you do not have to wait for the next restart of the router. This command should be used only for handling uncommon configurations. Anything that you commonly configure should still be handled by using the specific configuration commands. The following is a list of the current patch variables documented and supported for this release.

Syntax:

patch

- bgp-subnets
- dls-ignore-lfs
- ethernet-security
- filter-nr
- ip-default-ttl
- ip-mtu
- lnm-link-via-tbport
- more-lines
- mosheap-lowmark
- ospf-import-rate
- ping-size
- ping-ttl
- ppp-echo
- relax-jate
- rip-static-suppress

bgp-subnets *new value*
If you want the BGP speaker to advertise subnet routes to its neighbors, set *new value* to 1. The default is 0.

dls-ignore-lfs *new value*
When set to 1, DLSw ignores the "largest frame" size bits in source-routed frames when setting up a circuit. This avoids circuit setup problems with some older LAN products that do not set these bits correctly. The default is 0.

ethernet-security *new value*
When set to a non-zero value, zeros the padding that is applied to Ethernet packets whose data portion is less than the physical minimum of 60 bytes. This may be required for security reasons. Default: 0.

filter-nr
Allows the NetBIOS "Name Recognized" to be filtered along with the current list of NetBIOS frames filtered by bridge code. NetBIOS Name filters will pass all NetBIOS packets that are not one of the following types:

ADD_GROUP_NAME_QUERY, ADD_NAME_QUERY, DATAGRAM, NAME_QUERY. This parameter adds NAME_RECOGNIZED to the list of types.

ip-default-ttl *#_of_packets*
The TTL used in packets that are originated by the router. The default is 64.

Note: It is preferable to set this parameter with the **set ttl** IP configuration command. (See the "Set" section of the "Using and Configuring IP" chapter of *Protocol Configuration and Monitoring Reference Volume 1* .) This patch variable remains for compatibility with configurations from older releases.

ip-mtu *bytes*
This parameter limits the IP MTU size to the specified value. When this parameter is set, the IP MTU size on a given network interface is set to the lesser of the ip-mtu value and the largest value that network interface's configured frame size can accommodate.

lnm-link-via-tbport *new value*
Allows LNM to link to a token-ring over an Ethernet transparent bridge (TB) port.

When set to 1, the LNM link is allowed.

When set to 0, the default, the LNM link is not allowed.

more-lines *#_of_lines*
The number of lines to display on the console when listing the IP routing table, which uses a "more pipe" (¦).

mosheap-lowmark *new value*
This parameter specifies the percentage of free MOS heap memory, at which the device notifies the operator that an out-of-memory error is imminent. This notification allows the operator to take action to free up MOS heap memory before the device receives an error and stops.

When the operator receives notification, the operator can reconfigure the router and then reboot, minimizing the outage to the network. Specifying 0 for this parameter suppresses this warning.

Valid Values: 0 to 100

Default Value: 10

ospf-import-rate *rate*
Number of routes imported per second.

ping-size *bytes*
The size of the data portion (that is, excluding IP and ICMP headers) of the ICMP PING packet that is sent via the IP>**ping** command. Default: 56 bytes. (The size of the PING data can also be entered as a parameter of the **ping** command as described in the "Ping" section of the "Monitoring IP" chapter of *Protocol Configuration and Monitoring Reference Volume 1* .)

ping-ttl *seconds*
The TTL (time-to-live) sent in PINGs by the IP>**ping** command. Default: 64. (The TTL can also be entered as a parameter of the **ping** command as described in the "Ping" section of the "Monitoring IP" chapter of *Protocol Configuration and Monitoring Reference Volume 1*.

ppp-echo *new value*
When set to 1, the device will not send PPP Echo Requests on any PPP

interface. PPP Echo Requests are sent to remote devices as part of PPP maintenance to ensure the remote device is operational. Consider enabling this variable when running PPP on a slow line and using that line to transmit large data packets such that the PPP maintenance packets are not exchanged often enough to keep the PPP interface up.

relax-jate
Relaxes JATE ISDN restriction.

rip-static-suppress *new value*
When set to a non-zero value, static routes will not be advertised by RIP over a given interface unless the `IP config>` **enable send static** command is given for the interface. This changes the semantics of the **enable send static** command. When rip-static-suppress is equal to 0 (the default), the list of the routes advertised via RIP is the union of those specified by the interface's RIP flags.

Note: You must specify the complete name of the patch variable that you want to change. You cannot use an abbreviated syntax for the patch name.

Performance

Use the **performance** command at the `GWCON>` prompt (+) to enter the configuration environment for performance. See "Chapter 14. Configuring and Monitoring Performance" on page 197 for more information.

Protocol

Use the **protocol** command at the `Config>` prompt to enter the configuration environment for the protocol software installed in the router.

Syntax:

protocol [*prot#* or *prot_name*]

The **protocol** command followed by the desired protocol number *or* short name lets you enter a protocol's command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol. To return to `Config>`, enter the **exit** command.

Notes:

1. To see the names and numbers of the protocols in your software load, at the `Config>` prompt, enter **list configuration**.
2. When you change a user-configurable parameter, you must restart the router for the change to take effect. To do so, enter the **restart** command at the OPCON prompt (*).

   The changes you make through CONFIG are kept in a configuration database in nonvolatile memory and are recalled when you restart the router.

Qconfig

Use the **qconfig** command to initiate Quick Config. Quick Config allows you to configure parameters for bridging and routing protocols without entering separate configuration environments.

Syntax:

qconfig

Note: For complete information on using the Quick Config software provided with your router, see “Appendix A. Quick Configuration Reference” on page 571.

Set

Use the **set** command to configure various system-wide parameters.

Syntax:

set
- contact-person . . .
- baud-rate
- data-link . . .
- down-notify . . .
- dump enable-mode
- dump save-mode
- dump target
- global-buffers
- hostname
- inactivity-timer
- input-low-water
- location . . .
- logging level
- packet-size
- prompt-level
- receive-buffers
- spare-interfaces

baud-rate
Specifies the baud-rate of the 2212 service port. The valid values are 2400, 9600, 14400, 19200, 28800, 38400,57600, or 115200 bps.

contact-person *sysContact*
Sets the name or identification of the contact person for this managed SNMP node. There is a limit of 80 characters for the *sysContact* name length.

This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

data-link *type interface#*
Select the data link type for a serial interface or a dial circuit interface. The *type* can be one of:

- BSC
- FRAME-RELAY
- PPP
- SDLC
- SRLY

- V25BIS
- X25

Notes:

1. PPP, SDLC, and Frame Relay are the only data-links supported on dial circuit interfaces. X.25 is supported on ISDN BRI D-channel only.

Note: When you change the data-link type, none of the protocol or feature configuration data associated with the interface is changed. Therefore, you must re-configure any protocol or feature configuration support that is data-link dependent.

Interface# is the number of the interface you are configuring.

down-notify *interface# # of seconds*

Allows the user to specify the number of seconds before declaring an interface as being down. The normal maintenance packet interval is 3 seconds, and it takes four maintenance failures to declare the interface as down.

The **set down-notify** command is used primarily when tunneling LLC traffic over an IP network using OSPF. If an interface goes down, OSPF cannot detect it fast enough because of the length of time that it takes for an interface to be declared down. Therefore, LLC sessions would begin to timeout. You can set the down-notify timer to a lower value, allowing OSPF to sense that an interface is down quicker. This enables an alternate route to be chosen more quickly, which will prevent the LLC sessions from timing out.

Note: If the **set down-notify** command is executed on one end of a serial link, the same command must be performed at the other end of the link or the link may not come up and stay up.

Interface#
The number of the interface you are configuring.

# of seconds
The down notification time value that specifies the maximum time that will elapse before a down interface is marked as such. Large values will cause the router to ignore transient connection problems, and smaller values will cause the router to react more quickly. The range of values is 1 to 300 seconds and the default is 0, which sets the 3-second period. Setting the down notification time to 0 will restore the default time for that interface.

The **list devices** command will show the down notification time setting for any interface that has the default value overridden.

dump enable-mode

Specifies whether dumping is enabled following the next system dump. If you configure the save mode (see the **set dump save-mode** command) to save the first three dumps and the system has already created the third dump file, dumping is disabled regardless of your specification. At the time the system creates the third dump file, you will receive the following message:

```
Active Dump Detected.
Dump Compression in Progress, please be patient ...
```

```
*** System dumping is being DISABLED because dumping is ***
*** configured to save the 3 initial dumps, but 3       ***
*** dump files already exist.                           ***
```

Example:

```
Config> set dump enable-mode

Current System Dump Settings:
   Disable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Do you want to change system dump enable-mode to
re-enable System Dump following the next system dump ? (Yes, No): [No] Yes

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  2
```

Default value: disable

Note: Dumping is enabled with the **enable dump-memory** command.

dump save-mode

Specifies whether to save the first three (initial) system dump files or the last three (most recent). See the **dump enable-mode** for a consideration for using recent mode as opposed to initial mode.

Example:

```
Config> set dump save-mode

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Do you want to change system dump save-mode to
save the first (initial) dump files ? (Yes, No): [No] Yes

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the first 3 (initial) dump files, then disable system dump.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  2
```

Default value: recent

dump target

Specifies the location where the system memory image information will be written. Valid targets are the local hard disk, if one is present, or a remote host on a LAN.

If the target is a network, then IP and TFTP parameters of both the local LAN interface and the remote host are required. An additional parameter determines whether the file will be sent by TFTP as compressed or uncompressed data.

Example:

```
Config>set dump target

Current System Dump Target Settings:

   Dump Target:  Local Hard Disk

Do you want to change the System Dump Target ? (Yes, No): [No] Yes
Enter Dump Target (D-Disk or N-Network): [D]? N
```

```
Setting Dump Target to "Network".
Set or Change settings for dumping to the Network ? (Yes, No): [No] Yes
Enter Local LAN Interface Type (E-Eth or T-Tkr): [E]? E
Enter Slot Number (1-2): [1]? 1
Enter Port Number (1-2): [1]? 1
Enter Local IP Address: [9.9.9.6]? 9.9.9.5
Enter Local Netmask: [255.255.255.0]?
Enter Remote IP Address: [9.9.9.1]? 9.9.9.11
Remote Path and File name:  /tmp/netdump
Enter Path and File name (32 chars max):  /tmp/dump_to_host
Enter File Compression Mode (C-Comp or U-Uncomp): [U]? C
Do you want to save your changes ? (Yes, No): [No] Yes

New System Dump Target Settings:

   Dump Target:  Remote Host on Network
   Local Interface Settings:
     Device Type:  Ethernet
     Slot Number:  1
     Port Number:  1
     IP address:  9.9.9.5
     Net Mask:  255.255.255.0
   Remote Host Settings:
     IP address:  9.9.9.11
     Remote Filename:  /tmp/dump_to_host
     Remote file will be compressed and "0.cmp", "1.cmp", or "2.cmp" will be
     appended to the end of the filename.
```

When the system dump file is sent by TFTP to the remote host, it will be written as multiple files, which must first be concatenated. For example, if the remote file was specified as /tmp/dump_to_host, and remote files are sent as compressed. The files written on the remote workstation are:

- dump_to_host0.cmp
- dump_to_host0.cm1

Depending on the total size of the dump, there may be additional files, named as:

- dump_to_host0.cm2
- dump_to_host0.cm3, and so forth.

In order to decompress and view the dump information, the files must be combined as follows into a single file (note that order is critical):

/tmp> **cat dump_to_host0.cmp dump_to_host0.cm1 dump_to_host0.cm2 dump_to_host0.cm3 > dump_to_host0_cat.cmp**

As a result, the combined file dump_to_host0_cat.cmp will contain a complete system memory dump image.

If the file was sent by TFTP as uncompressed, the file extensions are .unc, .un1, .un2, and .un3 instead of .cmp, .cm1, .cm2, and .cm3. The uncompressed files must also be concatenated to create a complete system memory dump image. For Example:

/tmp>**cat dump_to_host0.unc dump_to_host0.un1 dump_to_host0.un2 dump_to_host0.un3 > dump_to_host0_cat**

Note: The output file, dump_to_host0_cat. does not require a file extension because the file is not compressed.

global-buffers *max#*

Sets the maximum number of global packet buffers, which are the packet buffers used for locally originated packets. The default is to autoconfigure for the maximum number of buffers (up to 1000). To restore the default, set the value to 0. To display the setting for global-buffers, use the **list configuration** command.

hostname *name*

Adds or changes the router name. The router name is for identification only; it does not affect any router addresses. The *name* must be less than 78 characters and is case sensitive.

inactivity-timer *#_of_min*

Changes the setting of the Inactivity Timer. The Inactivity Timer logs out a user if the remote or physical console is inactive for the period of time specified in this command. This command affects only consoles that require login. The default setting of 0 turns the inactivity timer off, indicating that no logoff is performed, no matter how long a console remains inactive.

input-low-water *interface# low_ #_of_receive_buffers*

Allows you to configure the value of the low number of receive buffers, or packets, on a per-interface basis, thus overriding the default values.

The memory allocation strategy changes to conserve buffers when the number of free buffers is equal to or less than the low or low-water mark value. When a packet is received, and the current value of the interface is less than the low water value, then that packet is eligible for flow control (dropping).

The range of values is 1 to 255. The default is both platform and device specific. Setting the value to 0 restores the autoconfigured default.

Interface# is the number of the interface you are configuring. *Low_#_of_receive_buffers* is the low water value.

Lowering the value will make it less likely that packets from this interface will be dropped when sent on congested networks. However, lowering the value may negatively affect performance if it drops packets to the extent that the receive queue is frequently empty. Raising the value has the opposite effect.

Type the **QUEUE** or **BUFFER** command at the GWCON prompt (**+**) to show the low setting.

location *sysLocation*

Sets the physical location of an SNMP node. There is a limit of 80 characters for the *sysLocation* name length. This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

logging level *#*

Controls the output of messages that have not yet been converted to the ELS. (Refer to for more information about the ELS.) The logging level is recorded in the configuration. When the router is powered on or restarted, the logging level takes effect and determines message output. The default logging level is 76. Logging level 0 equates to no logging level.

```
Example: set logging level 76
```

packet-size *max_packet_size_in_bytes*

Establishes or changes the maximum size for global buffers and receive buffers. If you specify a value of 0 as the maximum packet size, the size of receive buffers for an interface is based on that interface's configured packet size and the packet size of global buffers are autoconfigured. If you specify a non-zero value, the configured value is used as the global buffer packet size and any interfaces that have a configured packet size that is larger than the maximum packet size will use the maximum packet size for their receive buffers. A value of 0 (for autoconfigure) is the default.

Attention: Use this command only under direct instructions from your service representative. ***Never*** use it to reduce packet size – ***only*** to increase it.

prompt-level *user-defined-name*

Adds a user-defined name as a prefix to all operator prompts, replacing the hostname.

The user-defined-name can be any combination of characters, numbers, and spaces up to 80 characters. Special characters may be used to request additional functions as described in Table 10.

Example:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

Table 10. Additional Functions Provided by the Set Prompt Level Command

Special Characters	Function Provided by the Set Prompt Level Command

$n	Displays the hostname. This is useful when you want the hostname included in the prompt. For example:
	`Config> set prompt`
	`What is the new MOS prompt [y]? $n`
	`hostname:: Config>`

$t	Displays the time. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $t`
	`02:51:08[GMT-300] Config>`

$d	Displays the current date-month-year. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $d`
	`26-Feb-1997 Config>`

$v	Displays the software VPD information in the following format: `program-product-name Feature xxxx Vx Rx.x PTFx RPQx`
$e	Erases one character *after* this combination within the user-defined prompt.
$h	Erases one character *before* this combination within the user-defined prompt.
$_	Adds a carriage return to the user-defined prompt.
$$	Displays the $.

Note: You can combine these commands. For example:
`Config> set prompt`
`What is the new MOS prompt [y]? $n::$d`
`hostname::26-Feb-1997 Config>`	

receive-buffers *interface# max#*

Adjusts the number of private receive buffers for most interfaces.

The range is 5 to 1000.

Note: This command is not applicable for ISDN Primary Rate Interfaces . For ISDN PRI, the number of receive buffers is fixed at 5 per

B-channel, 115 for T1 and 150 for E1. When in channelized mode, the PRI gets 5 receive buffers per configured timeslot.

(On some devices, the maximum value is restricted further, as shown in Table 11.) To restore the default, set the value to 0. The **set receive-buffers** command can be used to increase the receive performance of an interface. In addition, this command can be used to reduce flow control drops when the router is forwarding many packets from a fast interface to a slow interface. The effect of this command is visible on the GWCON **buffer** command.

Attention: Use the **set receive-buffer**command only under direct instructions from your service representative.

Table 11. Default and Maximum Settings for Interfaces

Interface	Default	Maximum
10 Mbps Ethernet	40	1000
10/100 Mbps Ethernet	64	1000
Serial	24	24
TKR	40	1000

spare-interfaces *n*

Defines ***n***, the number of spare interfaces, for this device. See “Configuring Spare Interfaces” on page 68 for additional information.

System Retrieve

Use the **system retrieve** command to retrieve one or more memory image files from the installed hard file after a serious error has occurred. If dumping is configured to dump to a remote host on the network, only the summary headers will be retrieved.

Syntax:

system retrieve

Uses TFTP to send selected memory image files to a remote host. The system will prompt you for the remote host’s IP address and file names.

If there are no dump files, you will receive the following message:

```
No dump files exist to retrieve
```

Example:

```
Config>system retrieve

Current System Dump Settings:

   Dump Target:  Local Hard Disk

   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Number of existing dump files:  1

Do you want to see a summary of the dump files ? (Yes, No): [No] Yes
-----------------------------------------------------
Filename: core0.cmp

Dump Date:  Mon Jul 27 10:20:03 1998

Fatal messages:
```

```
  Data St. Excp Reading 0x40000000 at 0x123d0  in thread MOSDBG (0x1b1cb8)
  STACK:0x123D0< 0x123C8< 0x1155C< 0x306C44EC< 0x306BE888< 0x3050ABC0< 0x2DB48

CMVC Build:  cc_157a
Builder:  build
Build Name:  LML.ld
Retain Name:   AIS.EH1
Product Number:  2212-AIS
Build Date:  Mon Jul 27 14:07:09 1998

-----------------------------------------------------

Destination IP address [0.0.0.0]? 9.9.9.1

Filename: core0.cmp
Dump Date:  Mon Jul 27 10:20:03 1998

Do you want to retrieve this file ? (Yes, No): [No] Yes
Fully qualified destination path/file name [/tmp/dump0.cmp]? /tmp/dump_from_disk0.cmp
The memory image file is 11.7 Mb long.

Proceed? [No]: Yes
Sending memory image file by tftp
TFTP transfer of /hd0/core0.cmp complete, size=11734001 status: OK
tftp transfer completed successfully.
```

System View

Use the **system view** command to display the current system dump settings and the status of the system dumps, including how many dump files exist. You can also display a summary of the dump files.

Syntax:

system view

Example:

```
Config>system view

Current System Dump Settings:

   Dump Target:  Remote Host on Network
   Local Interface Settings:
     Device Type:  Ethernet
     Slot Number:  1
     Port Number:  1
     IP address:  9.9.9.6
     Net Mask:  255.255.255.0
   Remote Host Settings:
     IP address:  9.9.9.1
     Remote Filename:  /tmp/netdump
     Remote file will be uncompressed and "0.unc", "1.unc", or "2.unc" will be
     appended to the end of the filename.

   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  1


Do you want to see a summary of the dump files ? (Yes, No): [No] Yes
-----------------------------------------------------
Filename: core0.cmp
```

```
Dump Date:  Mon Jul 27 10:20:03 1998

Fatal messages:
  Data St. Excp Reading 0x40000000 at 0x123d0  in thread MOSDBG (0x1b1cb8)
  STACK:0x123D0< 0x123C8< 0x1155C< 0x306C44EC< 0x306BE888< 0x3050ABC0< 0x2DB48

CMVC Build:  cc_157a
Builder:  build
Build Name:  LML.ld
Retain Name:  AIS.EH1
Product Number:  2212-AIS
Build Date:  Mon Jul 27 14:07:09 1998

-----------------------------------------------------
```

Time

Use the **time** command to set the 2212 system clock and date, and to display the values on the user console. These values can then be used to time-stamp ELS messages.

Note: The 2212 has a hardware clock that maintains the date and time after router reinitialization.

Syntax:

time host . . .
list
offset
set . . .
sync . . .

host *IP_address*
Sets the IP address of the RFC 868-compliant host that will be used as the time source. This is the address of a host which will respond to an empty datagram on UDP port 37 with a datagram containing the current time.

list Displays all configured time-related parameters. This includes the current time (if set) and the source of the time (operator or IP address from which time was last received).

```
Example: time list
05:20:27  Wednesday December 7, 1994
Set by: operator
Time Host:  131.210.4.1
Sync Interval: 10 seconds GMT
Offset:  -300 minutes
```

offset *minutes*
Defines the time zone, in minutes, offset from GMT (Greenwich Mean Time). Note that values west of GMT are negative. For example, EST is 5 hours earlier than GMT, so the command would be **time offset -300**.

Valid values: -720 to 720

Default value: 0

set <*year month date hour minute second***>**
Prompts you to set the current time. If you do not specify the entire time in

the command, you are prompted for the remaining values. You can change the date as shown in the following example.

```
Example: time set
year [1996] 1997
month [12]?
date [6]? 7
hour [11]? 12
minute [3]?
second [2]?
```

sync *seconds*

Sets the period, in seconds, at which the router will poll the time host for the current time.

Unpatch

Use the **unpatch** command to restore the values of the patch variables entered with the **patch** command to their default values. See the **patch** command in “Patch” on page 97 for details.

Syntax:

unpatch *variable_name*

Note: You ***must*** specify the long name of the patch variable to be restored.

Update

Use the **update** command to update the configuration memory when you receive a new software load.

Syntax:

update version-of-SRAM

Follow the instructions on the release notice sent with the software. The **update** command is the last command that you enter when loading new software. After you enter this command, the console displays a message indicating configuration memory is being updated.

Write

Use the **write** command to save a configuration to the device before reloading.

Syntax:

write

If you fail to issue the write command and try to reload the device, you will be asked if you want to save the configuration. The configuration is saved in the next CONFIG on the hard disk in the bank you are currently using.

Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands

This chapter describes the GWCON process and includes the following sections:

- "What is GWCON?"
- "Entering and Exiting GWCON"
- "GWCON Commands"

What is GWCON?

The Gateway Console (monitoring) process, GWCON (also referred to as CGWCON), is a second-level process of the router user interface.

Using GWCON commands, you can:

- List the protocols and interfaces currently configured in the router.
- Display memory and network statistics.
- Set current Event Logging System (ELS) parameters.
- Test a specified network interface.
- Communicate with third-level processes, including protocol environments.
- Enable and disable interfaces.

The GWCON command interface is made up of levels called modes. Each mode has its own prompt. For example, the prompt for the IP protocol is `IP>`.

If you want to know the process and mode you are communicating with, press **Return** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access the various modes in GWCON.

Entering and Exiting GWCON

To enter the GWCON command environment from OPCON and obtain the GWCON prompt enter the **talk 5**

```
* talk 5
```

The console displays the GWCON prompt (+). If the prompt does not appear, press **Return**. Now, you can enter GWCON commands.

To return to OPCON, enter the OPCON intercept character. (The default is **Ctrl-P**.)

GWCON Commands

This section contains the GWCON commands. Each command includes a description, syntax requirements, and an example. The GWCON commands are summarized in Table 12 on page 112.

To use the GWCON commands, access the GWCON process by entering **talk 5** and enter the GWCON commands at the (+) prompt.

Table 12. GWCON Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Activate	Enables a newly configured spare interface.
Buffer	Displays information about packet buffers assigned to each interface.
Clear	Clears network statistics.
Configuration	Lists status of the current protocols and interfaces.
Disable	Takes the specified interface or slot off line.
Enable	Enables all interfaces of an adapter.
Error	Displays error counts.
Event	Enters the Event Logging System environment.
Feature	Provides access to console commands for independent router features outside the usual protocol and network interface console processes.
Interface	Displays network hardware statistics or statistics for the specified interface.
Memory	Displays memory, buffer, and packet data.
Network	Enters the console environment of the specified network.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Queue	Displays buffer statistics for a specified interface.
Reset	Disables the specified interface and then re-enables it using new interface, protocol and feature configuration parameters.
Statistics	Displays statistics for a specified interface.
Test	Enables a disabled interface or tests the specified interface.
Uptime	Displays time statistics for the router.

Activate

Use the **activate** command to enable a spare interface on this device. See “Configuring Spare Interfaces” on page 68 for more information.

Syntax:

activate *interface#*

Buffer

Use the **buffer** command to display information about packet buffers assigned to each interface or range of interfaces.

Note: Each buffer on a device is the same size and is dynamically built. Buffers vary in size from one device to another.

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

buffer [*network#* or *range_of_network#*]

To display information about multiple interfaces, specify the range_of_network# (or a combination of *network#* and *range_of_network#*). For example, specifying **`buffer 0 3 25-50`** displays the information for nets 0, 3, and 25 through 50.

Example:

```
+buffer
                    Input Buffers        Buffer sizes                    Bytes
Net   Interface     Req Alloc Low Curr   Hdr  Wrap  Data Trail Total    Alloc
0     PPP/0          24    24   4   24    87    92  2044    17  2240    53760
1     PPP/1          24    24   4   24    87    92  2044    17  2240    53760
2     PPP/2          24    24   4   24    87    92  2044    17  2240    53760
3     PPP/3          24    24   4   24    87    92  2044    17  2240    53760
4     TKR/0          40    40   7   40    85    92 18144     7 18328   733120
5     TKR/1          40    40   7    0    85    92  2052     7  2236    89440
6     TKR/2          40    40   7    0    85    92  2052     7  2236    89440
7     TKR/3          40    40   7   40    85    92 18144     7 18328   733120
8     TKR/4          40    40   7   40    85    92 18144     7 18328   733120
9     Eth/0          64    64  10   64    84    92  1500     4  1680   107520
10    Eth/1          64    64  10    0    84    92  1500     4  1680   107520
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Buffers:

Req Number of buffers requested.

Alloc Number of buffers allocated.

Low Low water mark (flow control).

Curr Current number of buffers on this device. The value will be 0 if the device is disabled. When a packet is received, if the value of *Curr* is below *Low*, then the packet is eligible for flow control. (See the **queue** command for conditions.)

Buffer Sizes:

Hdr Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Data Maximum data link layer packet size.

Trail Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer.

Bytes Alloc
Amount of buffer memory for this device. This value is determined by multiplying the values of *Alloc x Total*.

Clear

Use the **clear** command to delete statistical information about one or all of the router's network interfaces. This command is useful when tracking changes in large counters. Using this command does not save space or speed up the router.

Enter the interface (or net) number as part of the command. To get the interface number, use the GWCON **configuration** command.

Syntax:

clear *interface#* or *range_of_interface#*

GWCON Process

To clear information about multiple interfaces, specify the range_of_network# (or a combination of *interface#* and *range_of_interface#*). For example, specifying **clear 0 3 25-50** clears the information for nets 0, 3, and 25 through 50.

Configuration

Use the **configuration** command to display information about the protocols and network interfaces. The output is displayed in three sections, the first section lists the router identification, software version, boot ROM version, and the state of the auto-boot switch. The second and third sections list the protocol and interface information.

Syntax:

configuration

To display information about multiple interfaces, specify the range_of_network# (or a combination of *network#* and *range_of_network#*). For example, specifying **configuration 0 3 25-50** displays the information for nets 0, 3, and 25 through 50.

Example:

configuration

```
Access Integration Services
2212-AIS Feature 3763 V3.2 Mod 0 PTF 0 RPQ 0 AIS.EH5   cc_156c
Num Name  Protocol
3   ARP    Address Resolution
7   IPX    NetWare IPX
11  SNMP   Simple Network Management Protocol
23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
24  HST    TCP/IP Host Services
25  LNM    LAN Network Manager

Num Name  Feature
2   MCF    MAC Filtering
7   CMPRS  Data Compression Subsystem
9   DIALs  Dial-in Access to LANs
10  AUTH   Authentication

11 Total Networks:
Net  Interface   MAC/Data-Link        Hardware                      State
0    PPP/0       Point to Point       SCC Serial Line               Up
1    PPP/1       Point to Point       SCC Serial Line               Down
2    PPP/2       Point to Point       SCC Serial Line               Down
3    PPP/3       Point to Point       SCC Serial Line               Down
4    TKR/0       Token-Ring/802.5     IBM Token Ring                Up
5    TKR/1       Token-Ring/802.5     IBM Token Ring                Not present
6    TKR/2       Token-Ring/802.5     IBM Token Ring                Not present
7    TKR/3       Token-Ring/802.5     IBM Token Ring                Up
8    TKR/4       Token-Ring/802.5     IBM Token Ring                Up
9    Eth/0       Ethernet/IEEE 802.3  10/100 Ethernet               Up
10   Eth/1       Ethernet/IEEE 802.3  10/100 Ethernet               Down
```

- The first line gives the product name.
- The second line lists the program/product number, Feature Number, Version, Release, PTF and RPQ information.
- The remaining lines list the configured protocols, followed by the configured features.

The following information is displayed for protocols:

Num Number that is associated with the protocol.

Name Abbreviated name of the protocol.

Protocol
Full name of the protocol.

The following information is displayed for features:

Num Number associated with the feature.

Name Abbreviated name of the feature.

Feature
Full name of the feature.

The following information is displayed for networks:

Net Network number that the software assigns to the interface. Networks are numbered starting at 0. These numbers correspond to the interface numbers discussed under the CONFIG process.

Interface
Name of the interface and instance of this type of interface.

MAC/Data Link
Type of MAC/Data link configured for the interface.

Hardware
Specific kind of interface by hardware type.

State Current state of the network interface.

Testing
Indicates that the interface is undergoing a self-test. Occurs when the router is first started, when a problem is detected on the interface, or when the **test command** is used. (The **enable slot** command can also be used to initiate a self-test of all interfaces on an adapter.)

When an interface is operational, the interface periodically sends out maintenance packets and/or checks the physical state of the port or line to ensure that the interface is still functioning correctly. If the maintenance fails, the interface is declared down and a self-test is scheduled to run in 5 seconds. If a self-test fails, the interface transitions to the down state and the interval until the next self-test is increased up to a maximum of 2 minutes. If the self-test is successful, the network is declared up.

Up Indicates the interface is operational.

Down Indicates that the interface is not operational and has failed a self-test. The network will periodically transition to the testing state to determine if the interface can become operational again.

Disabled
Indicates that the interface is disabled. An interface can be disabled by the following methods:

- An interface can be configured as disabled using the CONFIG **disable** command. Each time the router is reinitialized, the interface's initial state will be disabled. It will remain in the disabled state until an action is taken to enable it.

- An interface can be disabled using the GWCON **disable** command. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the router is reinitialized.
- The network manager can disable the interface through SNMP. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the router is reinitialized.

When an interface is disabled, it remains disabled until one of the following methods is used to enable it:

- The GWCON **test** command is used to start a self-test of the interface.
- The GWCON **enable slot** command is used to start a self-test on all interfaces on an adapter.
- The network manager initiates a self-test of the interface through SNMP.

WAN Reroute also can change the state of a disabled interface. If an interface is configured as an alternate interface for WAN Reroute and its configured state is disabled, WAN Reroute will start a self-test of the interface when the primary interface goes down. When the primary interface is operational and stable again, WAN Reroute puts the alternate interface back to its configured state. Refer to The WAN Reroute Feature in *Using and Configuring Features* for more information.

Available
Indicates that the interface has been configured as a secondary WAN Restoral interface and it is available to back up the primary interface.

Not Present
Indicates that the interface's adapter is not plugged in.

Not Present is also used as the state for a null device. Spare interfaces are displayed as null devices until they are activated.

HW Mismatch
Indicates that the configured adapter type does not match the adapter type that is actually present in the slot.

HW Failure
Indicates that there is an unrecoverable hardware error for the interface's hardware.

Diagnostics
Indicates that hardware diagnostics are running.

Disable

Use the **disable** command to take a network interface or slot off-line, making the interface or slot unavailable. This command immediately disables the interface or slot. You are not prompted to confirm, and no verification message displays. If you disable an interface or slot with this command, it remains disabled until you use the GWCON **test** command or an OPCON **reload** command to enable it.

Enter the interface, or net number or slot as part of the command. To obtain the interface number or slot number, use the GWCON **configuration** command.

Note: If the interface you are disabling is configured as an alternate WAN Reroute interface, you are asked if you want to disable any WAN Reroute primary/alternate pairings that include this alternate interface. If you answer *yes*, the interface is disabled and is no longer available to backup a primary interface. If you answer *no*, the alternate interface is disabled but WAN Reroute will attempt to bring it up if its corresponding primary interface goes down. You want to disable WAN Reroute on an alternate interface if you are disabling the interface so that you can remove its adapter. See The WAN Reroute Feature, Using WAN Restoral, and Configuring and Monitoring WAN Restoral in the *Using and Configuring Features* for additional information.

Syntax:

disable	interface *interface#*
	slot *slot#*

Enable

Use the **Enable** command to enable all interfaces of an adapter. This performs the same action as the **test** command (See “Test” on page 125) but performs the action for each interface using the adapter in the specified slot.

Syntax:

enable	slot *slot#*

Error

Use the **error** command to display error statistics for the network. This command provides a group of error counters.

Syntax:

error	[*network#* or *range_of_network#*]

To display information about multiple interfaces, specify the range_of_network# (or a combination of *network#* and *range_of_network#*). For example, specifying **error 0 3 25-50** displays the information for nets 0, 3, and 25 through 50.

Example:

```
+error
                    Input      Input     Input      Input     Output    Output
Net  Interface    Discards     Errors  UnkProto  Flow Drop   Discards    Errors
0    PPP/0              0          0         0          0          0
    0
1    PPP/1              0          0         0          0          0
    0
2    PPP/2              0          0         0          0          0
    0
3    PPP/3              0          0         0          0          0
    0
4    TKR/0              0          0        21          0          0
    0
5    TKR/1              0          0         0          0          0
    0
```

```
6    TKR/2              0          0          0          0          0
     0
7    TKR/3              0          0         17          0          0
     0
8    TKR/4              0          0         22          0          0
     0
9    Eth/0              0          0          0          0          0
     0
10   Eth/1              0          0          0          0          0
     0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Discards
Number of inbound packets which were discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. The packets may have been discarded to free buffer space.

Input Errors
Number of packets that were found to be defective at the data link.

Input Unk Proto
Number of packets received for an unknown protocol.

Input Flow Drop
Number of packets received that are flow controlled on output.

Output Discards
Number of packets that the router chose to discard rather than transmit due to flow control.

Output Errors
Number of output errors, such as attempts to send over a network that is down or over a network that went down during transmission.

Note: The sum of the discarded output packets is not the same as input flow drops over all networks. Discarded output may indicate locally originated packets.

Event

Use the **event** command to access the Event Logging System (ELS) console environment. This environment is used to set up temporary message filters for troubleshooting purposes. All changes made in the ELS console environment will take effect immediately, but will go away when the router is reinitialized. See “Chapter 12. Using the Event Logging System (ELS)” on page 129 for information about the Event Logging System and its commands. Use the **exit** command to return to the GWCON process.

Syntax:

event

Feature

Use the **feature** command to access console commands for specific 2212 features outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access that feature's console prompt, enter the **feature** command at the GWCON prompt followed by the feature number or short name. Table 9 on page 91 lists available feature numbers and names.

Once you access the prompt for that feature, you can begin entering specific commands to monitor that feature. To return to the GWCON prompt, enter the **exit** command at the feature's console prompt.

Syntax:

feature *feature#* or *feature-short-name*

Interface

Use the **interface** command to display statistical information about the network interfaces (for example, Ethernet or Token-Ring). This command can be used without a qualifier to provide a summary of all the interfaces (shown in the following output) or with a qualifier to reveal detailed information about one specific interface.

Descriptions of detailed output for each type of interface are provided in the specific interface *Monitoring* chapters found in this guide. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

interface [*interface#* or *range_of_interface#*]

To display information about multiple interfaces, specify the range_of_network# (or a combination of *interface#* and *range_of_interface#*). For example, specifying **`interface 0 3 25-50`** displays the information for nets 0, 3, and 25 through 50.

Example: `interface`

```
+interface
                                                    Self-Test  Self-Test Maintenance
Net   Net'   Interface                                 Passed     Failed      Failed
0     0      PPP/0                                         2          0
  0
1     1      PPP/1                                         0        165
  0
2     2      PPP/2                                         0        165
  0
3     3      PPP/3                                         0        165
  0
4     4      TKR/0       Slot: 5   Port: 1             1          0
  0
5     5      TKR/1       Slot: 1   Port: 1             0          0
  0
6     6      TKR/2       Slot: 1   Port: 2             0          0
  0
7     7      TKR/3       Slot: 2   Port: 1             1          0
  0
8     8      TKR/4       Slot: 2   Port: 2             1          0
  0
9     9      Eth/0       Slot: 3   Port: 1             1          0
  0
10    10     Eth/1       Slot: 3   Port: 2             0        125
  0
```

Note: The display varies depending on the device.

Nt Global interface number.

Nt' Reserved for dial circuit use. Interface number of the physical network interface that the dial circuit uses.

Interface
Interface name.

Slot-Port
Slot number and port number of the interface.

Self-Test Passed
Number of times self-test succeeded (state of interface changes from down to up).

Self-Test Failed
Number of times self-test failed (state of interface changes from up to down).

Maintenance Failed
Number of maintenance failures.

Memory

Use the **memory** command to display the current CPU memory usage in bytes, the number of buffers, and the packet sizes.

To use this command, free memory must be available. The number of free packet buffers may drop to zero, resulting in the loss of some incoming packets; however, this does not adversely affect router operations. The number of free buffers should remain constant when the router is idle. If it does not, contact your service representative.

Syntax:

memory

Example:

```
memory
Physical installed memory:        16 MB
Total routing (heap) memory:      12 MB
Routing memory in use:            13 %

                  Total  Reserve    Never     Perm     Temp     Prev
                                    Alloc    Alloc    Alloc    Alloc
Heap memory    12231155    26488 10687312  1438487   104924      432

Number of global buffers: Total = 300, Free = 300, Fair = 77, Low = 60
Global buff size: Data = 2048, Hdr = 17, Wrap = 72, Trail = 65, Total = 2208
```

Physical installed memory
The total amount of physical RAM installed in the router.

Total routing memory
The amount of memory available to the routing function, not including that allocated to the base operating system, system extensions, or options such as APPN. This is also called ″heap″ memory, and matches the ″Total″ heap memory size given in bytes shortly thereafter.

Routing memory in use
The percentage of total routing memory that is currently being used by the routing function. Heap memory currently in use is counted under the

following headings **Perm Alloc** and **Temp Alloc**.

Heap memory:
Amount of memory used to dynamically allocate data structures.

Total Total amount of space available for allocation for memory.

Reserve
Minimum amount of memory needed by the currently configured protocols and features.

Never Alloc
Memory that has never been allocated.

Perm Alloc
Memory requested permanently by router tasks.

Temp Alloc
Memory allocated temporarily to router tasks.

Prev Alloc
Memory allocated temporarily and returned.

Number of global buffers:

Total Total number of global buffers in the system.

Free Number of global buffers available.

Fair Fair number of buffers for each interface. (See “Low”.)

Low The number of free buffers at which the allocation strategy changes to conserve buffers. If the value of *Free* is less than *Low*, then buffers will not be placed on any queue that has more than the *Fair* number of buffers in it.

Global buff size:
Global buffer size.

Data Maximum data link packet size of any interface.

Header
Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Trailer Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer

Network

Use the **network** command to enter the console environment for supported networks, such as X.25 networks. This command obtains the console prompt for the specified interface. From the prompt, you can display statistical information, such as the routing information fields for Token-Ring networks.

Syntax:

network *interface#*

At the GWCON prompt (+), enter the **configuration** command to see the protocols and networks for which the router is configured. See “Configuration” on page 114 for more information on the configuration command.

GWCON Process

Enter **interface** at the + prompt for a display of the networks for which the router is configured.

Enter the GWCON **network** command and the number of the interface you want to monitor or change. For example:

```
+network 3
X.25>
```

In the example, the X.25> prompt is displayed. You can then view information about the X.25 interface by entering the X.25 operating commands.

After identifying the interface number of the interface you want to monitor, for interface-specific information, see the corresponding monitoring chapter in this manual for the specified network or link-layer interface. Console support is offered for the following network and link-layer interfaces:

- Bisync (BSC)
- Ethernet
- Frame Relay
- PPP
- SDLC
- SDLC Relay (SRLY)
- Token-Ring
- V.25bis
- X.25
- ISDN
- V.34
- Dial-In
- Dial-Out
- Multilink PPP (MP)
- Layer-2-Tunneling

Performance

Use the **performance** command at the Config> prompt to enter the monitoring environment for performance. See “Chapter 14. Configuring and Monitoring Performance” on page 197 for more information.

Protocol

Use the **protocol** command to communicate with the router software that implements the network protocols installed in your router. The **protocol** command accesses a protocol’s command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands that are specific to that protocol.

Syntax:

protocol *prot#*

Enter the protocol number or short name as part of the command. To obtain the protocol number or short name, enter the CONFIG command environment

(Config>), and then enter the **list configuration** command. See "Accessing the Configuration Process, CONFIG (Talk 6)" on page 16 for instructions on accessing Config>. To return to GWCON, enter **exit**.

See the corresponding monitoring chapter in this manual or in the *Protocol Configuration and Monitoring Reference* for information on a specific protocol's console commands.

Queue

Use the **queue** command to display statistics about the length of input and output queues on the specified interfaces. Information about input and output queues provided by the queue command includes:

- The total number of buffers allocated
- The low-level buffer value
- The number of buffers currently active on the interface.

Syntax:

queue *interface#*or *range_of_interface#*

To display information about multiple interfaces, specify the range_of_network# (or a combination of *interface#* and *range_of_interface#*). For example, specifying **queue 0 3 25-50** displays the information for nets 0, 3, and 25 through 50.

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Queue:

Alloc Number of buffers allocated to this device.

Low Low water mark for flow control on this device.

Curr Current number of buffers on this device. The value will be 0 if the device is disabled.

Output Queue:

Fair Fair level for the length of the output queue on this device.

Curr Number of packets currently waiting to be transmitted on this device. For locally originated packets, the eligibility discard depends on the global low water mark described in the **memory** command.

The router attempts to keep at least the Low value packets available for receiving over an interface. If a packet is received and the value of Curr is less than Low, then the packet will be subject to flow control. If a buffer subject to flow control is to be queued on this device and the Curr level is greater than Fair, then the buffer is dropped instead of queued. The dropped buffer is displayed in the Output Discards column of the **error** command. It will also generate ELS event GW.036 or GW.057.

Due to the scheduling algorithms of the router, the dynamic numbers of Curr (particularly the Input Queue Curr) may not be fully representative of typical values during packet forwarding. The console code runs only when the input queues have

been drained. Thus, Input Queue Curr will generally be nonzero only when those packets are waiting on slow transmit queues.

Reset

Use the **reset** command to disable the specified interface and then re-enable it using new interface, protocol and feature configuration parameters. See “Resetting Interfaces” on page 71 for more information.

Syntax:

reset *interface#*

Statistics

Use the **statistics** command to display statistical information about the network software, such as the configuration of the networks in the router.

Syntax:

statistics *interface#*or *range_of_interface#*

To display information about multiple interfaces, specify the range_of_network# (or a combination of *interface#* and *range_of_interface#*). For example, specifying **statistics 0 3 25-50** displays the information for nets 0, 3, and 25 through 50.

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Example:

```
+statistics
Net   Interface      Unicast  Multicast      Bytes    Packets      Bytes
                   Pkts Rcv   Pkts Rcv   Received      Trans      Trans
0     PPP/0            9815          0     371690       9815     371690
1     PPP/1               0          0          0          0          0
2     PPP/2               0          0          0          0          0
3     PPP/3               0          0          0          0          0
4     TKR/0            1542      19035     968165      40455   23191382
5     TKR/1               0          0          0          0          0
6     TKR/2               0          0          0          0          0
7     TKR/3           74578      32850  114045027      52537   51234542
8     TKR/4           49653      19228   52034171      87285  113444199
9     Eth/0               0         10        670       2438     146280
10    Eth/1               0          0          0          0          0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Unicast Pkts Rcv
Number of non-multicast, non-broadcast specifically-addressed packets at the MAC layer.

Multicast Pkts Rcv
Number of multicast or broadcast packets received.

Bytes Received
Number of bytes received at this interface at the MAC layer.

Packets Trans
Number of packets of unicast, multicast, or broadcast type transmitted.

Bytes Trans
Number of bytes transmitted at the MAC layer.

Test

Use the **test** command to verify the state of an interface or to enable an interface that was previously disabled with the **disable** command. If the interface is enabled and passing traffic, the **test** command will remove the interface from the network and run self-diagnostic tests on the interface.

Syntax:

test *interface#*

Note: For this command to work, you must enter the ***complete*** name of the command followed by the interface number.

Enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command. For example, when testing starts, the console displays the following message:

```
Testing net 0 TKR/0...
```

When testing completes or fails, or when GWCON times out (after 30 seconds), the following possible messages are displayed:

```
Testing net 0 Eth/0 ...successful
Testing net 0 Eth/0 ...failed
Testing net 0 Eth/0 ...still testing
```

Some interfaces may take more than 30 seconds before testing is done.

Note: If the interface you are testing is configured as an alternate WAN Reroute interface, you are prompted:

- If you want to enable the interface's primary-alternate pairings if WAN Reroute is currently disabled for the alternate interface.

  If you answer *yes*, the same action occurs as when you enter the **t 5 enable alternate-circuit** WAN reroute command described in Configuring and Monitoring WAN Restoral in *Using and Configuring Features*.
- If you want to test the interface.

  Normally an alternate WAN Reroute interface is disabled until it is needed to back up its corresponding primary interface. If you answer *yes*, a self-test is started for the interface. If you answer *no*, a self-test does not occur.

See The WAN Reroute Feature, Using WAN Restoral, and Configuring and Monitoring WAN Restoral in the *Using and Configuring Features* for additional information.

Uptime

Use the **uptime** command to display time statistics about the router, including the following:

- Number of restarts.
- Number of known crashes.
- Whether the router was last reloaded or restarted.
- Time elapsed since the last reload.
- Time elapsed since the last restart.

Syntax:

uptime

Chapter 11. The Messaging (MONITR - Talk 2) Process

This chapter explains how to collect and display messages. (Refer to “Chapter 12. Using the Event Logging System (ELS)” on page 129 for information about ELS and message formats. Refer also to the *IBM Event Logging System Messages Guide* for a description of each message. This chapter includes the following sections:

- “What is Messaging (MONITR)?”
- “Commands Affecting Messaging”
- “Entering and Exiting the Messaging (MONITR) Process”
- “Receiving Messages”

What is Messaging (MONITR)?

The MONITR process provides a view of activity inside the router and the networks. MONITR also displays logging messages from the software.

Commands Affecting Messaging

The following commands affect the messaging process:

- OPCON commands:
  - **divert** temporarily diverts output to a different device.
  - **flush** causes the software to discard the messages it collects.
  - **halt** reverses the action of the divert command.
  - **talk** displays message output.
- CONFIG **set logging disposition** command sets the initial device to which the software sends its output.

Entering and Exiting the Messaging (MONITR) Process

To enter the messaging process from OPCON enter the **talk 2** command.

The console displays the messages the software has accumulated.

To exit messaging and return to OPCON, enter the OPCON intercept character (the default is **Ctrl-P**).

Receiving Messages

To receive messages at your console, enter the messaging process as described in the previous section. The software then displays all the messages it has recorded since it was last invoked. While you are connected to the messaging process, it displays all messages as they arrive.

Use the OPCON **divert** and **halt** commands to view software messages while you are doing something else with the router. Permitted devices divert output to TTY0 (the local console), TTY1, or TTY2 (the remote consoles).

Chapter 12. Using the Event Logging System (ELS)

This chapter describes the Event Logging System (ELS). The ELS continually logs all events, filtering them according to parameters that you select. A combination of operational counters and the ELS provides information for monitoring the health and activity of the system. The information is divided into the following sections:

What is ELS?

ELS is a monitoring system and an integral part of the router operating system. ELS manages the messages logged as a result of router activity. Use ELS commands to set up a configuration that sorts out only those messages you feel are important. You can then display the messages on the console terminal screen, log them to a remote workstation, or send the messages to a network management station using Simple Network Management Protocol (SNMP) traps.

The ELS system and the operational counters are the best troubleshooting tools you have to isolate problems in the router. A quick scan of the event messages will tell you whether the router has a problem and where to start looking for it.

In the ELS configuration environment, the commands are used to establish a default configuration. This default configuration does not take effect until the router reinitializes.

Occasionally, it is helpful to temporarily view messages using parameters other than was set up in the ELS configuration environment, without having to reinitialize the router. The ELS operating and monitoring environment is used to:

- Temporarily change the default ELS display settings
  - Changes made in the ELS console environment take effect immediately
  - Changes made in the operating/monitoring environment are not stored in nonvolatile configuration storage.
- View statistical information regarding ELS uses of dynamic RAM

Note: Specific ELS messages are described in the *IBM Event Logging System Messages Guide*.

ELS is a subprocess that you access from the OPCON process.

Entering and Exiting the ELS Configuration Environment

The ELS configuration environment (available from the CONFIG process) is characterized by the `ELS Config>` prompt. Commands entered at this prompt create the ELS default state that takes effect after you restart the router. These commands are described in greater detail later in this chapter.

Configuration commands that have subsystem, group, or event as a parameter are executed in the following order:

- Subsystem
- Group
- Event

To set a basic ELS configuration, enter the **display subsystem all standard** command at the `ELS Config>` prompt. This command configures the ELS to display messages from all subsystems with the STANDARD logging level (that is, all errors and unusual informational comments).

Note: The router does not have a default ELS configuration. You must enter the ELS configuration environment and set the default state.

To enter the ELS configuration environment from OPCON:

1. Enter the **talk 6** command. The console displays the CONFIG prompt (`Config>`). If the prompt does not appear when you first enter CONFIG, press **Return**.
2. At the CONFIG prompt, enter the following command to access ELS:

   ```
   Config> eve
   ```

   The console displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

Event Logging Concepts

This section describes how events are logged and how to interpret messages. Also described are the concepts of subsystem, event number, and logging level. A large part of ELS function is based on commands that accept the subsystem, event number, and logging level as parameters.

Causes of Events

Events occur continuously while the router is operating. They can be caused by any of the following reasons:

- System activity
- Status changes
- Service requests
- Data transmission and reception
- Data and internal errors

When an event occurs, ELS receives data from the system that identifies the source and nature of the event. Then ELS generates a message that uses the data received as part of the message.

Interpreting a Message

This section describes how to interpret a message generated by ELS. Figure 5 shows the message contents.

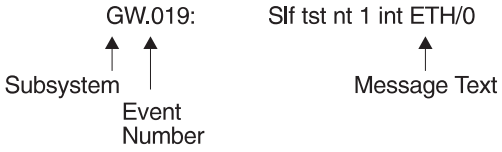

Figure 5. Message Generated by an Event

The information illustrated in Figure 5 as well as the ELS logging level information displayed with the **list subsystem** command is as follows:

Subsystem

Subsystem is a predefined short name for a router component, such as a protocol or interface. In Figure 5, **GW** identifies the subsystem through which this event occurred.

Other examples of subsystems include IP, TKR, and X25. On a particular router, the actual subsystems present depend on the hardware and software configured for that router. You can use the **list subsystem** command described in this chapter to see a list of the subsystems on your router.

Enter the subsystem as a parameter to an ELS command when you want the command to affect the entire subsystem. For example, the ELS command **display subsystem GW** causes all events (except the events with 'debug' logging level) that occur through the GW subsystem to be displayed.

Event Number

Event Number is a predefined, unique, arbitrary number assigned to each message within a subsystem. In Figure 5, **019** is the event number within the GW subsystem. You can see a list of all the events within a subsystem by using the **list subsystem** command, where *subsystem* is the short name for the subsystem.

The event number always appears with a subsystem identifier, separated by a period. For example: **GW.019**. The subsystem and event number together identify an *individual* event. They are entered as a parameter to certain ELS commands. When you want a command to affect only the specified event, enter the subsystem and event number as a parameter for the ELS command.

Logging Level

Logging level is a predefined setting that classifies each message by the type of event that generated it. Use the **list subsystem** ELS console command to display the setting of the logging level. Table 13 on page 132 lists the logging levels and types. ERROR, INFO, TRACE, STANDARD, and ALL are aggregates of other logging level types. STANDARD is the recommended default.

Table 13. Logging Levels

Logging Level	Type
UI ERROR	Unusual internal errors
CI ERROR	Common internal errors
UE ERROR	Unusual external errors
CE ERROR	Common external errors
ERROR	Includes all error levels above
UINFO	Unusual informational comment
CINFO	Common informational comment
INFO	Includes all comment levels above
STANDARD	Includes all error levels and all informational comment levels (default)
PTRACE	Per packet trace
UTRACE	Unusual operation Trace message
CTRACE	Common operation Trace message
TRACE	Includes all trace levels above
DEBUG	Message for debugging
ALL	Includes all logging levels

The logging level setting affects the operation of the following commands:

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

The logging level is set for a particular command when you specify it as a parameter to one of the above commands. For example:

```
display subsystem TKR ERROR
```

Including the logging level on the command line modifies the **display** command so that whenever an event with a logging level of either UI-ERROR or CI-ERROR occurs through subsystem TKR, the console displays the resulting message.

You cannot specify the logging level for operations affecting groups or events.

Message Text

Message Text appears in short form. In Figure 5 on page 131, `Slf tst nt 1 int ETH/0` is the message generated by this event. Variables, such as *source_address* or *network*, are replaced with actual data when the message displays on the console.

The variable *error_code* is referred to by some of the Event Logging System message descriptions (usually preceded by rsn or reason). They indicate the type of packet error detected. Table 14 describes the error or packet completion codes. Packet completion codes indicate the disposition of the packets received by the router.

Table 14. Packet Completion Codes (Error Codes)

Code	Meaning
0	Packet successfully queued for output

Table 14. Packet Completion Codes (Error Codes) (continued)

Code	Meaning
1	Random, unidentified error
2	Packet not queued for output due to flow control reasons
3	Packet not queued because network is down
4	Packet not queued to avoid looping or bad broadcast
5	Packet not queued because destination host is down (only on networks where this can be detected)

ELS displays network information as follows:

```
nt 1 int Eth/0 (or ) network 1, interface Eth/0,
```

where:

- 1 is the network number (each network on the router is numbered sequentially from zero).
- 0 is the unit number (the interfaces of each hardware type are numbered sequentially from zero).

Ethernet and 802.5 hardware addresses appear as a long hexadecimal number.

IP (Internet Protocol) addresses are printed as 4 decimal bytes separated by periods, such as 18.123.0.16.

Groups

Groups are user-defined collections of events that are given a name, the group name. Like the subsystem, subsystem and event number, and logging level, use the group name as a parameter to ELS commands. However, there are no predefined group names. You must create a group before you can specify its name on the command line.

To create a group, use the **add** configuration command, specify the name you want to call the group, and then specify the events you want to be part of the group. The events you add to the group can be from different subsystems and have different logging levels.

After creating a group, use the group name to manipulate the events in the group as a whole. For example, to turn off display of all messages from events that have been added to a group named grouptwo, include the group name on the command line, as follows:

```
nodisplay group grouptwo
```

To delete a group, use the **delete** command.

Using ELS

To use ELS effectively, do the following:

- Know what you want before using the ELS system. Clearly define the problem or events that you want to see before using the MONITR process.
- Execute the command **nodisplay subsystem all all** to turn off all ELS messages.
- Turn on only those messages that relate to the problem you are experiencing.

- Use the *IBM Event Logging System Messages Guide* to determine which messages are not normal.

When initially viewing ELS from the MONITR process, you will see a considerable amount of information. Because the router cannot buffer and display every packet under moderate to heavy loads the buffers are flushed. When this occurs the following message is displayed:

```
xx messages flushed
```

The router does not save these messages. When this message appears, tailor the ELS output to display only that information that is important to the current task you are monitoring, or use the advanced ELS commands to establish a message buffer. See “Using ELS Message Buffering” on page 145.

Managing ELS Message Rotation

It is also important to note that the ELS messages continually rotate through the router’s buffers. To stop and restart the displaying of ELS messages, use the following key combinations:

Ctrl-S to pause scrolling

Ctrl-Q to resume scrolling

Ctrl-P to go back to the last process

You may also want to capture the ELS output to a file. You can do this by starting a script file or log file from your location when Telneting to a router. You can also do this by attaching a PC to the router’s console port and starting a log file from within the terminal emulation package. This information is needed to help Customer Service diagnose a problem.

Capturing ELS Output Using a Telnet Connection on a UNIX Host

Use a Telnet connection on an AIX or UNIX host to capture the ELS messages on your screen to a file on the host. Before beginning, set up ELS for the messages you want to capture using the ELS console commands in “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 149.

To capture the ELS output to a file on an AIX or UNIX host, follow these steps:

1. From the host, enter **telnet** *router_ip_addr* **| tee** *local_file_name*

   router_ip_addr is the IP address of the router

   local_file_name is the name of the file on the host where you want the ELS messages to be saved.

   The **tee** command displays the ELS messages on your screen and, at the same time, copies them to the local file.
2. From the OPCON prompt (*****), enter **t 2**. This accesses the MONITR process, which is the process that displays ELS messages on your screen. Depending on which ELS messages you configured, you should see ELS messages appearing on the screen.

   As long as you are in the MONITR process, all ELS messages will be written to the local file. When you exit the MONITR process (by entering **Ctrl-P**) or terminate the Telnet session, the logging of messages to the local file will stop.

You can also use remote logging instead of capturing ELS output on a UNIX Host. For more information about remote logging, see “Using and Configuring ELS Remote Logging” on page 137.

Configuring ELS So Event Messages Are Sent In SNMP Traps

ELS can be configured so that event messages are sent to a network management workstation in an SNMP enterprise-specific trap. These traps are useful for reporting status and diagnostic results, and are often used for remote monitoring of a 2212. When ELS is configured appropriately, an SNMP trap will be generated each time the selected event occurs. For more information about SNMP, see *Protocol Configuration and Monitoring Reference*.

To tell ELS that a specific event should be activated to be sent as an SNMP trap, at the `ELS config>` prompt or at the `ELS>` prompt, using IP as an example, type:

```
trap event ip.007
```

Note: If you are at the `ELS config>` prompt, you will need to reboot.

To enable the ELS enterprise-specific trap, follow these steps:

1. At the `SNMP config>` prompt, using **public** as an example, type:

   ```
   SNMP config> add address public <network manager IP address>
   SNMP config> enable trap enterprise public
   SNMP config> set community access read_trap public
   ```

   Note: You need to reboot to activate these changes.
2. Enable your network management station to receive and properly display the enterprise-specific traps.

Follow these steps to trap groups, subsystems, and events.

Using ELS to Troubleshoot a Problem

If you are trying to troubleshoot a particular problem, display the messages related to the problem. For example, if experiencing a problem with bridging, turn on the bridging messages:

display subsystem srt all

display subsystem br all

Initially, because of the rapid pace of messages scrolling across the screen, you may want to record the numbers you see and look them up in the *Event Logging System Messages Guide* manual. Once you become familiar with different types of messages being displayed for a particular protocol, you can turn on and turn off only those messages that contain the information that you require to troubleshoot a problem. The following sections list specific ELS examples. Keep in mind that different problems may require different steps.

ELS Example 1

You are interested in looking at the frequency of polling on a Token-Ring interface, and finding out whether the polls are successful.

```
ELS> nodisplay subsystem all all
ELS> display subsystem tkr all
Ctrl-P
* t 2
```

As the messages begin to scroll by, look for ELS message tkr.031.

ELS Example 2

SRB bridging is not working.

1. Check the configuration.
2. Use the GWCON bridging console to verify that the bridging interfaces are enabled.
3. Enter:

   ```
   * t 6
   config> event
   ELS config> nodisplay subsystem all all
   ELS config> display subsystem srb all
   ELS config> exit
   config> Ctrl-P
   ```

4. Restart the routing subsystem. When the subsystem has restarted, enter the following:

   ```
   * t 2
   ```

ELS Example 3

Router cannot communicate with an IPX server on an Ethernet.

1. Enter the **talk** command and the PID for GWCON.

   ```
   * talk 5
   ```

   The console displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **Return**.
2. At the GWCON prompt (+), enter **IPX** to access the IPX console prompt (IPX>).
3. At the IPX console prompt, enter the **slist** command to verify that the server is listed. (See the section on monitoring IPX in the *Protocol Configuration and Monitoring Reference* for information on the **slist** command.)
4. Check the IPX configuration.
5. Enter the following:

   ```
   * t 5
   + event
   ELS> nodisplay subsystem all all
   ELS> display subsystem IPX all
   ELS> display subsystem eth all
   ELS> Ctrl-P
   * t 2
   ```

As the messages begin to scroll by, look for ELS message eth.001. This indicates that the server has a bad Ethernet type field.

Using and Configuring ELS Remote Logging

The remotely-logged ELS message contains all of the information that is contained in ELS messages found in the monitor queue, as viewed under talk 2, and also contains additional information as shown in Figure 6.

```
Date/Time         IP address      Sequence Number      Local Name      ELS Subsystem Name, &
                  assigned        used for detecting   assigned        Formatted message
                  by the user     missing messages     by the user

Nov 20 12:13:47   5.1.1.1         Msg [0444] from      ** IBM/2212 **  :els: ARP.011 Del ent ...
```

Figure 6. Syslog Message Description

Note the following differences in the remote log display:

- The month and day of month in addition to the time, which is always displayed as the time-of-day.
- An IP address, which is the user-specified source IP address. If a DNS server resolves the source IP address to a hostname, then the hostname will be displayed instead of the IP address.
- A Sequence number is added to the message by the source device to assist in detecting dropped messages. See “Remote Logging Output” on page 141 for an explanation of dropped messages. When the sequence number of the message reaches 9999, the next sequence number is 0001.
- A “Local Name” for the source router, to assist in distinguishing between messages from multiple sources. If you do not configure a local name, this field is blank.

Syslog Facility and Level

Remotely-logged ELS messages are transmitted over the network in UDP packets with the destination port number in the UDP header always equal to 514, the syslog port. To receive and process the UDP packets, the *syslog daemon* (syslogd) must be running in the remote workstation that is receiving and logging the ELS messages. See “Remote Workstation Configuration” for details.

Although it is not displayed in the remotely-logged ELS message, every ELS message sent on the network in a UDP packet must be assigned a *syslog_facility* and a *syslog_level*. The syslog daemon uses the combination of facility and level to determine where to route the message. Typically, you want the ELS messages to be written to one or more files in the remote host. Other options include displaying the message on the console, sending the message to one or more users, or sending the message to another workstation.

The commands you use to specify the *syslog_facility* and *syslog_level* values, along with other remote-logging related console commands, are described in “ELS Monitoring Commands” on page 171 and “ELS Configuration Commands” on page 149 . Review these commands before reading through the next section.

Remote Workstation Configuration

The following configuration assumes that a single 2212 is remote-logging to a single remote workstation. You can configure multiple 2212s to remote-log to the same

remote workstation. However, a particular 2212 can log to one and only one remote workstation. The operating system used in this example is AIX 4.2. Your environment may be slightly different. For more information on syslog, refer to the documentation for your operating system.

To perform the configuration on an AIX workstation, you must log in as **root**. To configure the workstation:

1. Create or edit a syslog.conf file to specify where ELS messages with particular *syslog_facility* and *syslog_level* values are to be written. See the bottom of Figure 7 on page 139 for an example of how to specify the message destination. Note that the full pathname of the log files must be specified. The default location for the syslog configuration file is /etc/syslog.conf.
2. Create the files for logging syslog messages that you specified in the syslog.conf file.
3. Start the syslog daemon by entering **syslogd**. To start the syslog daemon from SRC (System Resource Controller), enter **startsrc -s syslogd**. If the pathname of the configuration file is not /etc/syslog.conf, then enter **syslogd -f** *pathname*. To start the syslog daemon in debug mode, enter **syslogd -d**.

   Note: Running multiple instances of the syslog daemon is not supported.
4. If the syslog daemon is already running when you create or modify the syslog.conf file, it must be restarted so that the daemon reinitializes the configuration from syslog.conf.
5. Verify the setup by using the **logger** command as follows:

   ```
   logger -p user.alert  THIS IS A TEST MESSAGE (user.alert)
   logger -p news.info  THIS IS A TEST MESSAGE (news.info)
   ```

   If the setup is correct, `THIS IS A TEST MESSAGE...` will be written to the files specified in syslog.conf.

```
# @(#)34       1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>               <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#      * - all (except mark)
#      kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
#      emerg,alert,crit,err(or),warn(ing),notice,info,debug
#      (meaning all messages of this priority or higher)
#
# <destination> is:
#      /filename - log to this file
#      username[,username2...] - write to user(s)
#      @hostname - send to syslogd on this machine
#      * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
#  mail.debug          /usr/spool/mqueue/syslog
#  *.debug             /dev/console
#  *.crit                      *

#   syslog messages with facilty / priority values of LOG_USER,   LOG_ALERT
user.alert            /tmp/syslog_user_alert

#   syslog messages with facilty / priority values of LOG_NEWS,  LOG_INFO
news.info           /tmp/syslog_news_info
```

Figure 7. syslog.conf Configuration File

Configuring the 2212 for Remote Logging

To configure a 2212:

1. In talk 6, configure the remote-logging facility as shown in Figure 8 on page 140. The IP address specified as the *source-ip-addr* should be an IP address that is configured in the 2212 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address resolves quickly into a hostname by the name server or that

the name server at least responds quickly with “address not found.” To determine whether this happens, issue the **host** command on your workstation as follows:

```
workstation> host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address which resolves more quickly.

2. In talk 6 configure events and subsystems for remote-logging, as shown in Figure 9 on page 141.
3. Restart the 2212.

```
ELS config>set remote source-ip-addr 5.1.1.1
Source IP Addr = 5.1.1.1

ELS config>set remote remote-ip-addr 192.9.200.1
Remote Log IP Addr = 192.9.200.1

ELS config>set remote local-id ** IBM/2212 **
Remote Log Local ID = ** IBM/2212 **

ELS config>set remote no-msgs-in-buffer 100
Number of messages in Remote Log Buffer must be 100-512
Number of Messages in Remote Buffer = 100

ELS config><B>set remote facility log_news
Default Syslog Facility = LOG_NEWS

ELS config>set remote level log_info
Default Syslog Level = LOG_INFO

ELS config>set remote on
Remote Logging is ON

ELS config>list remote

------------------   Remote Log Status  -----------------

Remote Logging is ON
Source IP Address = 5.1.1.1
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_NEWS
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log =  100
Remote Logging Local ID = ** IBM / 2212 **
ELS config>
```

Figure 8. Configuring the 2212 for Remote Logging

```
ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info

ELS config>display event ip.068
ELS config>remote event ip.068 log_news log_info

ELS config>display event ip.058
ELS config>remote event ip.058 log_news log_info

ELS config>display event ip.022
ELS config>remote event ip.022 log_news log_info

ELS config>display event gw.022
ELS config>remote event gw.22 log_news log_info

ELS config>display event arp.011
ELS config>remote event arp.011 log_user log_alert

ELS config>display event arp.002
ELS config>remote event arp.022 log_user log_alert

ELS config>list status
Subsystem:    SNMP
Disp levels:  ERROR INFO TRACE
Trap levels:  none
Trace levels: none
Remote levels:  ERROR INFO TRACE
        Syslog Facility/Level: LOG_NEWS LOG_INFO

Event     Display Trap    Trace     Remote
SRT.017   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.068    On      Unset   Unset
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.058    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
GW.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
ARP.011   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
ARP.002   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
```

Figure 9. Configuring Subsystems and Events for Remote Logging

Remote Logging Output

Figure 10 on page 142 shows a sample from the /tmp/syslog_news_info file. Notice that the first message has a sequence number of 310. This means that the first 309 ELS messages were not sent from the source 2212. There are several reasons for this:

- The remote-logging facility had not completed initialization when the messages were first passed to ELS

- A route from the source 2212 to the remote workstation was not in the routing table
- The interface for the outbound UDP packet containing the ELS messages was not in the “Up” state

Notice in 1 that messages 311-313 did not get remote-logged. This is because an ARP request was outstanding and until the ARP response is received, all but the first packet is dropped in the source 2212. Additionally, the ARP cache is cleared at a user-configured refresh rate, and a new ARP request is issued. To determine when this is occurring, you can remote log events ARP.002 and ARP.011 in addition to the primary ELS events of interest. Figure 12 on page 143 shows ARP events logged to the *syslog_user_alert* file that account for events 445 and 446, which were indicated as missing in Figure 10.

```
Nov 20 12:03:16 workstа01 root:  THIS IS A TEST MESSAGE  (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / 2212 **: els:  IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0

1 ( messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see
  explanation in the text)

2 (messages 314 and 315 were logged to a separate
file - see explanation in the text)

Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / 2212 **: els:  IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / 2212 **: els:  IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / 2212 **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4


(message 319 was logged to a separate file)

Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / 2212 **: els:  IP.068: routing cache cleared

(120 messages not shown)

Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / 2212 **: els:  GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / 2212 **: els:  GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / 2212 **: els:  GW.022: Nt fld slf tst nt 11 int ISDN/0


(messages 444 and 447 were logged to a separate file)


(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / 2212 **: els:  GW.022: Nt fld slf tst nt 4 int PPP/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / 2212 **: els:  IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / 2212 **: els:  IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int PPP/0
```

Figure 10. Sample Contents from Syslog News Info File

If the initial ELS messages that are generated during and immediately after booting are of particular interest, then it is recommended that these messages also be displayed in the monitor queue, which is viewed with talk 2. Figure 11 on page 143 shows the talk 2 output including the initial messages that did not get remote-logged. Note that there is a message in the talk 2 output that indicates that the remote-logging facility is available. This does not indicate that a route exists to the remote workstation, nor that the associated interface is in the “Up” state. It simply provides a reference point before which no messages can be successfully remote-logged.

Also notice that you can account for the messages that were missing (indicated in Figure 10 with 2) in the talk 2 output.

```
12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:28   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28   IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int PPP/0

     ( 297 messages not shown )                                    Corresponding Sequence
                                                                   Numbers in
12:08:43   GW.022: Nt fld slf tst nt 12 int PPP/2                  Remote-Logging Files :
12:08:43   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48   IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0   [0310] first message logged
12:08:48  SRT.017: Enabling SRT on port 1 nt 0 int Eth/0          -- not logged (ARP request) --
12:08:48  STP.016: Select as root TB-1, det topol chg            -- not logged (ARP request)--
12:08:48  STP.026: Root TB-1, strt hello tmr                     -- not logged (ARP request)--
12:08:48  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0                 [0314]
12:08:48  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                 [0315]
12:08:48   IP.068: routing cache cleared                         [0316]


     ( 126 messages not shown )

12:13:38   GW.022: Nt fld slf tst nt 11 int ISDN/0               [0443]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                    [0444]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                    -- not logged (ARP request) --
12:13:47  ARP.002: Pkt in 1 1 800 nt 5 int Eth/4                 -- not logged (ARP request)--
12:13:47  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                 [0447]
12:13:50   GW.022: Nt fld slf tst nt 4 int PPP/0                 [0448]
```

Figure 11. Output from Talk 2

You can use the timestamp, which appears in both the remote-logging output file and the talk 2 output, to determine when the first ELS message is successfully remote-logged. To use the timestamp for this purpose, configure ELS such that the timestamp in the monitor queue displays the time-of-day.

Also notice in Figure 10 on page 142 that messages 311-313 did not get remote-logged. This is because an ARP request was outstanding and until the ARP response is received, all but the first packet is dropped in the source IBM 2212. The ARP cache is cleared at a user-configured refresh rate, and the device issues a new ARP request. To determine when ARP requests are occurring, events ARP.002 and ARP.011 can be remote-logged, in addition to the ELS events of interest. Figure 12 shows ARP events logged to the *syslog_user_alert* file that account for events 445 and 446, which were indicated as missing in Figure 10 on page 142 .

```
Nov 20 12:02:53 worksta01 root: THIS IS A TEST MESSAGE (user.alert)
Nov 20 12:08:48 5.1.1.1 Msg [0314] from ** IBM / 2212 **: els:  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0315] from ** IBM / 2212 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0319] from ** IBM / 2212 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0444] from ** IBM / 2212 **: els:  ARP.011: Del ent 1 3 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0447] from ** IBM / 2212 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
```

Figure 12. Sample Contents from Syslog_user_alert File

You can prevent the loss of ELS messages caused by this ARP sequence by establishing a static relationship between the IP address and the MAC address. The basic steps are outlined below and are illustrated in Figure 13 on page 144.

1. In talk 5, “ping” the remote workstation’s IP address
2. In talk 5, determine the interface (net) number used to send messages to the remote-workstation’s IP address
3. Use the net number from the previous step to determine the associated MAC address

4. In talk 6, add an ARP entry to establish a static IP address to MAC address relationship

```
*t 5
+p ip

IP>ping 192.9.200.1
PING 192.9.200.20 -> 192.9.200.1: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.9.200.1: icmp_seq=0. ttl=64. time=0. ms
----192.9.200.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

IP>dump

  Type   Dest net            Mask          Cost    Age       Next hop(s)
.
   Dir*  192.9.200.0         FFFFFF00      1       102305    Eth/0
.
IP>exit
+int
                                                    Self-Test  Self-Test   Maintenance
Net   Net'   Interface  Slot-Port                   Passed     Failed      Failed
0     0      Eth/0      Slot: 1   Port: 1               1          0           0
.
+p arp
ARP>dump
Network number to dump [0]? 0
Hardware Address        IP Address        Refresh
02-60-8C-2D-69-5D       192.9.200.1       2

Ctrl-P
*t 6
config>p arp
ARP config>add entry
Interface Number [0]? 0
Protocol [IP]? IP
IP Address [0.0.0.0]? 192.9.200.1
Mac Address []? 02608C2D695D
ARP config> list entry

Mac address translation configuration

IF #      Prot #  Protocol -> Mac address
   0           0  192.9.200.1 -> 02608C2D695D
ARP config>exit
Config>write

Ctrl-P

*reload
Are you sure you want to reload the gateway? (Yes or [No]): Yes

 (after reload, static ARP entry is active)
```

Figure 13. Example of Setting Up a Static ARP Entry

Additional Considerations

ELS Messages Containing IP Addresses

ELS messages containing an IP address which matches the IP address of the remote workstation will not be remote-logged, even if configured for remote-logging, and may appear under talk 2. These messages are discarded instead of being remote-logged in order to prevent excessive UDP packets from being sent on the network.

Duplicate Logging

If a facility value is repeated in *syslog.conf*, for example:

```
user.debug        /tmp/syslog_user_debug
user.alert        /tmp/syslog_user_alert
```

The syslog daemon will log *user.debug* messages only to the */tmp/syslog_user_debug* file while user.alert messages will be logged to both the */tmp/syslog_user_debug* file and the */tmp/syslog_user_alert* file. This is consistent with the syslog design that logs the more severe conditions in multiple places.

To prevent this duplicate logging, it is recommended that different facility values be specified in the *syslog.conf* file. A total of 19 facility values are available.

Recurring Sequence Numbers in Syslog Output Files

Depending upon the configuration of your network, it is possible for duplicate UDP packets containing ELS messages to arrive at the remote host. It is also possible for the packets to arrive in a different order than they were transmitted. An example of this phenomenon is shown in Figure 14. Notice that the messages with sequence numbers 628 through 633 are logged twice. Also notice that after the first occurrence of sequence number 0630, sequence number 0629 occurs again, followed by the second occurrence of 0630.

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

Figure 14. Example of Recurring Sequence Numbers in Syslog Output

Because neither Syslog nor UDP has the ability to handle duplicate or out of sequence packets, it is important to recognize the possibility of duplicate sequence numbers occurring.

Using ELS Message Buffering

Message buffering is an advanced feature of ELS that can help you with problem determination. You can set up defaults that ELS will use for message buffering or change how messages are buffered while the router is operating. Message buffering can minimize the information lost because messages have wrapped in the default message buffers. Message buffering is accessible through the **advanced** configuration or monitoring command. It enables you to:

- Specify whether buffering is active.
- Specify what events are written to the message buffer.
- Stop buffering and free the memory allocated for buffering.
- Display the status of the message buffer.
- Specify an event that stops message buffering and what action the system takes when the event occurs.

- Send a formatted version of the buffer to a file at a remote server.
- View a specific number or all of the ELS messages in the buffer.
- Write the buffer to a hard file if a hard file is present.
- Read a file that contains a formatted ELS message buffer from the hard file, if a hard file is present.
- Send a file that contains a formatted ELS message buffer from the hard file, if a hard file is present.

For specifics about the commands, see “ELS Message Buffering Configuration Commands” on page 167 and “ELS Message Buffering Monitoring Commands” on page 191 .

The following example shows how to configure ELS message buffering.

```
MOS Operator Control

*t 5 :Enter t 5 at the * prompt.

CGW Operator Console

+ev :Enter ev at the + prompt.
Event Logging System user console
ELS>a :Enter a for advanced at the ELS prompt.
Advanced ELS Console
ELS Advanced>li s :Enter li s to list status at the > prompt.
-----------------Advanced ELS Configuration-----------------------
Logging Status:  OFF  Wrap Mode:  ON   Logging Buffer Size: 0 KB
Stop-Event:  NONE   Stop-String:   NONE
Additional Stop-Action:  NONE
-----------------------Run-Time Status-----------------------------
Has Stop Condition Occurred?   NO   Messages currently in buffer:  0

ELS Advanced>s b :Enter s b to set buffer size.
Enter buffer size of 0 KB or between 148 and 593 KB  148 ?
Buffer size set to 148 KB
ELS Advanced>s s e gw.26 :Enter s s e to set stop event eg. gw.26
Stop Event "GW.026" has been set
ELS Advanced>ex :Enter ex to exit Advanced to list gw.26
ELS>list ev gw.26
Level: C-TRACE
Message: Mnt nt %n int %s/%d
Active:         Count: 742

ELS>a :Enter a to get back to advanced.
Advanced ELS Console
ELS Advanced>s s s Mnt nt 5 :Enter s s s to set the stop string.
Stop String set to "Mnt nt 5"
ELS Advanced>s s a ? :Enter s s a ? to query available stop actions.
NONE
APPN-DUMP  :Only available if APPN active and in the load image.
SYSTEM-DUMP
ELS Advanced>s s a s :Enter s s a s to set SYSTEM-DUMP stop action.
Stop Action has been set to SYSTEM-DUMP
ELS Advanced>s w off to :Enter s w on to set wrap mode off.
Advanced Wrap Mode set to OFF.

ELS Advanced>log sub gw all :Enter to enable the whole gw subsystem
ELS Advanced>s l on :Enter s l on to start the logging process.
Advanced Logging set to ON.
ELS Advanced>li s :Enter to list status of logging.
-----------------Advanced ELS Configuration-----------------------
Logging Status:  OFF  Wrap Mode: OFF  Logging Buffer Size: 148 KB
Stop-Event:     GW.026   Stop-String:  Mnt nt 5
Additional Stop-Action:  SYSTEM-DUMP
-----------------------Run-Time Status-----------------------------
Has Stop Condition Occurred?   YES  Messages currently in buffer:  7

ELS Advanced>v a n :Enter to view all messages in buffer. For this
                    trivial example any viewing command suffices.

 1  10:52:10   GW.026: Mnt nt 0 int Eth/0
 2  10:52:10   GW.026: Mnt nt 5 int Eth/1->This triggers stop action
 3  10:52:14   GW.026: Mnt nt 0 int Eth/0  Note that 5 more events
 4  10:52:14   GW.026: Mnt nt 5 int Eth/1  get logged before
```

```
 5  10:52:18   GW.026: Mnt nt 0 int Eth/0  logging stops and
 6  10:52:18   GW.026: Mnt nt 5 int Eth/1  the stop action occurs.
 7  10:52:22   GW.026: Mnt nt 0 int Eth/0


Bughlt: Dump initiated by ELS Stop Action.

BUGHLT+80; Dump initiated by ELS Stop Action.

Note:
In reality if the stop action is the SYSTEM-DUMP you will not be
able to list the final status as above nor view the buffer because
the router will be attempting to reload.
```

Chapter 13. Configuring and Monitoring the Event Logging System (ELS)

This chapter describes how to configure events logged by ELS and how to use the ELS commands. The information includes the following sections:

- "Accessing the ELS Configuration Environment"
- "ELS Configuration Commands"
- "Entering and Exiting the ELS Operating Environment" on page 170
- "ELS Monitoring Commands" on page 171

For more information on the Event Logging System and how to interpret ELS event messages, refer to "Chapter 12. Using the Event Logging System (ELS)" on page 129.

Accessing the ELS Configuration Environment

The ELS configuration environment is characterized by the `ELS config>` prompt. Commands entered at this prompt are described "Chapter 13. Configuring and Monitoring the Event Logging System (ELS)".

To enter the ELS configuration environment:

1. Enter **talk 6**.

   The monitoring displays the `Config>` prompt. If the prompt does not appear, press **Return**.
2. At the `Config>` prompt, enter the following command to access ELS:

   ```
   event
   ```

   The monitoring displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

ELS Configuration Commands

Table 15 summarizes the ELS configuration commands. The remainder of this section describes each one in detail. After accessing the ELS configuration environment, you can enter ELS Configuration commands at the `ELS Config>` prompt.

Table 15. ELS Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds an event to an existing group or creates a new group.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Clears all ELS configuration information.
Default	Resets the display or trap setting of an event, group, or subsystem.

Table 15. ELS Configuration Command Summary (continued)

Command	Function
Delete	Deletes an event number from an existing group or deletes an entire group.
Display	Enables message display on the console monitor.
Filter	Filter ELS messages based upon the net number.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to a remote workstation.
Notrace	Controls disablement of packet trace events.
Notrap	Keeps messages from being sent out in SNMP traps.
Remote	Allows messages to be logged to a remote workstation.
Set	Sets the pin parameter and the timestamp feature options.
Trace	Controls enablement of packet trace events.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Add

Use the **add** command to add an individual event to an existing group or to create a new group. Group names must start with a letter and are case sensitive. You cannot append an entire subsystem to a group.

Syntax:

add *group_name subsystem.event_number*

Note: If the specified group does not exist, the following prompt asks you to confirm the creation of a new group:

```
Group not found. Create new group? (yes or no)
```

Advanced

Use the **advanced** command to enter the advanced configuration environment. In this environment you configure message buffering.

Syntax:

advanced

Clear

Use the **clear** command to clear all of the ELS configuration information.

Syntax:

clear

Example:

```
clear

You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):
```

Default

Resets the display or trap setting of an event, group, or subsystem back to a disabled state.

Syntax:

default	display
	trap
	remote

display *event* **OR** *group* **OR** *subsystem*
Controls the output of the display of messages to the monitoring.

trap *event* **OR** *group* **OR** *subsystem*
Controls the generation of traps to the network management station.

remote *event* **OR** *group* **OR** *subsystem*
Controls the generation of traps to the remote station.

Delete

Use the **delete** command to delete an event number from an existing group or to delete the entire group. If the specified event is the last event to be deleted in a group, you will be notified. If *all* is specified instead of *subsystem.event_number*, a prompt asks you to confirm the deletion of the entire group.

Syntax:

delete	*group_name subsystem.event_number*

Display

Use the **display** command to enable message displaying on the monitoring monitor for specific events, a range of events for a subsystem, groups, or subsystems.

Syntax:

display	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Displays messages of the specified event (*subsystem.event#*).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Displays messages associated with the specified subsystem. To find out which subsystems are on the router, type **list subsystems**.

Note: Although ELS supports all subsystems on the router, not all devices support all subsystems. See *Event Logging System Messages Guide* for a list of currently supported subsystems.

Filter

Use the **filter** command to access the filter configuration command environment. See "ELS Net Filter Configuration Commands" on page 164 for complete command details.

Syntax:

filter net

List

Use the **list** command to get updated information regarding ELS settings and listings of selected messages.

Syntax:

list all
filter-status
groups
pin
remote-log status
status
subsystem . . .
subsystems all
trace-status

all Lists information from all the **list** categories.

filter-status
Lists ELS net number filters.

groups
Lists the user-defined group names and contents.

pin Lists the current number of ELS event messages sent in SNMP traps (per second).

remote-log status
Lists the current values of remote logging options.

Example:

```
list r

Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME
```

status Lists the subsystems, groups, and events that have been modified by the **display**, **nodisplay**, **trap**, **notrap**, **trace**, **notrace**, **remote**, and **noremote** commands.

Example:

```
list status

Subsystem:              TKR
Disp Levels:            STANDARD
Trap levels:            none
Trace levels:           none
Remote levels:          ERROR INFO TRACE
Syslog Facility/Level: LOG_USER LOG_INFO

Group        Disp     Trap    Trace  Remote
Mygroup     Unset    Unset    Unset    On
                                      Syslog Facilty/Level: LOG_DAEMON LOG_CRIT

Event        Disp     Trap    Trace  Remote
IP.007      Unset    Unset    Unset    On
                                      Syslog Facility/Level: LOG_CRON LOG_NOTICE
```

Note: Not only is remote logging enabled, but the display includes the Syslog Facility/Level values for each subsystem, group, and event. Ranges of events are listed as individual events.

subsystem

Lists names, events, and descriptions of all subsystems.

(Example output from a **list subsystem** command can be found beginning on page 174.)

subsystem *subsystem*

Lists all events in a specified subsystem.

Example:

```
list subsystem gw


Event      Level      Message

GW.001     ALWAYS   Copyright 1984 Mass Institute of Technology
GW.002     ALWAYS   Portable CGW %s Rel %s strtd
GW.003     ALWAYS   Unus pkt len %d nt %d int %s/%d
GW.004     ALWAYS   Sys %s q adv alloc %d excd %d
GW.005     ALWAYS   Bffrs: %d avail %d idle   fair %d low %d
GW.006     C-INFO    Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007     C-INFO    Ip err %x nt %d int %s/%d
GW.008     U-INFO    Ip ovfl nt %d int %s/%d, disc
GW.009     UI-ERROR  Nt dwn ip rstrt nt %d int %s/%d
GW.010     UI-ERROR  Ip q len %d no ip buf nt %d int %s/%d
GW.011     U-INFO    Op err %x hst %wo nt %d int %s/%d
GW.012     U-INFO    Op err cnt excd hst %wo nt %d int %s/%d
GW.013     U-INFO    Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014     UI-ERROR  Nt dwn op rstrt nt %d int %s/%d
GW.015     UI-ERROR  Nt dwn to hst %wo nt %d int %s/%d
GW.016     U-INFO    Op ovfl to hst %wo nt %d int %s/%d
GW.017     UE-ERROR  Intfc hdw mssng nt %d int %s/%d
GW.018     U-TRACE   Strt nt slf tst nt %d int %s/%d
GW.019     C-INFO    Slf tst nt %d int %s/%d
GW.020     U-TRACE   Nt pss slf tst nt %d int %s/%d
GW.021     UE-ERROR  Nt up nt %d int %s/%d
GW.022     U-TRACE   Nt fld slf tst nt %d int %s/%d
```

subsystems all

Lists all events in all subsystems.

trace-status

Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay event. . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*

Suppresses the displaying of a specified event (*subsystem.event#*).

group *groupname*

Suppresses the displaying of messages that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*

Suppresses the displaying of messages associated with the specified subsystem.

Noremote

Use the **noremote** command to suppress the logging of events to a remote workstation based on event number, group, range of events, or subsystem.

Note: With the **noremote** command, there is usually no need to specify a *syslog_facility* and *syslog_level*, such as there is with the **remote** command. However, for **noremote subsystem** command, there exists the option of selectively suppressing specific message levels (for example, “error” only or “trace” only) rather than turning them all off. (If you do not specify any

particular message level, “all” is assumed). Additionally, with the **noremote subsystem** command, you can set a *syslog_facility* and *syslog_level* for any remaining message levels that have not been turned off.

Syntax:

noremote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.019, gw.020, gw.021, and gw.022

subsystem *subsystem.name [syslog_facility syslog_level]*
Suppresses the remote logging of messages associated with the specified subsystem (*subsystem.name*).

Example 1:

```
noremote subsystem tkr
```

Suppresses the remote logging of all “tkr” messages.

Example 2:

```
ELS config> noremote subsystem tkr info
ELS config> SYSLOG FACILITY[LOG_USER]?
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

In this example, “LOG_USER” and “LOG_INFO” were the values last picked for subsystem TKR. The command specified turns off the remote logging for subsystem TKR only for messages coded for “info”. Because *syslog_facility* and *syslog_level* was not specified, the software prompts for *syslog_facility* and *syslog_level*. If you enter another value at the prompts, that value will replace *syslog_facility* and *syslog_level* for the remaining remote-logged messages for the TKR subsystem.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

For more information about *syslog_facility* and *syslog_level* see “Remote” on page 157 .

Notrace

Disables packet trace for the specified event/range/subsystem/group.

Syntax:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of packet trace data for the specified event#

group *groupname*
Suppresses the sending of packet trace data that was previously added to the specified group (groupname).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
trace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Suppresses the sending of packet trace data for the specified subsystem (subsystemname).

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*
Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname*
Suppresses the sending of messages in SNMP traps that are associated with the specified subsystem.

Remote

Use the **remote** command to select the events to be logged to a remote workstation by event number, range of events, group, or subsystem.

Syntax:

remote event . . .
range . . .
group . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*
Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert

log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM 2212. They are merely identifiers which are used by the syslog daemon on the remote workstation.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 157.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely on the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

group *group.name syslog_facility syslog_level*

Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 157.

subsystem *subsystem.name message_level syslog_facility syslog_level*

Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely at the files based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 157.

Message_level is a value such as “ALL,” “ERROR,” “INFO,” or “TRACE” . See “Logging Level” on page 131. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem TKR all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely based on log_user and log_info values at the remote host.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

Set

Use the **set** command to set the maximum number of tags per second, the timestamp feature, or to set tracing options.

Syntax:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin *max_traps*

Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number (*max_traps*) is sent every tenth of a second.)

remote-logging

Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
no-msgs
remote_ip_addr . . .
source_ip_addr ...
local_id

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the 'remote' command will be prevented from being logged.

facility

Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon

log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

no-msgs
Specifies the number of messages in the buffer for the remote log before log wraps.

remote_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255. It represents the ip address of the remote host where the log files reside.

source_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255.

You should use an IP address that is configured in the 2212 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

local_id
This is any character string of up to 32 characters, which is

included in the logged message at the remote file and can help identify which machine logged the message.

timestamp [timeofday or uptime or off]
Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message. Set timestamp can also be turned off.

Use the **set timestamp** command to enable one of the following timestamp options.

timeofday
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

trace Use the **set trace** command to configure tracing options. If you configure tracing options from the monitoring environment, the changes take effect immediately. They return to their previously configured settings when the device is rebooted.

Note: Tracing should be used only under the direction of trained support personnel. Tracing, especially when used with disk-shadowing enabled, uses device resources and can impact overall performance and throughput.

Syntax:

set trace
- decode
- default-bytes-per-pkt
- disk-shadowing
- max-bytes-per-pkt
- memory-trace-buffer-size
- off
- on
- reset
- stop-event
- wrap-mode

decode *off/on*
Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing [[off or on] or record-size or time-limit or delete-file or max-file-size]

Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

[off or on]

Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it can no longer be viewed from the monitoring.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

disk-shadowing delete-file

Deletes the trace file.

disk-shadowing max-file-size *Mbytes*

Sets the maximum file size for the trace file.

Valid Values: 1 Mbyte to 16 Mbytes

Default Value: 10 Mbytes

disk-shadowing record-size *bytes*

Sets the record size for trace file records:

Valid Values 1024, 2048, or 4096 bytes

Default 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

disk-shadowing time-limit *hours*

Sets the maximum time for disk-shadowing of traces:

Valid Values 1 - 72 hours

Default 24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

max-bytes-per-pkt *bytes*

Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*

Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

wrap-mode [off or **on]**
Turns the trace buffer wrap mode on or off. If wrap mode is on and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Trace

Enables packet trace for the specified event/range/subsystem/group. When the **trace** command is used from the `ELS Config>` prompt, the changes become part of the configuration, and a reboot is required to activate the changes.

Syntax:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the router monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the router monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the router.

ELS Net Filter Configuration Commands

ELS net filters give you the capability of looking only at ELS messages with certain net numbers and discarding other ELS messages.

When you create a filter, you specify the subsystem, event, or range of events to which the filter applies. You also specify the queue (for example, “DISPLAY”,

"TRAP", "TRACE", or "REMOTE-LOGGING"). Finally, you specify the net number (or range of net numbers) that you want to filter.

When you enable the filter, messages that have been turned on by the ELS commands are subject to filtering. The filter allows only messages with the specified net numbers. The filter causes the device to discard messages that do not contain the specified net numbers.

By reducing the number of ELS messages sent, you can more easily locate messages for the interfaces in which you are interested.

This section describes the commands to configure the ELS net filters. To configure these filters, enter the **filter net** command at the ELS> prompt. Then, enter the configuration commands at the `ELS Filter net>` prompt.

Table 16. ELS Net Filter Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Create	Creates a filter and assigns it a number. A maximum of 64 filters is allowed.
Delete	Deletes a specified filter number or all filters.
Disable	Disables a specified filter number or all filters.
Enable	Enables a specified filter number or all filters.
List	Lists a specified filter number or all filters.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Create

Use the **create** command to create an ELS net filter.

Syntax:

create ***queue*** event *event_name net#_start net#_end*
range *event_range net#_start net#_end*
subsystem *subsystem_name net#_start net#_end*

queue The queue for which you are setting the filter. The valid queues are:

Display
Trace
Trap
Remote

event *event_name net#_start net#_end*
Specifies the event and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **`create trap event GW.009 2 10`** filters traps for message GW.009 for net numbers 2 through 10.

range *event_range net#_start net#_end*
Specifies the range of ELS messages and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create remote range ipx 19 22 3 6** filters all ipx messages beginning with IPX.019 and ending with IPX.022 for net numbers 3 through 6 for remote logging.

subsystem *subsystem_name net#_start net#_end*
Specifies the subsystem and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create display subsys ip 1 1**, filters all ELS messages for the ip subsystem that contain net number 1 to the display. All other ip subsystem messages are discarded.

Delete

Use the **delete** command to delete a specific ELS filter or all ELS filters.

Syntax:

delete all
filter *filter#*

all Deletes all currently configured filters.

filter *filter#*
Deletes the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to delete.

Disable

Use the **disable** command to disable a specific ELS filter or all ELS filters.

Syntax:

disable all
filter *filter#*

all Disables all currently configured filters.

filter *filter#*
Disables the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to disable.

Enable

Use the **enable** command to enable a specific ELS filter or all ELS filters.

Syntax:

enable all
filter *filter#*

all Enables all currently configured filters.

filter *filter#*
Enables the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to enable.

List

Use the **list** command to list a specific ELS filter or all ELS filters.

Syntax:

list all
filter *filter#*

all Lists all currently configured filters.

filter Lists the filter specified by *filter#.*

ELS Message Buffering Configuration Commands

Table 17 describes the commands available at the `ELS Config Advanced>` prompt.

Table 17. ELS Message Buffering Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
List	Displays the configuration settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Config Advanced> list status
---------------------------------Configuration-----------------------------------
Logging Status:    OFF    Wrap Mode:   ON  Logging Buffer Size:    8500   Kbytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  NONE
```

See “Set” on page 169 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log event
group

range

subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event

group

range

subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Set

Use the **set** command to configure various ELS message buffering options.

Syntax:

set buffer-size *Kbytes*
logging [on or off]
stop action . . .
stop event *subsystem.event#*
stop string *text*
wrap on or off]

buffer-size *Kbytes*
Specifies the size, in kilobytes, of the message buffer that the system should allocate. The **mem** command displays this memory as "Never Alloc." Setting this value too high could prevent the router from operating correctly after a reboot because of insufficient memory for protocols and features.

Valid values: 0 KB to 80% of the memory available on the router.

Default value: 0 (no message buffering)

Note: You must allocate a buffer with this command before you can set logging on.

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the "stop event" (and if specified, the "stop string") occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard file. If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified “stop action.”

Logging remains stopped until the next time you issue the **set logging on** command or reboot the router.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**
Specifies the string to be used in conjunction with the “stop event” to stop logging. If you have not specified a stop event, the system ignores the “stop string.”

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the “stop string.”

Default value: none

wrap [on or **off]**
Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Entering and Exiting the ELS Operating Environment

The ELS monitoring environment (available from the GWCON process) is characterized by the ELS> prompt. Commands entered at this prompt modify the current ELS parameter settings. These commands are described “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 149.

To enter the ELS monitoring environment from OPCON:

1. Enter the **talk 5** command.

   ```
   * talk 5
   ```

   The monitoring displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **Return**.
2. At the GWCON prompt, enter the following command to access ELS:

   ```
   + event
   ```

   The monitoring displays the ELS monitoring prompt (ELS>). Now, you can enter ELS monitoring commands.

To leave the ELS monitoring environment, enter the **exit** command.

ELS Monitoring Commands

This section summarizes and then explains all the ELS monitoring commands. After accessing the ELS Monitoring environment, you can enter ELS monitoring commands at the ELS> prompt.

Table 18. ELS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Resets to zero the counts of messages associated with specified events, groups, or subsystems.
Display	Enables message display on the console.
Exit	Exits the ELS console process and returns the user to GWCON.
Filter	Filter ELS messages based upon the net number.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to file at remote workstation.
Notrace	Disables trace event display on the console.
Notrap	Keeps messages from being sent out in SNMP traps to the network management workstation.
Remote	Allows messages to be logged at a file on a remote workstation.
Remove	Frees up memory by erasing stored information.
Restore	Clears current settings and reloads initial ELS configuration.
Retrieve	Reloads the saved ELS configuration.
Save	Stores the current configuration.
Set	Sets the pin parameter and the timestamp feature.
Statistics	Displays available subsystems and pertinent statistics.
Trace	Enables trace event display on the console.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Advanced

Use the **advanced** command to enter the advanced monitoring environment. In this environment you change message buffering operation.

Syntax:

advanced

Clear

Use the **clear** command to reset to zero the counts of the display, trace, trap, or remote commands as they relate to specific events, groups or subsystems.

Syntax:

clear event . . .

group . . .

subsystem . . .

event *subsystem. event#*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified event (*subsystem.event#*).

group *group.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified group (*group.name*).

subsystem *subsystem.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified subsystem (*subsystem.name*).

Display

Use the display command to enable the message display on the monitoring monitor for specific events.

Syntax:

display
event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Displays messages for the specified event (subsystem.event#).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Displays any messages associated with the specified subsystem (*logging level*). If you do not specify a logging level, all messages for that subsystem are turned on.

Files Trace TFTP

Use the **files trace tftp** command to retrieve trace files from the subdirectory associated with:

- The currently active bank (bank A or bank B on the hard disk)
- Bank A on the hard disk
- Bank B on the hard disk

- The trace file stored in the Network Subdirectory (if there is no active bank)

Syntax:

files trace tftp	active-bank ...
	bank-a ...
	bank-b ...
	net-subdir ...

You are prompted for the *remote server IP address* and the *remote path/file name*.

active-bank
Retrieves the traces file from the currently active bank

bank-a
Retrieves the trace file from bank A.

bank-b
Retrieves the trace file from bank B.

net-subdir
Retrieves the trace file stored in the Network Subdirectory (if there is no active bank).

Filter

Use the **filter** command to access the filter configuration command environment. See “ELS Net Filter Monitoring Commands” on page 189 for complete command details.

Syntax:

filter	net

List

Use the **list** command to get updated information regarding ELS settings and to get listings of selected messages.

Syntax:

list	all
	active . . .
	event . . .
	filter-status
	groups . . .
	pin
	remote-log status
	subsystem . . .
	trace-status

all Lists all subsystems, defined groups, enabled subsystems, enabled events, and pins.

ELS Monitoring Commands (Talk 5)

active *subsystem.name*

Displays the events that are active for a specific subsystem and the count of the occurrence of the messages.

Example:

```
list active ip

EventActiveCount
IP.00789354
ETH.009D10
Subsystem X25: no event active
```

If Remote logging is turned on, those events displayed as active for a subsystem will have an “R” next to their name.

event *subsystem.event#*

Displays the logging level, the message, and the count of the specified event.

Example:

```
list event ip.007

Level: p-TRACE
Message: source_ip_address -> destination_ip_address
Active:  Count: 84182
```

If Remote-logging had been activated for this event, and the *syslog_facility* and *syslog_level* values were log_daemon and log_crit, the last lines would look like:

```
Active:  R count:84182
Syslog Facility: log_daemon   Syslog Level: log_crit
```

filter-status

Lists ELS net number filters.

groups *group.name*

Displays the user-defined group names.

pin Lists the current number of ELS event messages sent per second in SNMP traps. This is a threshold value that can be used to reduce the amount of SNMP trap traffic.

Example:

```
list pin

Pin: 100 events/second
```

remote-log status

Lists the current values of the remote logging options set in the **set remote-logging** command.

Example:

```
list r

Remote Logging is On
Source Ip Address = 192.9.200.8
Remote  Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_USER
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 256
Remote Logging Local ID =  SPHINX
```

subsystem *subsystem.name*

Lists event names, the total number of events that have occurred, and their descriptions.

Note: Although ELS supports all subsystems on the router, not all devices support all subsystems. See *ELS Messages* for a list of currently supported subsystems.

subsystem *subsystem.name*
Lists all events, logging levels, and messages for the specified subsystem.

Example:

```
list subsystem eth

Event      Level      Message
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.002    UE-ERROR   rcv unkwn typ packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.010    C-INFO     LLC unk SAP DSAP source_Ethernet_address ->
                      destination_Ethernet_address nt network
```

subsystem all
Lists all events, logging levels, and messages for every event that has occurred on the router.

trace-status
Displays information on the status of packettracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
------------------------ Run-time Status ---------------------------
Packets in RAM Trace Buffer:1   Free Trace Buffer Memory:99958
Trace Errors:0  First Packet:1  Last Packet:1
Trace Records Stored on HD:8  Trace Buffer File Size:16560
HD-Shadowing Time Exceeded? NO Elapsed Time:  0 hr,  0 min, 10 sec
Has Stop Trace Event Occurred? NO
```

- “Trace Status” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs.
- “HD Shadowing” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs or when Time Limit is exceeded.
- “Trace Buffer File Size” will display “<wrapped>” when a wraparound has occurred in the trace file.
- If disk-shadowing time limit is exceeded, but there has not been a trace record written since the time expired, then“ HD-Shadowing Time Exceeded? NO <Next trace will turn it OFF>” will be displayed. When the next trace record has been written, then “HD-Shadowing Time Exceeded? YES” will be displayed.

`ELS Config>`**LIST TRACE** command under **talk 6** displays information similar to the following:

```
------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the displaying of messages for the specified event.

group *group.name*
Suppresses the displaying of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Suppresses the displaying of messages associated with the specified subsystem (*logging level*).

Noremote

Use the **noremote** command to select and turn off messages logging to a remote workstation.

Syntax:

noremote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.19, gw.20, gw.21, and g.22

subsystem *subsystem.name*
Suppresses the remote logging of messages associated with the specified subsystem (*logging level*).

Example:

```
noremote subsystem tkr
```

Note: With Noremote, there is no need to specify a Syslog Facility and Level, such as there is with Remote.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Notrace

Use the **notrace** command to stop display of selected trace events at the monitoring.

Syntax:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the display of the specified tracing event.

group *groupname*
Suppresses the display of tracing events related to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
notrace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname [logging-level]*
Suppresses the display of tracing events that are associated with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress tracing for all logging levels for the subsystem.

Example:

```
notrace subsystem frl error

notrace subsystem frl
```

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event. . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*
Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname [logging-level]*
Suppresses the sending of messages in SNMP traps that are associated with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress trapping for all logging levels for the subsystem.

Example:

```
notrap subsystem tkr error
```

Remote

Use the **remote** command to select the events to be logged to a remote file by event number, range of events, group, or subsystem.

Syntax:

remote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*

Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM 2212. They are merely identifiers which are used by the syslog daemon on the remote workstation.

Example:

```
remote event gw.019 log_user log_info
```

group *group.name syslog_facility syslog_level*

Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command”.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level*. See “the remote event command”.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely to the files specified by the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

subsystem *subsystem.name message_level syslog_facility syslog_level*
Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely based on the *syslog_facility* and *syslog_level*. See “the remote event command” on page 179.

Message_level is a value such as “ALL,” “ERROR,” “INFO,” or “TRACE” . See “Logging Level” on page 131. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem TKR all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely to files specified by log_user and log_info at the remote host.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Remove

Use the **remove** command to free up memory by erasing stored information. If you have previously saved the current configuration with the **save** command, remove allows you to erase the saved configuration.

Syntax:

remove

Restore

Use the **restore** command to clear all current settings (except counters) and reload the initial ELS configuration. To retain the current settings, use the **save** command before restoring the initial configuration.

Syntax:

restore

Retrieve

Use the **retrieve** command to reload the saved ELS configuration. If you have previously saved the current configuration with the **save** command, use **retrieve** to reload it. **Retrieve** does not erase the saved configuration after it executes. To erase the saved configuration, use the **remove** command.

Syntax:

retrieve

Save

Use the **save** command to store the current configuration (except counters). **Save** does not affect the default configuration (the one you set with the configuration commands). Use **save** after modifying the configuration with the monitoring commands with the intention of saving this configuration over a restart. There can be only one saved configuration at a time. To reload the saved configuration, use the **retrieve** command.

Syntax:

save

Set

Use the **set** command to set the maximum number of traps per second, to set the timestamp feature, or to set the tracing options.

Syntax:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number *max_traps* is sent every tenth of a second.)

remote-logging
Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
local_id
remote_ip_addr . . .
source_ip_addr ...

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the **remote** command will be prevented from being logged.

facility

Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

local_id

Specifies a 1-32 character identifier that appears in the remote logging message that you can use to identify which machine logged a particular message.

remote_ip_addr

This is an IP address of the remote host where the log files reside.

source_ip_addr

Specifies the IP address of the machine that originated the message that is being remotely-logged.

You should use an IP address that is configured in the 2212 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that

this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

timestamp

Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message, or to turn off message timestamping.

Note: If you turn on timestamping, you must remember to go back into the CONFIG process and set the router's date and time using the time command. Otherwise, all messages will come out with 00:00:00, or negative numbers in the hours, minutes, and/or seconds, for example 00:-4:-5.

Use the **set timestamp** command to enable one of the following timestamp options:

timeofday

Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime

Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle of uptime for the router. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

Syntax:

set timestamp	[timeofday or uptime or off]

trace Use the **set trace** command to configure tracing options. When tracing options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set trace	decode . . .
	default-bytes-per-pkt . . .
	disk-shadowing . . .
	max-bytes-per-pkt . . .
	memory-trace-buffer-size . . .
	off
	on

reset

stop-event . . .

wrap-mode . . .

decode [off or on]
Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing [[off or on] or [delete-file or *record-size* **or** *time-limit*]]
Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

[off or on]
Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it can no longer be viewed from the monitoring.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

Turns disk shadowing on or off and sets the maximum trace file size. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it is no longer viewable through the monitoring.

record-size *bytes*
Sets the record size for trace file records:

Valid Values: 1024, 2048, or 4096 bytes

Default: 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

delete-file
Deletes the trace file (in the subdirectory associated with the active bank only).

Note: If disk shadowing is ON when the command is issued, “ Disk-shadowing must be set to OFF before trace file can be deleted” is displayed and the file is not deleted.

time-limit *hours*
Sets the maximum time for disk-shadowing of traces:

Valid Values:
1 - 72 hours:

Default
24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

max-bytes-per-pkt *bytes*
Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*
Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

Example:

```
set trace stop-event TCP.013
```

wrap-mode *off/on*
Turns the trace buffer wrap mode on or off. When wrap mode is enabled and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Statistics

Use the **statistics** command to display a list of all of the available subsystems and their statistics.

Note: The following example may not match your display exactly. The output of the command depends on the version and release of the installed software.

Syntax:

statistics

Example:

```
statistics

Subsys  Vector  Exist   String  Active    Heap

  GW     105     101      3411     0         0
```

```
 FLT      20       7       184     0         0
 BRS      50       5       201     0         0
 ARP     150     142      7030     0         0
  IP     100     100      2463     2        20
ICMP      30      21       529     0         0
 TCP      60      57      2420     0         0
 UDP      10       6       179     0         0
 BTP      40      13       695     0         0
 RIP      30      22       474     0         0
OSPF      80      73      2859     0         0
MSPF      40      17       593     0         0
TFTP      35      29       819     0         0
SNMP      30      28       821     0         0
 DVM      30      21       589     0         0
  DN     140     115      5842     0         0
  XN      35      21       780     0         0
 IPX     110     110      4705     0         0
CLNP      80      58      1763     0         0
ESIS      40      24       716     0         0
ISIS      80      58      2422     0         0
DNAV      50      26      1314     0         0
 AP2      80      70      1755     0         0
ZIP2      60      51      1859     0         0
R2MP      50      38      1185     0         0
 VIN      90      79      3159     0         0
 SRT     120      94      5040     0         0
 STP      60      32      1590     0         0
  BR      50      30      1616     0         0
SRLY      30      28      1409     0         0
 ETH      60      47      1098     0         0
  SL      50      35       584     0         0
 TKR      60      45      2031     0         0
 X25      70      53      1909     0         0
FDDI      30      27      1155     0         0
SDLC     100      95      4263     0         0
 FRL     130      97      6068     0         0
 PPP     190     186      6394     0         0
X251      50      16       546     0         0
X252      50      34       996     0         0
X253      50      42      1649     0         0
ISDN      50      43      1994     0         0
IPPN      20       4       132     0         0
 WRS      40      33      1938     0         0
 LNM      70      60      3137     0         0
 LLC     170     168      9840     0         0
 BGP      80      74      2477     0         0
 MCF      15       9       244     0         0
 DLS     500     497     24340     0         0
 V25B     30      28      1058     0         0
 BAN      30      29      1223     0         0
 COMP     80      26      1050     0         0
 NBS     100      50      3029     0         0
 ATM     300     216     10808     0         0
 LEC     200     174      7258     0         0
APPN     100      28       467     0         0
ILMI     150      23       487     0         0
SAAL      30      26       621     0         0
 SVC      30      26       465     0         0
 LES     400     361     22333     0         0
LECS     150     145      5666     0         0

EVLOG      1       1       105     0         0
 NOT      25      15       508     0         0
NHRP     250     211      8193     0         0
 XTP      64      58      2271     0         0
 ESC     150      67      3122     0         0
 LCS      40      22       858     0         0
 LSA      70      61      3506     0         0
 MPC     130      30      1677     3        44
 SCSP     40      34      1234     0         0
ALLC      50      36      1842     0         0
 NDR      50      38      1150     0         0
 MLP     100      93      4006     0         0
 SEC      50      30       688     0         0
ENCR     100       4       194     0         0
  PM      25       6       120     0         0
```

```
 DGW      20       9       238     0         0
QLLC      55      54      2411     0         0

Total   6490    4942    215805     5        64

Maximum:7976 vector, 155 subsystem
Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys
```

Subsys
Name of subsystem

Vector
Maximum size of subsystem

Exist Number of events defined in this subsystem

String Number of bytes used for message storage in this subsystem

Active Number of active (displayed, trapped, or counted) events in the subsystem

Heap Dynamic memory in use by subsystem

Trace

Use the **trace** command to select the trace events to be displayed on the system monitoring.

Syntax:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the router monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the router monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the router.

View

Use the **view** command to view traced packets.

Syntax:

view current
first
jump
last

next

prev

search ...

current
Displays the current trace packet. If the current packet is not valid, the first packet in the trace buffer is displayed.

first Displays the first traced packet in the trace buffer.

jump *n*
Displays the traced packet *n* packets ahead of or behind the current packet.

last Displays the last traced packet in the trace buffer.

next Displays the next traced packet.

prev Displays the previous traced packet.

search *hexstring*
Displays the next traced packet that contains the specified hex string.

ELS Net Filter Monitoring Commands

This section describes explains the commands to manipulate ELS net filters. To enter the filter environment, enter the **filter net** command at the ELS> prompt. Enter the monitoring commands at the `ELS Filter net>` prompt.

Table 19. ELS Net Filter Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Create	Creates a filter and assigns it a number. A maximum of 64 filters is allowed.
Delete	Deletes a specified filter number or all filters.
Disable	Disables a specified filter number or all filters.
Enable	Enables a specified filter number or all filters.
List	Lists a specified filter number or all filters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Create

Use the **create** command to create an ELS net filter.

Syntax:

create *queue*

event *event_name net#_start net#_end*

range *event_range net#_start net#_end*

subsystem *subsystem_name net#_start net#_end*

queue The queue for which you are setting the filter. The valid queues are:

Display

Trace

Trap

Remote

event *event_name net#_start net#_end*
Specifies the event and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create trap event GW.009 2 10** filters traps for message GW.009 for net numbers 2 through 10.

range *event_range net#_start net#_end*
Specifies the range of ELS messages and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create remote range ipx 19 22 3 6** filters all ipx messages beginning with IPX.019 and ending with IPX.022 for net numbers 3 through 6 for remote logging.

subsystem *subsystem_name net#_start net#_end*
Specifies the subsystem and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create display subsys ip 1 1**, filters all ELS messages for the ip subsystem that contain net number 1 to the display. All other ip subsystem messages are discarded.

Delete

Use the **delete** command to delete a specific ELS filter or all ELS filters.

Syntax:

delete all
filter *filter#*

all Deletes all currently configured filters.

filter *filter#*
Deletes the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to delete.

Disable

Use the **disable** command to disable a specific ELS filter or all ELS filters.

Syntax:

disable all
filter *filter#*

all Disables all currently configured filters.

filter *filter#*
Disables the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to disable.

Enable

Use the **enable** command to enable a specific ELS filter or all ELS filters.

Syntax:

enable all
filter *filter#*

all Enable all currently configured filters.

filter *filter#*
Enable the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to enable.

List

Use the **list** command to list a specific ELS filter or all ELS filters.

Syntax:

list all
filter *filter#*

all Lists all currently configured filters.

filter *filter#*
Lists the filter specified by *filter#*.

ELS Message Buffering Monitoring Commands

Table 20 describes the commands available at the `ELS Config Advanced>` prompt.

Table 20. ELS Message Buffering Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Flush	Clears the message buffer and turns off logging to the message buffer.
List	Displays the operational settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Read-file	Reads a formatted message buffer from a file and displays it on the console.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Tftp	Sends the ELS message buffer to a file at a remote host.
View	Displays all or a specific number of messages in the message buffer. You can also control how the messages scroll off the screen.
Write-buffer	Writes the ELS message buffer to the hard file. The buffer is formatted before it is written. The file name on the hard file is always ELSADV.LOG.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Flush

Use the **flush** command to set logging off, clear the messages from the buffer, and release the buffer memory for other use by the system.

Syntax:

flush buffer

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Advanced> list status
-----------------------------------Configuration--------------------------------
Logging Status:    OFF       Wrap Mode:   ON    Logging Buffer Size:    8500 Kytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  APPN DUMP
-----------------------------------Run-Time Status------------------------------
Has Stop Condition Occurred ?     YES       Messages currently in buffer:         1222
```

See “Set” on page 194 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log event

group

range

subsystem

event *subsystem.event#*

Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*

Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event
group
range
subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Read-file

Use the **read-file** command to read formatted ELS messages from a file on the hard file, `ELSADV.LOG`, created by the **write-buffer** command.

Note: If you enter this command and a hard file is not available, you will receive a message indicating the drive is unavailable.

Syntax:

read-file

Set

Use the **set** command to change configured ELS message buffering options.

Syntax:

set logging [on or off]

stop action . . .

stop event *subsystem.event#*

stop string *text*

wrap [on or off]

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the "stop event" (and if specified, the "stop string") occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard file. If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified "stop action."

Logging remains stopped until the next time you issue the **set logging on** command or the router reboots.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**
Specifies the string to be used in conjunction with the “stop event” to stop logging. If you have not specified a stop event, the system ignores the “stop string.”

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the “stop string.”

Default value: none

wrap [on or **off]**
Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Tftp

Use the **tftp** command to send the ELS message buffer to a remote host as a formatted file.

Syntax:

tftp buffer [formatted] *dest_ip_address dest_filename*

file *dest_ip_address dest_filename*

buffer [formatted] *dest_ip_address dest_filename*
Specifies that the ELS message buffer is to be sent to the remote host indicated by *dest_ip_address* as file *dest_filename.* The buffer can be either formatted.

View

Use the **view** command to view all of the messages or a specific number of messages in the message buffer.

Syntax:

view all [scroll/noscroll]

last [scroll/noscroll *number*]

all *scroll/noscroll*
Displays all of the messages in the message buffer.

[scroll]
Specifies that the screen pauses until you hit the spacebar.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll
Specifies that the messages will scroll off the screen if the number of messages exceeds the screen length.

last *scroll/noscroll number*
Display the last *number* messages in the message buffer.

[scroll]
Specifies that the screen pauses after displaying a full screen of messages and waits for the user to hit the space bar to get the next screen.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll
Specifies that the messages will continuously scroll off the screen with no scroll control until either all messages in the buffer (or the last number of messages requested) have been displayed.

number
Specify a number from 1 to the total number of messages in the message buffer. To display the total number of messages in the buffer, use the **list status** monitoring command.

Write-buffer

Use the **write-buffer** command to write formatted ELS messages to the hard file.

Note: If you enter this command and a hard file is not available, you will receive a message indicating the drive is unavailable.

Syntax:

write-buffer

Chapter 14. Configuring and Monitoring Performance

This chapter describes how to use the Performance configuration and monitor operating commands and includes the following sections:

Performance Overview

Configuring performance allows you to monitor your CPU load. In the idle (non-work load) state, performance reflects operations that the router continuously performs as a part of managing external interfaces. The CPU load registered in the idle state is dependent upon:

- Number of protocols running.
- Number of interfaces/cards installed.
- Type of interfaces installed.

The performance function can be used as a tool for trend analysis, bottleneck evaluation, and capacity planning. By collecting the CPU utilization information on the router, a network manager can monitor:

- CPU load versus time of day.
- CPU load versus location of the router in the network.
- CPU load versus traffic throughput.
- CPU load versus user load (for example: TN3270 sessions, ISDN dial in clients)

Performance Reporting Accuracy

If you request a performance analysis when the 2212 first comes online, you will see values that reflect an initialization state that has little or no network traffic, so it is of little use in helping to balance your network load.

It is best to use performance reports that are generated under normal loads after approximately 2 minutes of operation.

Accessing the Performance Configuration Environment

Use the following procedure to access the Performance monitor configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, see "Chapter 8. The Configuration Process (CONFIG - Talk 6) and Commands" on page 65 .) For example:

```
* talk 6
Config>
```

After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the CONFIG prompt, enter the **perf** command to get to the `PERF Config>` prompt.

Performance Configuration Commands

To configure Performance, enter the commands at the `PERF Config>` prompt.

Table 21. PERF Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable cpu statistics

t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable cpu statistics

t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Accessing the Performance Monitoring Environment

Use the following procedure to access the Performance monitoring commands. This process gives you access to the Performance *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, see “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 111.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the + prompt, enter the **perf** command to get you to the `PERF Console>` prompt.

   Example:

   ```
   + perf
   PERF Console>
   ```

Performance Monitoring Commands

This section describes the Performance monitoring commands.

Table 22. PERF Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Clear	Clear the CPU utilization high water statistics and resets the reporting period to a new cycle.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Report	Displays a report of performance statistics.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable	cpu statistics
	t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable	cpu statistics
	t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Report

Use the **report** command to display performance monitor statistics.

Syntax:

report

Example:

```
PERF Console>report
-------------------------------------------------------------
KEY:  SW = Short Window = 9 seconds
KEY:  LW = Long Window =  9.0 minutes  (60 x SW)

  CPU UTIL :   Most recent SW                    = 38%
               Most recent LW                    = 33%
               Highest for all SW's              = 92%
               Highest for all LW's              = 52%
               % of time cpu util (SW) was > 60%  = 16%
               % of time cpu util (SW) was > 70%  = 15%
               % of time cpu util (SW) was > 80%  = 1%
               % of time cpu util (SW) was > 90%  = 0%
               % of time cpu util (SW) was > 95%  = 0%
-------------------------------------------------------------
```

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Part 3. Understanding, Configuring and Operating Interfaces

Chapter 15. Getting Started with Network Interfaces

The chapters of this book describe how to configure and monitor network interfaces and link layer protocols supported by the Router. The purpose of this chapter is to give you some basic configuration and monitoring guidelines. This chapter also provides you with basic procedures and information needed for monitoring the interfaces via the GWCON **interface** command. This chapter includes the following sections:

Before You Continue

Before you continue, make sure that you have familiarized yourself with the procedures necessary for accessing the network interface configuration processes.

For more information on these procedures, refer to the sections that follow in this chapter.

Network Interfaces and the GWCON Interface Command

When configuring network interfaces, you may find it necessary to display certain information about specific interfaces. While some interfaces have their own console processes for monitoring purposes, the router displays statistics for *all* installed network interfaces when you use the **interface** command from the GWCON environment. (Refer to "Interface" on page 119.)

Accessing Network Interface Configuration and Console Processes

The follow references contain the background information and examples of how to access the configuration and console prompts for interfaces.

Refer to "Accessing Network Interface Configuration and Operating Processes" on page 18 , "Accessing the Network Interface Configuration Process" on page 18, and "Accessing the Network Interface Console Process" on page 21 for complete information on accessing interface configuration and console processes. Accessing these processes allows you to change and monitor software configurable parameters for network interfaces used in your router.

Accessing Link Layer Protocol Configuration and Console Processes

Refer to “Chapter 1. Getting Started” on page 3 for complete information on accessing the protocol configuration and console processes. Accessing these processes allows you to change and monitor configurable parameters for Link Layer protocols supported by your router.

Defining Spare Interfaces

There may be occasions when you will need to define interfaces on your device that do not currently exist. You accomplish this ***dynamic reconfiguration*** of a device by defining spare interfaces while you are configuring the device and then using the console process to activate the interfaces when they are present. See “Configuring Spare Interfaces” on page 68 and “Activate” on page 112 for details.

Chapter 16. Configuring IEEE 802.5 Token-Ring Network Interfaces

This chapter describes Token-Ring interfaces configuration and operational commands. It includes the following sections:

Accessing the Token-Ring Interface Configuration Process

To display the `TKR config>` prompt, enter the network command followed by the interface number of the Token-Ring interface. For example:

```
Config>network 0
Token-Ring interface configuration
TKR Config>
```

Use the **list devices** command at the `Config>` prompt to display a list of interface numbers configured on the router.

Note: Whenever you change a parameter, you must restart the router for the changes to take effect.

Token-Ring Configuration Commands

This section describes the Token-Ring configuration commands. Enter the commands at the `TKR config>` prompt. Table 23 lists Token-Ring configuration commands.

Table 23. Token-Ring Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
List	Displays the selected Token-Ring interface configuration.
LLC	Accesses the LLC configuration environment and subcommands.
Packet-size	Changes packet-size defaults for all Token-Ring networks.
Set	Sets the aging timer for the RIF cache and the physical (MAC) address.
Source-routing	Enables or disables source-routing on the interface.
Speed	Sets the interface speed in Mbps.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

List

Use the **list** command to display the current configuration for the Token-Ring interface.

Note: If the MAC address is 0, the default station address is used.

Syntax:

list

Example:

```
list
Token-Ring configuration:

    Packet size (INFO field): 2052
Speed:                    16 Mb/sec

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
```

Packet size
Size of the Token-Ring packet.

Speed Speed of the network.

RIF Aging Timer
Amount of time that the router holds the information contained in the Routing Information Field (RIF).

Source Routing
Status of the source-routing feature, enabled or disabled.

MAC Address
Configured MAC address that was set with the **set physical-address** command. If all zeros are displayed, the MAC address is the default address.

LLC

Use the **LLC** command to access the LLC configuration environment. See “LLC Configuration Commands” on page 217 for an explanation of each of these commands.

Syntax:

llc

Note: If APPN is not included in your router software load, you will receive the following message if you try to use this command:

```
LLC configuration is not available for this network.
```

The LLC configuration environment is only available if APPN is included in the software load.

Packet-Size

Use the **packet-size** command to change maximum packet-size for all Token-Ring networks. Enter the **packet-size** command followed by the desired number of bytes.

Syntax:

packet-size *bytes*

Table 24. Token-Ring 4/16 Valid Packet Sizes

Network Data Speed	Values (# of bytes)
4 Mbps	516 to 4498 **Note:** If a value greater than 4498 is defined for a 4 Mb TR then the software will set it to 4498. If the user does not specify a value, then the default is 2052.
16 Mbps	516 to 18144 **Note:** If you do not specify a value, then the default is 2052.

Note: If packet sizes are increased, buffer memory requirements will also increase.

Set

Use the **set** command to set the Routing Information Field (RIF) timer and the physical (MAC) address.

Syntax:

set physical-address

rif-timer

physical-address

Indicates whether you want to define a locally administered address for the Token-Ring interface's MAC sublayer address, or use the default factory station address (indicated by all zeroes). The MAC sublayer address is the address that the Token-Ring interface uses to receive and transmit frames.

Note: Pressing **Return** leaves the value the same. Entering **0** and pressing **Return** causes the router to use the factory station address. The default is to use the factory station address.

Valid values: Any 12-digit hexadecimal address.

Default value: burned-in address (indicated by all zeroes).

Example:

```
set physical-address
MAC address in 00:00:00:00:00:00 form []?
```

rif-timer

Sets the maximum amount of time (in seconds) that the information in the RIF is maintained before it is refreshed. The default is 120.

Example:

```
set rif-timer
RIF aging timer value [120]?  120
```

Source-routing

Use the **source-routing** command to enable or disable end station source routing. Source routing is the process by which end stations determine the source route to use to cross source routing bridges. Source routing allows the IP, IPX, and AppleTalk Phase 2 protocols to reach nodes on the other side of the source routing bridge.

This switch is completely independent of whether this interface is providing source routing via the SRT forwarder. The default setting is enabled.

Some stations cannot properly receive frames with a Source Routing RIF on them. This is especially common among NetWare drivers. Disabling source routing in this situation will allow you to communicate with these stations.

Source routing should be enabled only if there are source-routing bridges on this ring that you want to bridge IP, IPX, and AppleTalk Phase 2 packets through. Source routing must also be enabled so LLC test response messages can be returned.

Syntax:

source-routing	enable
	disable

Speed

Use the **speed** command to change data speed. The default speed is autosense (AUTO).

Syntax:

speed *speed-value*

speed-value

The speed to which you are setting the token-ring interface.

Valid values:

- A - AUTO
- B - 4 Mbps
- C - 16 Mbps

Note: If you specify AUTO, the adapter will open at the current ring speed. However, if this adapter is the only adapter on the ring with autosense speed configured and no ring speed was established at open, the adapter will not open. The open failure prevents the adapter from setting an incorrect ring speed.

Default value: Autosense

Accessing the Interface Monitoring Process

To display the Token-Ring monitoring prompt (TKR>), enter the network command followed by the interface number of the Token-Ring interface. For example:

```
+network 0
TKR>
```

Use the **list devices** command at the Config> prompt to display a list of interface numbers configured on the router.

Follow the procedure described in “Accessing the Network Interface Configuration Process” on page 18 to access the interface monitoring process for the interface described in this chapter. Once you have accessed the desired interface monitoring process, you can begin entering monitoring commands.

Token-Ring Interface Monitoring Commands

This section summarizes the Token-Ring monitoring commands. Enter commands at the TKR> monitoring prompt. Table 25 lists the monitoring commands.

Table 25. Token-Ring Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Dump	Displays a dump of the RIF cache.
LLC	Displays the LLC monitoring prompt.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Dump

When source routing is enabled in the tkr config> process, you can use the **dump** command to request a dump of the RIF cache contents.

Syntax:

dump

Example:

```
dump
MAC address    State     Usage   RIF
0000C90B1A57   ON_RING   Yes     0220
```

MAC address
Displays the MAC address of the Token-Ring interface.

State Displays one of the interface states:

On_ring - indicates that a RIF was found for a node on the ring.

Have_route - indicates that a RIF was found for a node on a remote ring.

No_route - is displayed for a brief period of time as an explorer frame is sent out and the router is waiting for a return.

Discovering - indicates that the router sent an explorer frame to rediscover the RIF.

St_route - indicates that a route obtained from a Spanning tree explorer.

Usage Indicates that a RIF was used in a packet. The number is arbitrary and has no functional significance.

RIF Displays a code that indicates the RIF in hexadecimal.

Note: The RIF is displayed only if Source Route Bridging is enabled on the Token-Ring interface.

- NetBIOS RIF data can be displayed using the following sequence of commands: **talk 5, protocol ASRT, name-caching, list cache rifs.**
- Data Link Switching RIF data can be displayed using the following sequence of commands: **talk 5, protocol dlsw, list llc2 session all.**

LLC

Use the **LLC** command to access the LLC monitoring prompt. LLC commands are entered at this new prompt. See “LLC Monitoring Commands” on page 221 for an explanation of each of these commands.

Syntax:

llc

Token-Ring Interfaces and the GWCON Interface Command

While Token-Ring interfaces have their own monitoring processes for monitoring purposes, the router also displays complete statistics for installed network interfaces when you use the **interface** command from the GWCON environment.

Statistics Displayed for 802.5 Token-Ring Interfaces

The following statistics display when you enter the **interface *<net#>*** command for a Token-Ring interface from the GWCON environment.

```
                                          Self-Test  Self-Test  Maintenance
Nt Nt'  Interface  Slot-Port              Passed     Failed     Failed
4  4    TKR/0      Slot: 5  Port: 1           1          0          0

  Token-Ring/802.5 MAC/data-link on IBM Mezzanine Token-Ring interface

  Physical address        0004AC4C8D05
  Microcode Level         PX13CB
  Configured speed        Autosense
  Network speed           16 Mbps
  Network duplex          Half-Duplex
  Max packet size (INFO)  2052
  Handler state           Ring open
  Last Reported Ring status  SERR | CO
  # times Signal lost        0    # times Beaconing          0
  Hard errors                0    Lobe wire faults          0
  Auto-removal errors        0    Removes received          0
  Ring recovery actions      0    Soft Errors               0

  Line errors                0    Burst errors              0
  ARI/FCI errors             0    Inputs dropped            0
  Frame copy errors          0    Token errors              0
  Lost frames                0    Output Underrun           0
  Input overflows            0    Driver output errors      0
```

The following section describes general interface statistics:

Nt Global interface number

Nt’ Applies only to dial circuits

Interface
Interface name and Number of this interface within interfaces of type “intrfc”

Port Port number

Slot Slot number

Self-Test: Pass
Number of times self-test succeeded

Self-Test: Fail
Number of times self-test failed

Maint: Fail
Number of maintenance failures

The following section describes the statistics displayed that are specific to the Token-Ring interfaces:

Physical address
Specifies the physical address of the Token-Ring interface.

Configured speed
The speed configured for the adapter.

Network speed
Specifies the speed of the Token-Ring network that connects to the interface. The Network Speed counter displays the number of packets that the interface can pass per second.

Network duplex
The duplex mode of the adapter.

Max packet size (info)
Displays the maximum packet size configured for that interface. The Max Packet Size counter displays the maximum length, in bytes, of a packet that the interface transmits or receives. This counter is user-defined.

Handler state
Displays the current state of the Token-Ring handler. The Handler state counter displays the state of the handler after the self-test runs.

Last ReportedRing status
Last Ring Status of the Token Ring interface.

SIGL SIGNAL_LOSS The interface has detected a loss of signal on the ring.

HERR HARD_ERROR The interface is presently transmitting or receiving beacon frames on the ring.

SERR SOFT_ERROR The interface has transmitted a report error MAC frame.

BEAC TRANSMIT_BEACON The interface is transmitting beacon frames to or from the ring.

LWF LOBE_WIRE_FAULT The interface has detected an open or short circuit in the cable between the interface and the wiring concentrator. The interface is closed and is at the state following initialization.

ARMV AUTO_REMOVAL_ERROR The interface has failed the lobe wrap test, which resulted from the beacon auto-removal process, and has removed itself from the ring. The interface has closed and is at the state following initialization.

RMVD REMOVED_RECEIVED The interface has received a remove ring station MAC frame request and has removed itself from the ring. The interface is closed and is at the state following initialization.

CO COUNTER_OVERFLOW One of the following error counters has incremented from 254 to 255: Line, ARI/FCI, Frame Copy, Lost Frames, Burst, Lobe wire faults, Removes received. This display shows these error counters.

SSTA SINGLE_STATION The interface has sensed that it is the only station on the ring.

RR RING_RECOVERY The interface observes claim Token MAC frames on the ring. The interface may be transmitting the claim Token frames. This status remains until the interface transmits a ring purge frame.

# of times signal lost
Specifies the total number of times that the router was unable to transmit a packet due to loss of signal.

Hard errors
Displays the number of times the interface transmits or receives beacon frames from the network.

Auto-removal errors
Displays the number of times the interface, due to the beacon auto-removal process, fails the lobe wrap test and removes itself from the network.

Ring recovery actions
Displays the number of times the interface detects claim token medium access control (MAC) frames on the network.

Soft Errors
Displays the number of Soft Error Report MAC frames the interface has transmitted.

Line errors
The Line Errors counter increments when a frame is repeated or copied and the Error Detected Indicator (EDI) is zero for the incoming frame:

One of the following conditions must also exist:

- A token with a code violation exists.
- A frame has a code violation between the starting and ending delimiter.
- A Frame Check Sequence (FCS) error occurs.

ARI/FCI errors
The ARI/FCI (Address Recognized Indicator/Frame Copied Indicator) Errors counter increments if the interface receives either of the following:

An Active Monitor Present (AMP) MAC frame with the ARI/FCI bits equal to zero and a Standby Monitor Present (SMP) MAC frame with the ARI/FCI bits equal to zero.

More than one SMP MAC frame with the ARI/FCI bits equal to zero, without an intervening AMP MAC frame.

This error indicates that the upstream neighbor copied the frame but is unable to set the ARI/FCI bits.

Frame copy errors
Displays the number of times the interface in receive/repeat mode recognizes a frame addressed to its specific address but finds the address recognize indicator (ARI) bits not equal to zero. This error indicates a possible line hit or duplicate address.

Lost frames
Displays the number of times the interface is in transmit mode (stripping) and fails to receive the end of a transmitted frame.

Output Underruns
Displays the number of times the transmit channel FIFO queue is empty

when the network logic requires data for the ring.

Input overflows
Specifies the number of frames that were received that were larger than the input buffer size. Frames that are too large to fit into a single input buffer are discarded.

 # times beaconing
Displays the number of times the interface transmits a beacon frame to the network.

Lobe wire faults
Displays the number of times the network detects an open or short circuit in the cable between the interface and the wiring concentrator.

Removes received
Displays the number of times the interface receives a remove ring station MAC frame request and removes itself from the network.

Burst errors
Displays the number of times the interface detects the absence of transitions for five half-bit times between the start delimiter (SDEL) and the end delimiter (EDEL) or between the EDEL and the SDEL.

Inputs dropped
Displays the number of times an interface in repeat mode recognizes a frame addressed to it but has no buffer space available to copy the frame.

Token errors
The token errors counter increments when the active monitor detects a token protocol with any of the following errors:

The MONITOR_COUNT bit of token with nonzero priority equals one.

The MONITOR_COUNT bit of a frame equals one. No token or frame is received within a 10-ms window.

The starting delimiter/token sequence has a code violation in an area where code violations must not exist.

Chapter 17. Configuring and Monitoring LLC Interfaces

This chapter describes how to configure specific LLC interfaces in the router by using either the interface commands or the GWCON interface command.

Logical Link Level can be thought of as a “sub-protocol”. It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (monitoring) environment. Instead, it is accessed from the Token Ring, Point-to-Point (PPP), or Frame Relay protocols by entering an **LLC** command.

This chapter includes the following sections:

Accessing the Interface Configuration Process

Access the configuration commands for the protocol you wish to configure over LLC:

- Token Ring, as described in “Chapter 16. Configuring IEEE 802.5 Token-Ring Network Interfaces” on page 207
- Point-to-Point, as described in “Chapter 27. Using Point-to-Point Protocol Interfaces” on page 371
- Frame Relay, as described in “Chapter 25. Using Frame Relay Interfaces” on page 309

Each of these prompt levels has an LLC command. Enter **LLC** to access the LLC configuration commands and perform LCC configuration. When you are finished, enter **Exit** to return to the prompt level for the protocol you are configuring.

LLC Configuration Commands

LLC configuration is required when you need to pass packets over an SNA network. To enter these commands, you must first enter the LLC configuration environment (see “Accessing the Token-Ring Interface Configuration Process” on page 207).

This section summarizes and then explains all of the LLC configuration commands. These commands, shown in Table 26, enable you to configure LLC when you need to pass packets over a SNA network.

Table 26. LLC Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
List	Displays the selected LLC configuration.
Set	Sets the timers associated with LLC, and the size of the transmit and receive windows.

Table 26. LLC Configuration Command Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

List

Use the **list** command to display the current configuration for the LLC.

Syntax:

list

Example:

```
list
Reply Timer (T1):                 1 seconds
Receive ACK Timer (T2):           100 milliseconds
Inactivity Timer (Ti):            30 seconds
Max Retry value (N2):             8
Rcvd I-frames before ACK (N3):    1
Transmit Window (Tw):             2
Receive Window (Rw):              2
Acks needed to increment Ww (Nw): 1
```

Reply Timer (T1)
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station.

Receive ACK Timer (T2)
This timer is used to delay sending of an acknowledgment for a received I-format frame.

Inactivity Timer (Ti)
This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 retry count is exceeded. Default is 30 seconds.

Max Retry value (N2)
The maximum number of retries by the LLC protocol. Default is 8.

Rcvd I-frames before ACK (N3)
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. This counter sets a specified value and decrements each time an I-frame is received. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1.

Receive Window (Rw)
Indicates the maximum number of unacknowledged sequentially numbered I-frames that an LLC can receive from a remote host.

Transmit Window (Tw)
Indicates the maximum number of I-frames that can be sent before receiving an RR.

Acks needed to increment Ww (Nw)
This field is set to a default value of 1.

Set

Use the **set** command to configure the LLC.

Attention: Changing LLC parameters from the defaults can affect how the LLC protocol works.

Syntax:

set n2-max-retry *count*
n3-frames-rcvd-before-ack *count*
nw-acks-to-inc-window *count*
rw-receive-window *count*
t1-reply-timer *seconds*
t2-receive-ack-timer *seconds*
ti-inactivity-timer *seconds*
tw-transmit-window *count*

n2-max-retry
The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

Example:

```
set n2-max-retry
Max Retry value (N2) [8]?
```

n3-frames_rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value decrements. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

Example:

```
set n3-frames_rcvd-before-ack
Number I-frames received before sending ACK(N3) [1]?
```

rw-receive-window
Indicates the maximum number of unacknowledged sequentially numbered I-frames that an LLC can receive from a remote LLC peer. This value must be equal to or less than 127.

Example:

```
set rw-receive-window
Receive Window (Rw), 127 Max. [2]?
```

nw-acks-to-inc-ww
This field is set to a default value of 1.

t1-reply-timer
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

Example:

```
set t1-reply-timer
Reply Timer (T1) in sec. [1]?
```

t2-receive-ack-timer

This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received. The timer is reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Example:

```
set t2-receive-ack-timer
Receive Ack timer (T2) in 100 millisec. [1]?
```

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames_rcvd-before-ack** =1).

ti-inactivity-timer

This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 retry count is exceeded. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

Example:

```
set ti-inactivity-timer
Inactivity Timer (Ti) in sec. [30]?
```

tw-transmit-window

Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Example:

```
set tw-transmit-window
Transmit Window (Tw), 127 Max. [2]?
```

Accessing the Interface Monitoring Process

Access the monitoring commands for the protocol you wish to monitor over LLC:

- Token Ring, as described in “Chapter 16. Configuring IEEE 802.5 Token-Ring Network Interfaces” on page 207
- Point-to-Point, as described in “Chapter 28. Configuring and Monitoring Point-to-Point Protocol Interfaces” on page 387
- Frame Relay, as described in “Chapter 26. Configuring and Monitoring Frame Relay Interfaces” on page 327

Each of these prompt levels has an LLC command. Enter **LLC** to access the LLC monitoring commands to monitor LCC. When you are finished, enter **Exit** to return to the prompt level for the protocol you are monitoring.

LLC Monitoring Commands

This section summarizes and then explains all of the LLC monitoring commands. These commands, shown in Table 27, let you monitor the LLC while passing packets over an SNA network.

Table 27. LLC Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Clear-counters	Clears all statistical counters.
List	Displays interface, SAP, and session information.
Set	Allows the user to dynamically configure LLC parameters that are valid for the life of the session.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Clear-Counters

Use the **clear-counters** command to clear all the LLC statistical counters.

Syntax:

clear-counters

List

Use the **list** command to display interface, service access point (SAP), and session information.

Syntax:

list interface
sap . . .
session

interface
Displays all SAPs opened on this interface.

Example:

```
list interface
SAP      Number of Sessions
F4       1
```

sap sap_number
Displays information for the specified SAP on the interface.

Example:

```
list sap
SAP value in hex (0FE) [1]? F4

Interface                       0, TKR/0
Reply Timer(T1)                 1 sec
Receive ACK Timer (T2)          100 millisec
Inactivity Timer (Ti)           30 sec
MAX Retry Value (N2)            8
MAX I-field Size (N1)           2052
Rcvd I-frames before ACK (N3)   1
Transmit Window Size (Tw)       2
Acks Needed to Inc Ww (Nw)      1
```

```
Frame                          Xmt   Rcvd
UI-frames                      4     5
TEST-frames                    0     1
XID-frames                     0     0
I-frames                       291   26
RR-frames                      81    291
RNR-frames                     0     0
REJ-frames                     0     0
SABME-frames                   1     0
UA-frames                      0     1
DISC-frames                    0     0
DM-frames                      0     0
FRMR-frames                    0     0
I-frames discarded by LLC            0
I-frames Refused by LLC user         0

Cumulative number of sessions        1
Number of active sessions            1

Session ID                                          Remote
(int-sap-id)   Local MAC           Remote MAC          SAP   State
00F40000     00:00:C9:08:41:DB   10:00:5A:F1:02:37   F4    OPENED
```

SAP value in hex (0FE)
The SAP value of the session.

Interface
The interface number and type over which the session is running.

Reply Timer (T1)
Indicates the time it takes for this timer to expire when the LLC fails to receive an acknowledgment or response from the other LLC station.

Receive ACK Timer (T2)
Indicates the time delay the LLC uses before sending an acknowledgment for a received I-frame.

Inactivity Timer (Ti)
Indicates the time the LLC waits during inactivity before issuing an RR.

MAX Retry Value (N2)
The maximum number of retries by the LLC protocol.

MAX I-field Size (N1)
Maximum amount of data (in bytes) allowed in the I-field of an LLC2 frame.

Rcvd I-frame before ACK (N3)
Indicates the value that is used with T2 timer to reduce acknowledgment traffic for received I-frames.

Transmit Window Size (Tw)
Indicates the maximum number I-frames that can be sent before receiving an RR.

Acks Needed to Inc Ww (Nw)
This field is set to a default value of 1.

Frames Xmt and Rcvd
Counter that displays the total number of frame types transmitted (Xmt) and (Rcvd).

I-frames discarded by LLC
Counter that displays the total number of I-frames discarded by the LLC, usually because the sequence number is out of sequence.

I-frames refused by LLC user
Counter that displays the number of I-frames discarded by the software above the LLC. For example, DLSw (Data Link Switching).

Cumulative number of sessions
The total number of sessions that were opened over this SAP.

Number of active sessions
The total number of currently active sessions that are running over the interface.

Session ID (int-sap-id)
The session ID for the monitoring interface.

Local MAC
The router's LLC MAC address.

Remote MAC
The remote LLC's MAC address.

Remote SAP
The remote SAP of the LLC connection.

Remote State
The finite state(s) that results from interaction between the LLC peers. There are 21 states that are described below.

Link_Closed
The remote LLC peer is not known to the local LLC peer and is considered as not existing.

Disconnected
The local LLC peer is known to the other peer. This LLC peer can send and receive XID, TEST, SABME, and DISC commands; and XID TEST, UA, and DM responses.

Link_Opening
The state of the local LLC peer after sending a SABME or UA in response to a received SABME.

Disconnecting
The state of the local LLC after sending a DISC command to the remote LLC peer.

FRMR_Sent
The local LLC peer has entered the frame reject exception state and has sent a FRMR response across the link.

Link_Opened
The local LLC peer is in the data transfer phase.

Local_Busy
The local LLC peer is unable to receive additional I-frames.

Rejection
A local LLC peer that has received one or more out-of-sequence I-frames.

Checkpointing
The local LLC peer has sent a poll to the remote LLC peer and is waiting for an appropriate response.

CKPT_LB
A combination of checkpointing and local busy states.

CKPT_REJ
A combination of the checkpointing and rejection states.

Resetting
The local LLC peer has received a SABME and is reestablishing the link.

Remote_Busy
The state that occurs when an RNR is received from the remote LLC peer.

LB_RB
A combination of local_busy and remote_busy states.

REJ_LB
A combination of rejection and local_busy states.

REJ_RB
A combination of rejection and remote_busy states.

CKPT_REJ_LB
A combination of checkpointing, rejection, and local_busy states.

CKPT_CLR
A combination state resulting from the termination of a local_busy condition while the LLC peer is CKPT_LB.

CKPT_REJ_CLR
A combination state resulting from the transfer of an unconfirmed local busy clear while the link station is in the CKPT_REJ_LB state.

REJ_LB_RB
A combination of the rejection, local_busy, and remote_busy states.

FRMR_Received
The local LLC peer has received an FRMR response from the remote LLC peer.

Session
Displays information on the specified LLC session that is open on the interface.

Example:

```
list session
Session Id: [0]? 00-F4-0000

Interface0,                     TKR/0
Remote MAC addr                 10:00:5A:F1:02:37
Source MAC addr                 00:00:C9:08:35:47
Remote SAP                      F4
Local SAP                       F4
RIF                             (089E 0101 0022 0010)
Access Priority                 0
State                           LINK_OPENED
Replay Timer                    1 sec
Receive ACK Timer (T2)          100 millisec
Inactivity Timer (Ti)           30 sec
MAX I-field Size (N1)           2052
MAX Retry Value (N2)            8
Rcvd I-frames before ACK (N3)   1
Transmit Window Size (Tw)       2
Working Transmit Size (Ww)      2
Acks Needed to Inc Ww (Nw)      1
Current Send Seq (Vs)           9
Current Rcv Seq (Vr)            7
Last ACK'd sent frame (Va)      9
No. of frames in ACK pend q     0
No. of frames in Tx pend q      0
Local Busy                      NO
Remote Busy                     NO
Poll Retry count                8
Appl output flow stopped        NO
Send process running            YES

Frame                            Xmt   Rcvd
I-frames                         1456  2678
```

```
RR-frames                       502   403
RNR-frames                      0     0
REJ-frames                      0     0
I-frames discarded by LLC             0
I-frames Refused by LLC user          0
```

Session Id
Indicates the session ID number.

Interface
Indicates the number of the interface over which this session is running.

Remote MAC addr
Indicates the MAC address of the remote LLC peer.

Source MAC addr
Indicates the MAC address of the local LLC.

Remote SAP
The remote side SAP of the LLC connection.

Local SAP
The local side SAP of the LLC connection.

RIF The actual RIF of the frame.

Access Priority
Priority of the packet. 07 for upper layer control.

State The finite state(s) that results from interaction between the LLC peers. Refer to the **list sap** command on page 221 for more information.

Receive ACK timer (T2)
Indicates the time delay the LLC uses before sending an acknowledgment for a received I-frame.

Inactivity timer (Ti)
Indicates the time the LLC waits during inactivity before issuing an RR.

MAX I-field size (N1)
Maximum size of the data field (in bytes) of a frame. Default is the size of the interface.

MAX Retry Value (N2)
The maximum number of times the LLC transmits an RR without receiving an acknowledgment

Rcvd I-frames before ACK (N3)
Indicates the value that is used with T2 timer to reduce acknowledgment traffic for received I-frames.

Transmit window size (Tw)
Indicates the maximum number of I-frames that can be sent before receiving an RR.

Working transmit size (Ww)
The maximum number of I-frames that are sent before receiving an RR.

Acks Needed to Inc Ww (Nw)
This field is set to a default value of 1.

Current send seq (Vs)
Send state variable (Ns value for the next I-frame to be transferred).

Current Rcv seq (Vr)
Receive state variable (next in-sequence Ns to be accepted).

Last ACK'd sent frame (Va)
Acknowledged state variable (last valid Nr received).

No. of frames in ACK pend q
Number of transmitted I-frames waiting for acknowledgment.

No. of frames in transmit pend q
Number of frames waiting to be transmitted.

Local Busy
The local side of the LLC connection is sending RNRs.

Remote Busy
The remote side of the LLC is receiving RNRs.

Poll Retry count
Indicates the current value of the retry of the counter (counts down) in the LLC protocol.

Appl output flow stopped
The LLC has told the application to stop giving it outgoing data frames.

Send process running
This process runs concurrently with all other frame actions and takes I-frames in the transmit queue and sends them.

Frames Xmt and Rcvd
Displays the total number of frame types transmitted (Xmt) and (Rcvd).

I-frames discarded by LLC
Counter that displays the total number of I-frames discarded by the LLC, usually because the sequence number is out of sequence.

I-frames refused by LLC user
Counter that displays the number of I-frames discarded by the software above the LLC. For example, DLSw (Data Link Switching).

Set

Use the **set** command to dynamically configure the LLC parameters on a current LLC session. Any changes that you make to the parameters are effective for the life of session. These parameters are the same as those listed in "Set" on page 219.

Attention: Changing LLC parameters from the default can affect how the LLC protocol works.

Syntax:

set n2-max_retry *count*
n3-frames-rcvd-before-ack *count*
nw-acks-to-inc-ww *count*

t1-reply-timer *seconds*

t2-receive-ack-timer *seconds*

ti-inactivity-timer *seconds*

tw-transmit-window *seconds*

n2-max_retry
The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

n3-frames-rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value is decremented. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

nw-acks-to-inc-ww
This field is set to a default value of 1.

t1-reply-timer
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

t2-receive-ack-timer
This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received and reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer
This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 timer expires. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

tw-transmit-window
Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Chapter 18. Using the 10/100 Mbps Ethernet Network Interface

This chapter describes how to use the 10/100 Mbps Ethernet interface. It includes the following section:

- "Displaying 10/100 Mbps Ethernet Statistics"

Displaying 10/100 Mbps Ethernet Statistics

You can use the **interface** command from the GWCON environment to display the following statistics.

```
+i 0
                                          Self-Test  Self-Test Maintenance

Nt  Nt'  Interface Slot-Port                 Passed     Failed      Failed
0   0    Eth/0     Slot: 1   Port: 1            1          0           0

  Ethernet/IEEE 802.3 MAC/data-link on 100MB Ethernet interface

  Physical address         10005A991431
  PROM address             10005A991431
  Actual address           10005991431
  Adapter Level            DE
  Configured Duplex         : Auto-Negotiation
  Actual Duplex             : Half Duplex
  Configured Speed          : Auto-Negotiation
  Actual Speed              : 100 Mbps

  Input statistics:
   failed, packet too long           0   failed, CRC error           0
   failed, alignment error           0   failed, receive Overflow    0
  *receive collision                 0  *missed frame               0
 **frames filtered                   0   receive underrun            0

   Output statistics:
   one retry                         0   single collision            0
   multiple collisions               0   failed, transmit underflow  0
   failed, excess collisions         0   failed, loss of carrier     0
   late collisions                   0   more than one retry         0
   buffer error                      0   total collisions            0
   excessive deferal                 0   deferred                    0
   memory error                      0

  * cannot be cleared
 ** cleared automatically when read
```

These statistics have the following meaning:

Nt Global network number.

Nt′ This field is for the serial interface card. Disregard the output.

Interface
Interface name and its instance number.

Self-Test: Passed
Number of self-tests that succeeded.

Self-Test: Failed
Number of self-tests that failed.

Maintenance: Failed
Number of maintenance failures.

Physical address
The Ethernet address of the device currently in use. This may be the PROM address or an address overwritten by some other protocol.

PROM address
The permanent unique Ethernet address in the PROM for this Ethernet interface.

Actual address

Adapter level

Configured duplex
The value configured for duplex. Values can be Half Duplex, Full Duplex, or Auto-Negotiation.

Actual duplex
The value at which the adapter is presently operating. It might be different from the value configured, depending on the switch capability. If the adapter is not Up, the value displayed will be ″Unknown″. Otherwise the value can be Half Duplex or Full Duplex.

Note: The value indicated here might not be accurate. This is due to the implementation of the negotiation and link signaling support in the manufacturer's products.

Configured speed
The value configured for speed. Values can be 10 Mbps, 100Mbps, or Auto-Negotiation.

Actual speed
The speed at which the adapter is presently operating. It might be different from the speed configured, depending on the switch capability. If the adapter is not Up, the value displayed will be ″Unknown″. Otherwise the value can be 10 Mbps or 100 Mbps.

Note: The value indicated here might not be accurate. This is due to the implementation of the negotiation and link signaling support in the manufacturer's products.

Input statistics:

failed, packet too long or failed, frame too long
The Failed, Packet Too Long counter increments when the interface receives a packet that is larger than the maximum size of 1518 bytes for an Ethernet frame. This data is exported via SNMP as the dot3StatsFrameTooLongs counter.

failed, CRC error or failed, FCS (Frame Check Sequence) error
The Failed, CRC (Cyclic Redundancy Check) Error counter increments when the interface receives a packet with a CRC error. This data is exported via SNMP as the dd3StatsFCSErrors counter.

failed, alignment error
The Failed, Framing Error counter increments when the interface receives a packet where the length in bits is not a multiple of eight.

failed, receive overflow
Overflow error indicates that the receiver has lost all or part of the incoming frame, due to an inability to move data from the receive FIFO into memory buffer before the internal FIFO overflowed.

receive collision
Indicates the total number of collisions encountered by the receiver support on the adapter.

Note: This counter cannot be cleared by the **clear statistics** command because it is maintained on the adapter. The **test network** command is the only way to reset this counter.

missed frame
Indicates the number of incoming receive frames lost due to unavailability of a receive buffer in the system. This error indicates that the system is not processing received frames as fast as they are being received from the local network.

Note: This counter cannot be cleared by the **clear statistics** command because it is maintained on the adapter. The **test network** command is the only way to reset this counter.

frames filtered
Indicates the number of incoming frames that were discarded by the adapter. This counter is updated only when bridging is enabled.

Note: This counter is maintained on the adapter, and is cleared every time it is read. This counter will be cleared by the **interface statistics** and the **test network** commands.

receive underrun
Indicates the number of times the adapter did not have a second buffer to store a long frame (requiring more than one buffer).

Output statistics:

one retry
Indicates that exactly one retry was needed to transmit a frame. This data is exported via SNMP as the dot3StatsDeferredTransmissions counter.

single collision
The Single Collision counter increments when a packet has a collision on the first transmission attempt, and then successfully sends the packet on the second transmission attempt. This data is exported via SNMP as the dot3StatsSingleCollisionFrames counter.

multiple collisions
The Multiple Collisions counter increments when a packet has multiple collisions before being successfully transmitted. This data is exported via SNMP as the dot3MultipleCollisionFrames counter.

failed, transmit underflow
Transmit underrun indicates that transmitter has truncated a message because it could not read data from the memory fast enough. It also indicates that the FIFO on the adapter has emptied out before the end of the frame was reached. IFO into memory buffer before the internal FIFO overflowed.

failed, excess collisions
The Failed, Excess Collisions counter increments when a packet transmission fails due to 16 successive collisions. This error indicates a high volume of network traffic or hardware problems with the network. This data is exported via SNMP as the dot3StatsExcessiveCollisions counter.

failed, loss of carrier
Loss of carrier is set when the carrier is lost during transmission. The adapter does not retry upon loss of carrier. It will continue to transmit the whole frame until done.

late collisions
A late collision indicates that a collision has occurred after the first channel slot time has elapsed. The adapter does not retry on late collisions.

more than one retry
More than one retry indicates that more than one retry was needed to transmit a frame.

buffer error
Buffer error occurs if there is a memory corruption problem in the system, or under certain FIFO underflow conditions on the adapter.

total collisions
The Total Collisions counter increments by the number of collisions a packet incurs.

excessive deferral
Excessive deferral indicates that the transmitter on the adapter has experienced Excessive Deferral on this a transmit frame, where Excessive Deferral is defined in the ISO 8802-3 (IEEE/ANSI 802.3) standard.

deferred
Deferred indicates the number of times the adapter had to defer while trying to transmit a frame. This condition occurs if the DMA channel is busy when the adapter is ready to transmit.

memory error
Memory errors occur when the adapter is not given access to the system interface bus within the programmable length of time. This error will normally occur during transmit operations, indicating transmit underrun.

Chapter 19. Configuring and Monitoring the 10/100 Mbps Ethernet Network Interface

This chapter describes the 10/100 Mbps Ethernet interface configuration and operational commands. It includes the following sections:

Accessing the Interface Configuration Process

Use the following procedure to access the configuration process. This process gives you access to an Ethernet interface's *configuration* process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to "Chapter 3. The OPCON Process" on page 27.) For example:

   ```
   * talk 6
   Config>
   ```

   The CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.
3. Record the interface numbers.
4. Enter the **network** command and the number of the Ethernet interface you want to configure. For example:

   ```
   Config> network 0
   Ethernet 100 interface configuration
   ETH100 Config>
   ```

   The 10/100 Mbps Ethernet configuration prompt (`ETH100 Config>`), is displayed.

10/100 Mbps Ethernet Configuration Commands

This section describes the 10/100 Mbps Ethernet configuration commands. Enter the commands at the `ETH config>` prompt.

Table 28. 10/100 Mbps Ethernet Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Duplex	Sets the duplex mode.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X'0800') or IEEE (802.3 with SNAP).
List	Displays the current connector-type, and IP encapsulation.
Physical-Address	Sets the physical MAC address.
Speed	Sets the link speed.

Table 28. 10/100 Mbps Ethernet Configuration Command Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Duplex

Use the **duplex** command to set the duplex mode.

Note: The default value of **auto** is recommended. The value **half-duplex** or **full-duplex** should be specified only if the link partner is also configured for the same mode.

Syntax:

duplex half_duplex
full_duplex
auto

Half_duplex
The interface will not transmit while receiving or receive while transmitting.

Full_duplex
The interface will transmit and receive simultaneously.

Auto The interface will automatically select half-duplex or full duplex depending on the link partner’s capability.

IP-Encapsulation

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X’0800’) or IEEE 802.3 (Ethernet 802.3 with SNAP). Enter **e** or **i** for the type.

Syntax:

IP-encapsulation *type*

Example: `IP-encapsulation e`

List

Use the **list** command to display the current configuration for the 10/100 Mbps Ethernet interface.

Syntax:

list all

Example:

```
list all

The duplex is   HALF DUPLEX
The speed is   100Mb
IP Encapsulation:   Ether

MAC Address:        023456789A56
```

Physical-Address

Use the **physical-address** command to set the physical (MAC) address.

Syntax:

physical-address *address*

physical-address
This command lets you indicate whether you want to define a locally administered address for the Ethernet interface's MAC sublayer address, or use the default burned-in address (indicated by all zeros). The MAC sublayer address is the address that the Ethernet interface uses to receive and transmit frames.

Note: Pressing **Enter** leaves the value the same. Entering **0** causes the router to use the burned-in address. The default is to use the burned-in address.

Valid Values: Any 12-digit hexadecimal address.

Default Value: burned-in address (indicated by all zeros).

Example:

```
physical-address
MAC address in 00:00:00:00:00:00 form []? 12:15:00:FA:00:FE
```

Speed

Use the **speed** command to set the speed used by this interface.

Note: The default value of **auto** is recommended. The values of **ten** and **hundred** should be specified only if the link partner is also configured for the same speed.

Syntax:

speed ten
hundred
auto

Ten The interface will operate at 10 Mbps.

Hundred
The interface will operate at 100 Mbps

Auto The interface will automatically select the speed (10 Mbps or 100 Mbps) depending on the link partner's capability.

Accessing the 10/100 Mbps Interface Monitoring Process

To monitor information related to the 10/100 Mbps Ethernet Network Interface, access the interface monitoring process by doing the following:

1. At the OPCON prompt, enter **talk 5**. For example:

```
* talk 5
```

The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.

2. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

```
+ configuration
```

See “Configuration” on page 114 for sample output of the **configuration** command.

3. Enter the **network** command and the number of the Ethernet interface. In this example:

```
+ network 0
ETH100>
```

The 10/100 Mbps Ethernet monitoring prompt is displayed. You can now view information about the 10/100 Mbps Ethernet interface by entering monitoring commands.

10/100 Mbps Ethernet Interface Monitoring Commands

This section summarizes the 10/100 Mbps Ethernet monitoring commands. Enter commands at the ETH100> prompt. Table 29 lists the monitoring commands.

Table 29. Ethernet Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Collisions	Displays collision statistics for the specified Ethernet interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Collisions

This command displays the counts of transmissions for packets that incurred collisions before successful transmission. Counters are displayed for packets sent after 15 collisions. An increased number of packets transmitted with collisions and higher numbers of collisions per packet are signs of transmitting onto a busy Ethernet.

These counters are cleared by the OPCON **CLEAR** command. This data is exported via SNMP as the dot3CollTable counter.

Syntax:

collisions

Example:

```
Eth100> coll

Transmitted with  1 collisions:0
Transmitted with  2 collisions:0
Transmitted with  3 collisions:0
Transmitted with  4 collisions:0
Transmitted with  5 collisions:0
Transmitted with  6 collisions:0
Transmitted with  7 collisions:0
Transmitted with  8 collisions:0
Transmitted with  9 collisions:0
Transmitted with 10 collisions:0
```

```
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

Chapter 20. Configuring Serial Line Interfaces

This chapter describes the interface configuration process for a serial interface and includes the following sections:

- "Accessing the Interface Configuration Process"
- "Network Interfaces and the GWCON Interface Command" on page 240

IMPORTANT: To configure Frame Relay, PPP, X.25, V.25bis, Bisync, SDLC Relay, and SDLC protocols on the serial interface, use the commands in this chapter and then refer to the commands in the chapters that describe the specific protocol.

See "Configuring the Network Interface" on page 20 for a table of protocols and the interfaces that support those protocols.

Accessing the Interface Configuration Process

See "Accessing Network Interface Configuration and Operating Processes" on page 18 for a description of how to add a serial interface. Once you have done that, the following paragraphs describe how to set the data-link of the interface correctly and how to access that data-link's configuration commands.

To access the interface configuration process for a serial interface, first access the `Config>` prompt and issue the command **set data-link**. Next, at the `Config>` prompt, enter the interface type and number to access the configuration environment for the interface.

For example, to configure a serial interface for X.25, you must access the `X.25 config>` environment by issuing the following commands:

```
Config> set data-link X25 2
Config> network 2
```

From the `X.25 config>` environment, you can complete your configuration of X.25 on the serial interface. See "Chapter 21. Using the X.25 Network Interface" on page 241.

When you are done configuring the serial interface, enter the **restart** command after the OPCON prompt (*) and respond **yes** to the prompt to enable the new configuration.

Clocking and Cable Type

This section applies to all uses of a serial port for: FR, PPP, X.25, SDLC Relay, Bisync,and SDLC.

If a modem or CSU/DSU is attached to the serial port then the router is taking on the DTE role in terms of clocking on the line, so configure a DTE cable type and external clocking.

If you want to attach two routers directly without a modem, CSU/DSU, or modem eliminator, then one of the routers will take on the DCE role in terms of clocking on the line. Connect a direct attach cable to the router that will act as the DCE and configure the following parameters for its serial interface.

1. A DCE cable type
2. Internal clocking
3. The clocking/line speed

The other router will take on the DTE role in terms of clocking and should be configured as if it were attached to a modem or CSU/DSU

Note: Configuring a DTE as opposed to a DCE cable has no impact on whether or not the WAN net handler takes on the peer device. For example, the router always acts as a Frame Relay DTE device and uses a FR UNI interface even when a Frame Relay interface is configured to use a DCE cable.

Network Interfaces and the GWCON Interface Command

While serial line interfaces do not have their own console process for monitoring purposes, routers can display complete statistics for all installed network interfaces when you use the **interface** command from the GWCON environment. For more information on the **interface** command and displaying statistics, see Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands.

Chapter 21. Using the X.25 Network Interface

The X.25 network interface connects a router to an X.25 virtual circuit switched network. The X.25 network interface software and hardware allows the router to communicate over a public X.25 network. The X.25 network interface complies with CCITT 1980, CCITT 1984, CCITT 1988 and ISO 8208 1990 specifications for X.25 interfaces offering multiplexed channels and reliable end-to-end data transfer across a wide area network.

This chapter includes the following sections:

For information on configuring X.25 Transport Protocol (XTP) for transporting X.25 traffic over TCP/IP, see "Chapter 23. Using XTP" on page 283.

Basic Configuration Procedures

This section outlines the minimal configuration steps required to get the X.25 interface up and running. The X.25 parameters must be consistent with the X.25 network the interface on the router will connect to. For more information, refer to the configuration commands described in this chapter.

Note: You must restart the router for the configuration changes to take effect.

1. At the OPCON prompt (*), type **talk 6**.

   The `Config>` prompt appears.
2. Type **list devices** to display a list of the interfaces from which you can select. Use the appropriate interface number in the following step.
3. Type **set data-link x25**.

   The `Interface Number [0]?` prompt appears.
4. Type the appropriate interface number.
5. Connect to the network by typing **net** *#* at the `Config>` prompt.

   The `X.25 Config [#]>` prompt appears.
6. At this prompt, type **set address** *x.25-node-address*.

   The X.25 address is a unique X.121 address that is used during call establishment. For DDN networks, use the **add htf-addr** and the **set htf-addr** commands to convert the protocol address associated with this interface to the X.121 address format required for DDN address translation. Failure to set the network address prevents the X.25 interface from joining the attached network.
7. Type **set equipment-type** and specify whether the frame and packet levels act as DCE or DTE. The default for this command is DTE.
8. Type **set svc** and define the lowest and highest SVCs that you are using. The default is for 1 SVC.
9. Type **add protocol** *protocol_name* to add the protocols that will be running over the X.25 interface. You will be prompted for window size, default packet size, maximum packet size, circuit idle time, and max VCs.

Note: You need to add the protocols only once for all X.25 networks on the router.

10. Type **add address** *protocol_name* to add an address translation for each protocol's destination address reachable over this interface.
11. Type **exit** to return to the `Config>` prompt.
12. Press **Ctrl-P** to return to the OPCON prompt (*).
13. Type **restart** and respond **yes** to the prompt.

Setting the National Personality

Each public data network, such as GTE's Telenet or DDN's Defense Data Network, has its own standard configuration. The term *National Personality* specifies a group of variables used to define a public data network's characteristics. The configuration information in the National Personality provides the router with control information for packets being transferred over the link. The National Personality option defines 27 default parameters for each public data network.

To view the configuration values that are in your X.25 National Personality, execute the X.25 configuration **list detailed** command. Configure each public data network connected to the router by executing the X.25 configuration **national-personality set** command.

The National Personality is a generalized template for network configuration. If necessary, you can individually configure each frame and packet layer parameter.

Understanding the X.25 Defaults

The following tables list the defaults for the various parameters for the X.25 *set, national set* and *national enable* commands.

Table 30. Set Command

Parameter	Default
address ...	none
cable	none
calls-out ...	4
clocking ...	external
default-window-size ...	2
encoding	NRZ
equipment-type ...	DTE
htf addr ...	none
inter-frame-delay ...	0
mtu	1500
national-personality ...	GTE Telenet
pvc ...	low=0 high=0
speed	9600
svc	low inbound=0, high inbound=0 low 2-way=1, high 2-way=64 low outbound=0, high outbound=0
throughput-class ...	inbound=outbound=2400

Table 30. Set Command (continued)

Parameter	Default
vc-idle ...	30

Table 31. National Enable Parameters

Parameter	DDN Default	GTE Default
accept-reverse-charges	off	on
bi-cug	off	off
bi-cug-with-outgoing-access	off	off
cug	off	off
cug-deletion	off	off
cug-insertion	off	off
cug-with-incoming-access	off	off
cug-with-outgoing-access	off	off
cug-zero-override	off	off
flow-control-negotiation	on	on
frame-ext-seq-mode	off	off
packet-ext-seq-mode	off	off
request-reverse-charges	off	on
suppress-calling-addresses	off	off
throughput-class-negotiation	on	on
truncate-called-addresses	off	off

Table 32. National Set Parameters

Paramter	DDN Default	GTE Default
call-req	20 decaseconds	20 decaseconds
clear-req ...	retries=1	retries=1
	18 decaseconds	18 decaseconds
disconnect-procedure ...	passive	passive
dp-timer	500 milliseconds	500 milliseconds
frame-window-size	7	7
n2-timeouts	20	20
packet-size ...	128, max=256	128, max=256
reset ...	retries=1	retries=1
	18 decaseconds	18 decaseconds
restart ...	retries=1	retries=1
	18 decaseconds	18 decaseconds
min-recall	10 seconds	10 seconds
min-connect	90 seconds	90 seconds
collision-timer	10 seconds	10 seconds
standard-version	1984	1984
t1-timer	4 seconds	4 seconds
t2-timer	0	0

Table 32. National Set Parameters (continued)

Paramter	DDN Default	GTE Default
truncate-called-addr-size	2	2

Null Encapsulation

Null Encapsulation allows the user to multiplex multiple network layer protocols over one X.25 circuit. This function may be used to avoid using an unreasonable number of virtual circuits.

Limitations

Null Encapsulation is not supported for QLLC. This function is supported for Switched Virtual Circuits (SVCs), but not for Permanent Virtual Circuits (PVCs).

Configuration Changes

The encapsulation option NULL has been added for the following T6 commands:

Under X25 config: add address IP (may input enc type = NULL)

Under X25 config: add address IPX (may input enc type = NULL)

Under X25 config: add address DNA (may input enc type = NULL)

Under X25 config: add address VINES (may input enc type = NULL)

Under X25 config: list addr will show active enc type = NULL if the priority 1 type is NULL.

T5 commands:

Under X25 ıint▪: List SVCS will include enc type = NULL

Configuring Null Encapsulation and Closed User Groups (CUG)

Since More than one Protocol can run over one virtual circuit while using Null Encapsulation, the CUG(s) defined for each protocol over that circuit must be the same. It is strongly suggested that the user configure multiple Protocols same destination as follows:

Configure CUG using the add address. The CUG(s) defined must be the same for each protocol defined at the same address.

If the CUG is defined at the add protocol level, The CUG(s) must be the same for all peers. (This method is more restrictive).

Configure CUG at the interface level. This insures all peers have the same CUG values. (This method is the most restrictive)

Any of the above methods may be used as long as any incoming call CUG definition must be valid for all protocols sharing that circuit. Valid means that the CUG was defined for the specific address or was defaulted to use either the protocol or interface circuit definition.

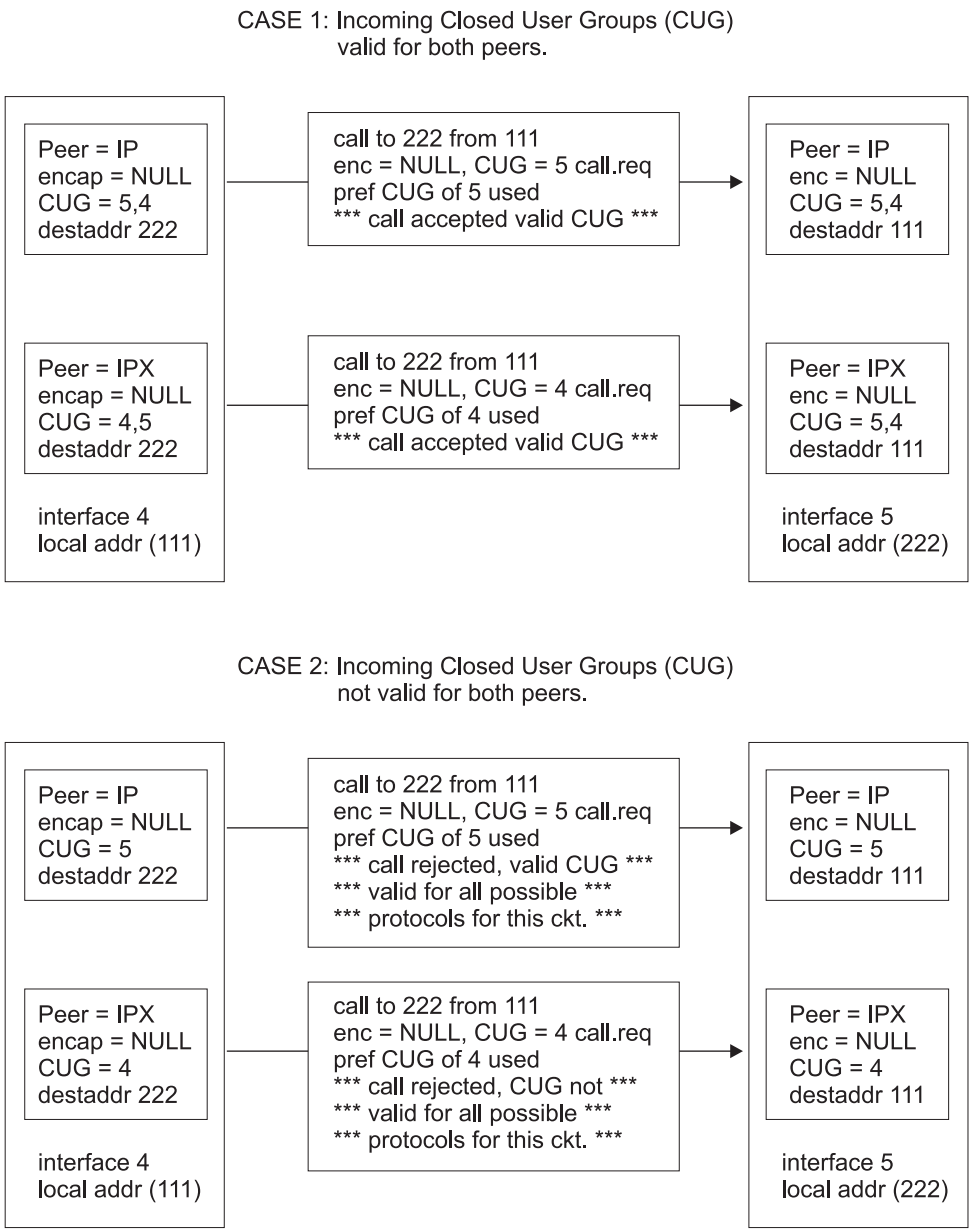

Figure 15. Closed User Group Null Encapsulation

Understanding Closed User Groups

A *closed user group (CUG)* is a group of X.25 DTEs allowed to establish connections with other specific DTEs. CUG numbers are defined by your network provider and you can only use the CUGs the provider assigns you. You can configure an address-specific CUG, a protocol-specific CUG, or an interface-specific CUG. If all of three types of CUG numbers are configured for a DTE, the closed user group facility uses the address-specific destination CUG in a call request when contacting another DTE. If only a protocol-specific and an interface-specific CUG are configured for a DTE, the closed user group facility uses the protocol-specific CUG in a call request when contacting another DTE.

A single DTE can belong to multiple CUGs. You must specify a preferred CUG for that DTE. The preferred CUG is used when the router initiates calls to other DTEs. A single DTE cannot have more than a total of 5 preferred or normal closed user groups.

Bilateral Closed User Groups

A *bilateral closed user group (BCUG)* is a closed user group consisting of only two DTEs. The DTEs within the BCUG can originate calls to members of the BCUG and any DTEs that are not members of any CUG or BCUG. A single DTE cannot have more than a total of 5 preferred or normal bilateral CUGs.

A DTE uses a BCUG to establish circuits in the same way the DTE uses CUGs to establish circuits (see Table 33), however, if both a BCUG and a CUG is defined for an interface, protocol, or address, the BCUG is used to establish the circuit.

Types of Extended Closed User Groups

The following extensions to closed user groups are supported:

CUG with Outgoing Access
The DTE can belong to one or more CUGs. The DTE can originate calls to members of the CUG and to any DTE belonging to other CUGs with Incoming Access.

CUG with Incoming Access
The DTE can belong to one or more CUGs. The DTE can receive calls from DTEs not belonging to any CUG or from DTEs belonging to other CUGs with Outgoing Access.

BCUG with Outgoing Access
The DTE can belong to one or more BCUGs. The DTE can originate calls to members of the BCUG and to any DTE not belonging to any BCUG.

Establishing X.25 Circuits with Closed User Groups on a Device

When you have enabled the closed user group facility, and a DTE receives a call request, it uses the CUG in the call request to determine whether to accept or reject the call from the DTE. If the CUG in the call request does not match a configured CUG on the interface, protocol, or on the destination associated with the calling DTE, the request is rejected. Table 33 summarizes how X.25 circuits are established based on CUGs, if the interface, protocol, and address CUG numbers are different and incoming access is not enabled.

Table 33. Establishing Incoming X.25 Circuits for Closed User Groups

Incoming Call Request Contains	Receiving DTE CUG Definition							
	Interface CUG Only	Protocol CUG Only	Address Specific CUG	Interface and Protocol CUG	Interface and Address CUG	Protocol and Address CUG	All CUGs	No CUGs
No CUG	Reject	Reject	Reject	Reject	Reject	Reject	Reject	Accept
Interface CUG	Accept	Reject	Reject	Reject	Reject	Reject	Reject	Reject

Table 33. Establishing Incoming X.25 Circuits for Closed User Groups (continued)

Protocol CUG	Reject	Accept	Reject	Accept	Reject	Reject	Reject	Reject
Address Specific CUG	Reject	Reject	Accept	Reject	Accept	Accept	Accept	Reject

For outgoing calls on an interface, if you have enabled either the CUG or the BCUG facility, each call request will contain the configured preferred CUG (if any) for the destination or, if no address-specific CUG is configured, the CUG used is the CUG defined for the protocol, or if no protocol-specific CUG is configured, the CUG used is the CUG defined for the interface. If no CUG number has been configured, the CUG facility is not included in any outgoing call request.

Overriding Closed User Group Processing for CUG 0

You can configure the DTE such that it does not validate incoming calls with a CUG of 0 in the call request. This ability allows you to permit specific calls to complete even when you have not enabled incoming access. Using the **national enable cug 0 override** command forces the device to ignore the CUG facility if the CUG number is 0. The call request will not be compared with any configured CUG number.

Configuring X.25 Closed User Groups

To use closed user groups on X.25 interfaces:

1. Request CUG numbers from your network provider. You will need these numbers when configuring X.25.
2. Enable the closed user group facility using the **national enable cug** command and related commands.
3. Enable the bilateral closed user group facility, if desired, using the **national enable bi-cug** command and related commands.
4. Configure the appropriate CUG numbers for the DTEs. Specify the preferred CUG, CUG, preferred bilateral CUG, and bilateral CUG, as needed. This is done through the **add address** command.
5. Configure the appropriate CUG and bilateral CUG for the protocol, if required. This is done through the **add protocol** command.

   Note: You should only configure these CUGs if you are restricting all X.25 circuits established over the X.25 interface for this protocol to DTEs belonging to this set of unique CUGs or BCUGs unless you override it with an address-specific CUG.
6. Configure the appropriate CUG and bilateral CUG for the interface, if required. This is done through the **add cug** command.

   Note: You should only configure these CUGs if you are restricting all X.25 circuits established over the X.25 interface to DTEs belonging to this set of unique CUGs or BCUGs unless uyou override it with an address or protocol-specific CUG.

Chapter 22. Configuring and Monitoring the X.25 Network Interface

This chapter describes the X.25 configuration and operational commands and includes the following sections:

X.25 Configuration Commands

This section summarizes and explains all the X.25 configuration commands.

The X.25 configuration commands allow you to specify network parameters for router interfaces that transmit X.25 packets. The information you specify with the configuration commands activates when you restart the router.

Enter the X.25 configuration commands at the `X.25 config>` prompt. Table 34 shows the commands.

Table 34. X.25 Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Set	Sets the local and DDN X.25 node addresses, window size for packet levels, identifies the National personality, the MTU, and the maximum number of calls. Defines the PVC and SVC channel ranges, the number of seconds that a switched circuit can be idle before it is cleared, and specifies whether one router needs to act as a DCE (when two routers are directly connected without an intervening X.25 network) or the more normal method of acting at a DTE connected to an X.25 network. Sets speed, encoding, clocking, throughput class, and cable type.
Enable/Disable	Enables/Disables incoming-calls-barred feature, outgoing-calls-barred feature, dynamic DDN address translations, and lower-dtr feature.
National Enable or National Disable	Enables/Disables the parameters defined by the National Personality configuration.
National Set	Sets parameters defined by the National Personality configuration.
National Restore	Restores the National Personality configuration to its default values.
Add/Change/Delete	Adds/Changes/Deletes an address translation, a protocol encapsulation, or a PVC definition.
List	Lists the defined address translations, National Personality parameters, protocol encapsulation, or PVC definitions.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Set

Use the **set** command to configure local X.25 node addresses, maximum number of calls, frame and packet level window size, lowest to highest PVC and SVC channels, and the idle time for a switched circuit.

Syntax:

set
- address . . .
- cable
- calls-out . . .
- clocking . . .
- default-window-size . . .
- encoding
- equipment-type . . .
- htf addr . . .
- inter-frame-delay . . .
- mtu
- national-personality . . .
- pvc . . .
- speed . . .
- svc
- throughput-class . . .
- vc-idle . . .

address *x.25-node-addr*

Sets the local X.25 interface address (*x.25-node-addr*). Set the X.25 node address to 0, not to 00, to delete the local X.25 address.

Example: `set address 8982800`

cable *type*

Sets the cable type as follows:

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- X21 DTE
- X21 DCE

A DTE cable is used when you are attaching the router to some type of DCE device (for example, a modem or a DSU/CSU).

A DCE cable is used when the router is acting as the DCE and providing the clocking for direct attachment.

calls-out *value*

Sets the maximum number of locally initiated, simultaneously active SVCs.

Valid Values: 1 to 239

Default Value: 4

clocking *external* **or** *internal*
To connect to a modem or DSU, configure clocking as external. To connect directly to another DTE device, use a DCE cable, set the clocking to internal, and configure the line speed.

Default: external

default-window-size *value*
Sets the window size for the packet level assigned by the router if there is no window-size facility in the Call-Request packet. The range is determined by the National Personality packet modulus (PACKET-EXT-SEQ-MODE).

Default: 2

Example: `set default-window-size 3`

encoding *NRZ* **or** *NRZI*
Sets the HDLC transmission encoding scheme for the interface. Encoding may be set for NRZ (non-return to zero) or NRZI (non-return to zero inverted). NRZ is the more widely used encoding scheme while NRZI is used in some IBM configurations.

Default: NRZ

equipment-type *DCE* **or** *DTE*
Specifies whether the frame and packet levels act as DCE or DTE. This command has no relation to the cable type in use.

Default: DTE (must be DTE for X.31)

htf addr *x.25-node-addr*
Sets the local DTE address when DDN is used. It converts the IP address to an X.121 address as opposed to the **set address** command, which is used to set the local DTE address when CCITT is used.

inter-frame-delay *value*
This parameter defines the minimum delay between transmitted frames. Setting this parameter is useful when interfacing directly to older equipment. This parameter is the amount of time between frames in seconds.

Default: 0

mtu *value*
Sets the Maximum Transmit Unit (MTU) in bytes. This is the maximum message size that will be delivered to the X.25 interface to package and transmit over the serial line. The range is 576 to 16384.

Default: 1500

If you are encountering packet reassembly timeouts when transferring data over the X.25 interface, you should determine what the minimum packet size is for all LAN or serial interfaces that lead to the end-point, then calculate a more suitable X.25 MTU. You should not directly consider the actual X.25 packet size in this calculation because X.25 tends to use a smaller packet size. X.25 usually sends up to 7 packets at one time before waiting for an acknowledgment.

For example, consider a network topology that includes:

– A Token-Ring LAN having a packet size of 4000

– An X.25 serial line having a packet size of 128 with a window size of 7 and a bit rate of 9600 bps
– An Ethernet LAN with a packet size of 1500

In this case, you should probably set the X.25 MTU to 1500. That means that about 12 packets will be sent over the X.25 interface. (MTU / X.25 packet size = number of X.25 packets to be sent).

When using an MTU of 4096, 32 packets must be sent over the X.25 interface. (4000 /128 = 31.25). In this case, packet reassembly timeouts will probably occur if the X.25 modem speed is 9600 bps. Using an X.25 modem speed of 56 Kbps would probably solve this problem.

Notes:

1. The MTU parameter has significant impact on the memory requirements and memory utilization of the device. Use an MTU value of 8192 or less for devices with less than 8M of memory.
2. The amount of memory available while the device is running limits the number of SVCs that can be established and still maintain optimal performance. For recommendations on the maximum number of SVCs see the product home page on the World Wide Web.

national-personality *GTE-Telenet* **or** *DDN*

Sets the 28 default parameters for either GTE-Telenet or DDN National Personality.

Default: GTE-Telenet

pvc low/high *value*

Defines the lowest to the highest Permanent Virtual Circuit channel number. Zero indicates no PVCs. By default there are no PVCs.

pvc low

0

pvc high

0

The range is 1 to 4095. These values are setting boundaries of a given VC range. There is a maximum of 2500 PVCs.

Example: `set pvc low 40`

Note: Values must not overlap values set for SVCs.

speed *speed-setting*

For internal clocking, this command specifies the speed of the transmit and receive clock lines.

Valid values: 2400 to 2048000 bps.

For external clocking, this command does not affect the hardware but it sets the speed for some protocols, such as IPX, used to determine routing cost parameters. In these cases, set the speed to match the actual line speed. The maximum line speed that can be configured if using external clocking is 6 312 000 bps.

Default: 9600

Note: The X.25 software is supported only at speeds up to 256 000 bps.

svc low/high *inbound* **or** *two-way* **or** *outbound value*

Defines the lowest to the highest switched virtual circuit channel number. When low=high=0, no VCs in this category are defined.

Example: `set SVC low-two-way 1`

Inbound

Specifies the range of logical channel numbers to be assigned to inbound SVCs. By default, there are no inbound-only SVCs.

Valid values: 0 to 4095

Default values: 0

Two-way

Specifies the range of logical channel numbers to be assigned to two-way SVCs. By default, there are sixty-four 2-way SVCs.

Valid values: 0 to 4095

Default values:

svc low
1

svc high
64

Outbound

Specifies the range of logical channel numbers to be assigned to outbound SVCs. By default, there are no outbound-only SVCs.

Valid values: 0-4095

Default: 0

Note: Values in each range must not overlap other SVC ranges nor the PVC range. Table 35 shows a possible VC configuration.

Table 35. Example VC Definitions

	Low	High
PVC	1	40
inbound	0	0
two-way	41	59
outbound	60	500

throughput-class inbound *or* outbound *bit-rate*

Defines the throughput class requested when making a call request while throughput negotiation is enabled.

Default: 2400 bps

This setting is ignored when processing incoming call requests.

vc-idle *value*

Defines the number of seconds that a switched circuit can be idle before it is cleared by the router. Zero indicates that the router never clears an idle circuit.

Valid values: 1 to 255

Default: 30 seconds

Enable

Use the **enable** command to enable DDN address translations, interface resets, or the incoming-calls-barred, outgoing-calls-barred, and lower-dtr features.

Syntax:

enable ddn—address-translations

Note: Enabling ddn-address-translations is no longer allowed. This feature defaults to enabled when the national personality selected is DDN, and defaults to disabled in all other cases.

incoming-calls-barred

lower-dtr

outgoing-calls-barred

incoming-calls-barred
Specifies that the router will not accept incoming calls. The default setting for this parameter is disabled or *off*, which allows incoming calls.

lower-dtr
This parameter determines the way the data terminal ready (DTR) signal is handled for leased serial-line interfaces that are disabled. If this parameter is set to ″disabled″ (the default), the DTR signal will be raised when the interface is disabled.

If *lower-dtr* is set to ″enabled,″ the DTR will be lowered when the interface is disabled. This behavior may be desirable in situations where the interface has been configured as an alternate link for WAN Reroute and the interface is connected to a dial-out modem which maintains its dial connection based on the state of the DTR signal.

When lower-dtr is enabled and the interface is disabled, the DTR signal is low and the modem keeps the dial connection down. When the interface is enabled, due to a WAN Reroute backup scenario, DTR is raised and the modem dials a stored number to the backup site. When the primary interface is restored, the alternate interface is disabled, DTR is lowered, and the modem hangs up the dial connection.

The following cable types are supported:

RS-232

V.35

V.36

The default setting is disabled.

outgoing-calls-barred
Specifies that the router will not allow outgoing calls. The default setting for this parameter is disabled or *off*, which allows outgoing calls.

Disable

Use the **disable** command to disable DDN address translations, interface resets as part of network certification, or the incoming-calls-barred or outgoing-calls-barred features.

Note: If you set DDN as the national personality, DDN address translation is enabled automatically and this parameter has no effect.

Syntax:

disable ddn-address-translations

Note: Disabling ddn-address-translations is no longer allowed. This feature defaults to enabled when the national personality selected is DDN, and defaults to disabled in all other cases.

incoming-calls-barred

lower-dtr

outgoing-calls-barred

National Enable

Use the **national enable** command to enable a feature defined in the National Personality configuration.

Syntax:

national enable accept-reverse-charges

bi-cug

bi-cug-outgoing-access

cug

cug-deletion

cug-incoming-access

cug-insertion

cug-outgoing-access

cug-zero-override

flow-control-negotiation

frame-ext-seq-mode (required for X.31)

packet-ext-seq-mode

request-reverse-charges

suppress-calling-addresses

throughput-class-negotiation

truncate-called-addresses

accept-reverse-charges
Accepts reverse charge calls during call establishment. This option is not available for DDN.

DDN Default
off

GTE Default
on

bi-cug Enables the bilateral closed user group facility on this device. By default, this facility is disabled.

Note: You cannot add any bilateral CUGs unless this parameter is enabled.

bi-cug-outgoing-access
Enables the bilateral CUG with outgoing access facility on this device. By default, this facility is disabled.

cug Enables the closed user group facility on this device. By default, this facility is disabled.

Note: You cannot add any CUGs unless this parameter is enabled.

cug-deletion
Deletes a CUG facility from a call packet received from XTP before transmitting it over X.25. By default, this function is disabled.

cug-incoming-access
Enables the CUG with incoming access facility on this device. By default, this facility is disabled.

cug-insertion
Inserts the appropriate (address-specific, protocol-specific, or interface-specific) preferred cug number into a call request received by XTP from the X.25 interface before transmitting the request over IP. If there is already a CUG facility in the call packet, it will not be replaced. By default, this function is disabled.

cug-outgoing-access
Enables the CUG with outgoing access facility on this device. By default, this facility is disabled.

cug-zero-override
Causes the closed user group facility to ignore any CUG facility in call request packets with a CUG number of 0. By default, this function is disabled.

flow-control-negotiation
Enables the negotiation of packet and window size during call setup of SVCs.

DDN Default
on

GTE Default
on

frame-ext-seq-mode
Sets the frame layer sequence numbering to modulo 128 (i.e., 0 through 127).

DDN Default
off (must be on for X.31)

GTE Default
off

packet-ext-seq-mode
Enables the packet layer to use extended sequence numbers (0 through 127).

DDN Default
off

GTE Default
off

request-reverse-charges
Requests reverse charges for all outgoing calls.

DDN Default
off

GTE Default
on

suppress-calling-address
Suppresses the source address in call packets.

DDN Default
off

GTE Default
off

throughput-class-negotiation
Enables the registration of throughput class.

DDN Default
off

GTE Default
on

truncate-called-addresses
Enables truncation of the called DTE address when transmitting a call to a DTE. This option applies only to XTP circuits.

DDN Default
off

GTE Default
off

National Disable

Use the **national disable** command to disable a feature defined by the National Personality configuration.

Syntax:

national disable accept-reverse-charges
bi-cug
bi-cug-outgoing-access
cug
cug-deletion
cug-incoming-access
cug-insertion
cug-outgoing-access
cug-zero-override

flow-control-negotiation
frame-ext-seq-mode
packet-ext-seq-mode
request-reverse-charges
suppress-calling-addresses
throughput-class-negotiation
truncate-called-addresses

National Set

Use the **national set** command to set one or all of the default values made to the National Personality configuration.

Syntax:

national set call-req
clear-req . . .
disconnect-procedure . . .
dp-timer
frame-window-size
n2-timeouts
packet-size . . .
reset . . .
restart . . .
min-recall
min-connect
collision-timer
standard-version
t1-timer
t2-timer
truncate-called-addr-size

call-req
Specifies the number of 10-second intervals permitted before giving up on a call request and clearing it. A zero indicates an infinite wait. In a list command output, this is displayed as the t21 timer.

DDN Default
20 decaseconds

GTE Default
20 decaseconds

clear-req *retries* **or** *timer*
Specifies the number of clear request retransmissions.

Retries
Number of clear request transmissions permitted before action is taken. In a list command output, this is displayed as the r23 retry count.

DDN Default
retries=1

GTE Default
retries=1

Timer Number of 10–second intervals to wait before retransmitting a clear request packet. A zero in the timer value indicates an indefinite wait. In a list command output, this is displayed as the t23 timer.

DDN Default
18 decaseconds

GTE Default
18 decaseconds

disconnect-procedure *passive* **or** *active*
Specifies the type of connect procedure to use when connecting.

DDN Default
passive

GTE Default
passive

Passive
Specifies that SABM frames are not initiated by the router when connecting.

Active Specifies that SABM frames are initiated by the router when connecting.

dp-timer
Specifies the number of milliseconds that the frame level remains in a disconnected state. Zero indicates immediate transition from disconnected phase to link setup state.

DDN Default
500 milliseconds

GTE Default
500 milliseconds

frame-window-size
Specifies the number of frames that can be outstanding before acknowledgment.

DDN Default
7

GTE Default
7

n2-timeouts
Specifies the number of times the retransmit timer (T1) can expire before the interface is recycled.

DDN Default
20

GTE Default
20

packet-size *default* **or** *maximum* **or** *window*
Specifies the size of the packet.

default
Number of bytes in the data portion of the packet. Possible options include 128, 256, 512, 1024, 2048, and 4096. This value is used in the absence of packet size negotiation. *Default* cannot be greater than *maximum*.

DDN Default
128

GTE Default
128

maximum
Maximum number of bytes in the data portion of the packet. Possible options include 128, 256, 512, 1024, 2048, and 4096.

DDN Default
256

GTE Default
256

window
Number of outstanding I-frames permitted before acknowledgment is required. The range is determined by the National Personality Packet Modulus.

Related configuration parameters are

- Protocol max default window
- Set default window size

reset *retries* **or** *timer*
Specifies the number of reset request retransmissions.

Example: `national set reset retries 2`

retries
Number of reset request transmissions permitted before the call is cleared. The range is 0 to 255. In a list command output, this is displayed as the r22 retry count.

DDN Default
1

GTE Default
1

timer Number of 10-second intervals to wait before retransmitting a reset request packet. The range is 0 to 255. A zero in the timer value indicates an indefinite wait. In a list command output, this is displayed as the t22 timer.

DDN Default
18 decaseconds

GTE Default
18 decaseconds

restart *retries* **or** *timer*
Specifies the number of restart request transmissions.

retries
Number of restart request transmissions permitted before the interface is recycled. The range is 0 to 255. In a list command output, this is displayed as the r20 retry count.

DDN Default
1

GTE Default
1

timer Number of 10–second intervals to wait before retransmitting a restart request packet. The range is 0 to 255. A zero in the timer value indicates an indefinite wait. In a list command output, this is displayed as the t20 timer.

DDN Default
18 decaseconds

GTE Default
18 decaseconds

min-recall
Specifies the minimum number of seconds to wait prior to reinitiating a call to open an SVC. The range is 0 to 255 seconds.

DDN Default
10 seconds

GTE Default
10 seconds

min-connect
Specifies in seconds, the minimum amount a time an SVC will remain established once the connection is made barring any error conditions. The range is 0 to 255 seconds.

DDN Default
90 seconds

GTE Default
90 seconds

collision-timer
Specifies in seconds, the time delay used prior to reinitiating a call to open an SVC if the original attempt resulted in a call collision. The range is 0 to 255 seconds.

DDN Default
10 seconds

GTE Default
10 seconds

standard-version
Options are none, v1980, v1984, and v1988.

DDN Default
1984

GTE Default
1984

t1-timer
Specifies the frame retransmit time in seconds. The range is 1 to 255.

DDN Default
4 seconds

GTE Default
4 seconds

t2-timer
Specifies the amount of time in seconds to delay before acknowledging an I-frame. This is an optimization parameter. Setting the timer to 0 disables it. The range is 0 to 255.

DDN Default
0

GTE Default
0

truncate-called-addr-size
Specifies the number of characters truncated from the end of a called address. This parameter pertains only to XTP circuits. The range is 0 to 10.

DDN Default
2

GTE Default
2

National Restore

Use the **national restore** command to restore one or all of the default values made to the National Personality configuration via the **national set**, **national enable**, or **national disable** command.

Syntax:

national restore

all
accept-reverse-charges
bi-cug
bi-cug-outgoing-access
call-req
clear-req . . .
cug
cug-deletion
cug-incoming-access
cug-insertion
cug-outgoing-access
cug-zero-override
disconnect-procedure . . .
dp-timer
flow-control-negotiation

frame-ext-seq-mode
frame-window-size
min-collission-timer
min-connect-timer
min-recall-timer
network-type . . .
n2-timeouts
packet-size . . .
packet-ext-seq-mode
request-reverse-charges
reset . . .
restart . . .
standard-version
suppress-calling-addresses
throughput-class-negotiation
t1-timer
t2-timer
truncate-called-addresses
truncate-called-addr–size

Add

Use the **add** command to add an X.121 address, a DDN X.25 Address, a protocol configuration, or a PVC definition.

Syntax:

add address
bi-cugs
cugs
htf-address
protocol
pvc

address

Adds an X.121 address translation for a protocol supported in the configuration of the router. The prompts that appear depend on the protocol address that you are adding. (See the following examples.) The protocol address and X.121 address being entered represent the protocol and X.121 DTE address of the remote DTE connecting to the router X.25 interface. The mapping of a protocol address and the X.121 address must be unique unless the protocol is APPN or DLSw. A protocol address cannot map to more than one X.121 address. Also, a specific X.121 address cannot map to more than one protocol address. The **set address** command is used to set the local X.25 address. After setting the local X.25 address, you can use

an X.25 remote address to dial out and an optional incoming remote address for call ID. IF only remote called address is entered, then this address will be used for outgoing calls and incoming call verification.

Example: `add address`

IP example:

```
Protocol [IP]?  IP
IP Address [0.0.0.0]? 128.185.1.2
Enc Priority 1 []? CC
Enc Priority 2 []? SNAP
Enc Priority 3 []? Null
X.25 Address []? 1234590
Remote address []?
Pref CUG  []? 11
CUG (2)  []? 12
CUG (3)  []? 13
CUG (4)  []? 14
CUG (5)  []? 15
Pref BI-CUG  []? 21
BI-CUG (2)  []? 22
BI-CUG (3)  []?
```

IPX example:

```
Protocol [IP]?  IPX
CUD Field Usage (Standard or Proprietary)
IPX Host Number (in hex) []?
Enc Priority 1 []? SNAP
Enc Priority 2 []?Null
X.25 Address []?
Pref CUG [] ?
Pref Bi-CUG[]? 1
BI-CUG (2)[]? 3
BI-CUG (3)[]
```

Protocol

Specifies the protocol type of the address mapping you are adding. The valid values are APPN, DECnet, DLSw, IP, IPX and VINES. The default is IP.

Enc Priority

Determines the encapsulation type, as defined in RFC 1356, that will be put in the CUD. For IP, valid choices are CC, SNAP, or Null. For IPX, valid choice is SNAP or Null.

IP Address

Specifies the destination's IP address.

CUD Field Usage

This field is for IPX to X.25 address mapping only. It determines how the Call User Data (CUD) field is filled in when call request packets are received for IPX. The CUD field can be either Standard or Proprietary. Standard indicates that the usage is protocol multiplexing used in RFC 1356. Proprietary indicates a proprietary CUD field that can only be used with 2212 or compatible routers. The default is Standard.

IPX Host Number

Specifies the IPX host number of the destination.

X.25 Address

Specifies the X.121 DTE address of the remote DTE connecting to the router X.25 interface. The maximum address length is 15 digits.

pref cug

Specifies the preferred closed user group number for this DTE. The DTE uses this CUG when placing outgoing calls.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the closed user group facility using the **national enable** command.

CUG Specifies the closed user group numbers for this DTE. Up to five CUGs may be defined, including the pref CUG.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the closed user group facility using the **national enable** command.

pref bi-cug
Specifies the bilateral closed user group number for this DTE. The DTE uses this CUG when placing outgoing calls.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the bilateral closed user group facility using the **national enable** command.

bi-cug Specifies the bilateral closed user group numbers for this DTE. Up to five CUGs may be defined.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the bilateral closed user group facility using the **national enable** command.

cugs Specifies the closed user group number for this X.25 interface.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the closed user group facility using the **national enable** command.

Example:

```
add cugs
Pref CUG  []? 23
CUG (2)  []? 24
CUG (3)  []? 25
CUG (4)  []? 26
CUG (5)  []? 27
```

pref cug
Specifies the preferred closed user group number for this DTE. This DTE uses this CUG when placing outgoing calls.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the closed user group facility using the **national enable** command.

cug Specifies the closed user group numbers for this DTE. Up to five CUGs may be defined.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the closed user group facility using the **national enable** command.

bi-cugs

Specifies the closed user group number for this DTE.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the closed user group facility using the **national enable** command.

Example:

```
add bi-cugs
Pref BI-CUG  []? 23
BI-CUG (2)  []? 24
BI-CUG (3)  []? 25
BI-CUG (4)  []? 26
BI-CUG (5)  []? 27
```

pref bi-cug

Specifies the preferred closed user group number for this DTE. This DTE uses this BI-CUG when placing outgoing calls.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the bilateral closed user group facility using the **national enable** command.

bi-cug Specifies the closed user group numbers for this DTE. Up to five BI-CUGs may be defined.

Valid values: 0 to 9999

Default value: None

Note: You will not be prompted for this value if you have not enabled the bilateral closed user group facility using the **national enable** command.

htf-address

Adds a Defense Data Network (DDN) X.25 address translation.

Example:

```
add htf-address
Protocol [IP]
Convert HTF address
```

Protocol

Specifies the protocol that you are running over the X.25 interface. DDN supports IP only.

Convert HTF address

Converts the protocol address to a destination X.121 address in Host Table Format (HTF) format. Also see ddn-address-translations in the Enable/Disable commands section.

protocol

Enables a protocol encapsulation and defines the associated parameters.

Example:

```
add protocol
Protocol [IP]?
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
Circuit Idle Time [30]?
Max VCs [4]?
Pref CUG  []? 1
CUG (2)  []? 2
CUG (3)  []? 3
CUG (4)  []? 4
CUG (5)  []? 5
Pref BI-CUG  ]? 11
BI-CUG (2)  []? 12
BI-CUG (3)  []? 13
BI-CUG (4)  []? 14
BI-CUG (5)  []? 15
```

QLLC example:

```
X.25 Config> add prot
Protocol [IP]? dls
Idle timer [30]?
QLLC response timer (in decaseconds) [2]?
QLLC response count [3]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI  (2) SEC  (3) (PEER) [3]?
Max Packet Size [128]?
Packet window size [7]?
Max Message Size [1500]?
Call User Data (in hex, 0 for null) []?
Pref CUG  []? 20
CUG (2)  []? 21
CUG (3)  []?
Pref BI-CUG  []?
```

Protocol

Specifies which protocol's encapsulation parameters you want to add: APPN, XTP, IP, DECnet, IPX, DLSw, or Banyan VINES. The default is IP.

Window Size

Specifies the maximum negotiable packet window size, the number of packets that can be outstanding before requiring packet confirmation. The default is 2. The window size can be negotiated down to 1 by the called DTE.

Related configuration parameters are:

- Set Default Window

Default Packet Size

Specifies the default requested packet size for SVCs. This value serves as the lowest negotiable packet size and must be equal to or less than the maximum packet size specified with the **national set packet-size** command. The maximum *default packet size* is 4096 bytes. The default value for this parameter is 128 bytes.

Related configuration parameters are:

- National Set Packet Size Default
- National Set Packet Size Maximum

Maximum Packet Size

Specifies the maximum negotiable packet size for SVCs. This value must be equal to or less than the maximum packet size specified with the **national set packet-size** command. The default value for this parameter is 256 bytes. The maximum value that can be configured for this parameter is 4096 bytes. This value is utilized in calculating the maximum frame size for this X.25 interface.

Related configuration parameters are:

- National Set Packet Size Default
- National Set Packet Size Maximum

Circuit Idle Time

Specifies the number of seconds that an SVC can be idle before it is cleared by the router. The range is 0 to 65365. The default is 30 seconds. A 0 (zero) specifies that the circuit is never cleared by the router.

Maximum VCs

Specifies the maximum number of circuits that are open to the same DTE address for a protocol. Refer to RFC 1356 for information on utilizing this parameter. The Valid range is 1 to 10. The default is 4.

pref CUG, CUG, pref bi-cug, bi-cug

See **add address** command.

The following are QLLC unique parameters:

QLLC response timer

The number of seconds to wait for a Q-response packet before retransmitting.

QLLC response count

The maximum number of times QLLC will retransmit. Upon exhausting this number of retries, the upper layer is notified which may result in the circuit being cleared or reset by the router.

Accept Reverse Charges

Allows this protocol to override the setting of this National Personality parameter. This does not affect the National Personality parameter.

Request Reverse Charges

Allows this protocol to override the setting of this National Personality parameter. This does not affect the National Personality parameter.

Station Type
Specifies the default station type for this protocol:

Pri Primary Station

Sec Secondary Station

Peer Peer Station

Max message size
The maximum message size for this protocol. Specify a value that is less than, or equal to, the Max MTU size of the interface.

Call User Data
Specifies the default CUD field used in call packets for this protocol. Specify from 1-to-16 characters. If you do not specify characters, the default 0xC3 is used.

pvc Adds PVC, window size, and packet size definitions.

Example: `add pvc`

IP example:

```
Protocol [IP]?  IP
Packet Channel Range Start [1]?
Destination X.25 Address[]?
Packet Channel Range End [1]?
Window Size [2]?
Packet Size [128]?
```

Protocol
Specifies which protocol's encapsulation you want to modify: APPN, XTP, DECnet, Banyan Vines, DLSw, IP or IPX. The default is IP.

Packet Channel Range Start
Specifies the starting circuit number of this range of PVCs.

Packet Channel Range End
Specifies the last circuit number of this range of PVCs. Defaults to the value of the Packet Channel Range Start.

Destination X.25 Address
Specifies the X.25 address of the PVC's destination.

Remote Address
Specifies the remote address for caller ID on received calls.

Window Size
Specifies the number of packets that can be outstanding before requiring packet confirmation. The default is 2.

Related configuration parameters are:

- Set Default Window

Packet Size
Specifies the maximum negotiable packet size for PVCs. This value must be equal to or less than the maximum packet size specified with the **national set packet-size** command. The default value for this parameter is 128 bytes. The maximum value that may be configured for this parameter is 4096 bytes. The maximum for X.31 is 256 bytes. This value is utilized in calculating the maximum frame size for this X.25 interface.

Related configuration parameters are:

- Nat Set Packet Size Default
- Nat Set Packet Size Maximum

Change

Use the **change** command to change an X.121 address, an DDN X.25 Address, a protocol configuration, or a PVC definition.

Note: To change an IP address that is associated with an X.121 address, you must delete the record that contains the address correlation, then redefine the address mapping.

Syntax:

change address
htf-address
protocol
pvc

address

Modifies a X.121 address translation. The prompts that appear depend on the protocol that is changing.

Example: `change address`

IP example:

```
Protocol [IP]  IP
IP Address [0.0.0.0]?
Enc Priority []?
X.25 Address [00000124040000]?
```

IPX example:

```
Protocol [IP]  IPX
CUD Field Usage (Standard or Proprietary) [Standard]?
IPX Host number (in hex) []?
Enc Priority []?
X.25 Address [00000124040000]?
```

htf address

Changes a Defense Data Network (DDN) X.25 address translation.

Example:

```
change htf-address
Protocol [IP]
Change HTF address [0.0.0.0]?
New HTF address [10.4.0.124]?
```

protocol

Changes a protocol configuration definition.

Example:

```
change protocol
Protocol [IP]
Window Size [2]
Default Packet Size [128]
Maximum Packet Size [256]
Circuit Idle Time [30]
Maximum VCs [6]
```

QLLC example:

```
X.25 Config> change prot
Protocol [IP]? dls
Idle Timer [30]?
QLLC response timer (in decaseconds) [15]?
QLLC response count [255]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI (2) SEC (3) PEER [3]?
Max Packet Size [256]?
Packet Window size [7]?
Max message size [2048]?
Call User Data (in HEX, 0 for Null) []? C3010000525450
```

pvc Changes PVC, window size, and packet size definitions.

Note: To change the protocol, packet channel or destination X.25 address, you must delete the record which contains the definition, then add it back with the changed parameters. A change will apply to *all* PVCs in the range of circuits defined by the Packet Channel Range Start parameter.

Example:

```
change pvc
Protocol [IP]?  IP
Packet Channel Range Start[1]?
Destination X.25 Address [ ]?
Packet Channel Range End [1]
Window Size [2]?
Packet Size [128]?
```

Delete

Use the **delete** command to delete an X.121 address, a protocol configuration definition, or a PVC definition.

Syntax:

delete address | bi-cugs | cugs | protocol . . . | pvc

address

Deletes an X.121 address translation.

Example: `delete address`

IP example:

```
Protocol [IP]?
IP Address [0.0.0.0]?
```

IPX example:

```
Protocol [IP]? IPX
IPX Host Number (in hex) [2]?
```

bi-cugs

Deletes a bilateral closed user group number used by this interface.

Valid values:

Y Deletes the current CUG.

N Does not delete the current CUG.

ALL Deletes all remaining CUGs.

Q Stops deleting any remaining CUGs.

Example:

```
delete bi-cugs
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cugs Deletes the closed user group numbers used by this interface. This command works similar to the **delete bi-cug** command.

Example:

```
del cug

Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

protocol *prot-type*
Deletes a protocol encapsulation configuration definition. *Prot-type* is the name or number of the protocol encapsulation that is currently defined in the router's configuration.

pvc Deletes a PVC definition. *All* PVCs in the range of circuits defined by the Packet Channel Range Start parameter will be deleted.

Example:

```
delete pvc
Protocol [IP]?
Destination X.25 Address [ ]?
Packet Channel Range Start [ ]?
```

List

Use the **list** command to display the current configuration for the specified parameter.

Syntax:

list address
all
cugs
detailed
protocols
pvc
summary

address
Lists all the X.121 address translations.

Example:

```
list address
IF#      Prot #     Active Enc     Protocol ->    X.25 address
1         0(IP)        CC           10.1.2.3 ->    1238765742
1         7(IPX)       SNAP         10       ->    12389
            CUGS: 11 12 13 14 15         BI-CUGS: 21 22
```

all Lists all the X.25 addresses, National Personality parameters, all defined protocols and their values, and all defined PVCs.

Example:

```
list all

X.25 Configuration Summary

Node Address:       313131
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           64000        Clocking:  Internal
MTU:              2048        Cable:     V.35 DCE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 1    high: 1
Inbound          low: 0    high: 0
Two-Way          low: 2    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Request Reverse Charges:  on  Accept Reverse Charges:     on
Frame Extended seq mode:  off Packet Extended seq mode:   off
Incoming Calls Barred:    off Outgoing Calls Barred:      off
Throughput Negotiation:   on  Flow Control Negotiation:   on
Suppress Calling Addresses: off  DDN Address Translation:  off
Truncate Called Addresses:  off
Number of digits to truncate called addresses to:  2
CUG Support: off                BI-CUG Support: off
CUG Outgoing Access: off        CUG Incoming Access : off
BI-CUG Outgoing Access: off     CUG 0 Override: off
CUG Isertion: off               CUG deletion: off
Call Request Timer:     20 decaseconds
Clear Request Timer:    18 decaseconds (1 retries)
Reset Request Timer:    18 decaseconds (1 retries)
Restart Request Timer:  18 decaseconds (1 retries)
Min Recall Timer        10 seconds
Min Connect Timer       90 seconds
Collision Timer          5 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  2.00 seconds     DP Timer:    500 milliseconds
Standard Version:     1984      Network Type: CCITT
Disconnect Procedure: passive
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 128    Maximum: 256

X.25 protocol configuration

No protocols defined

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration
No address translations defined
```

cugs Lists the CUG and BI-CUG numbers for each X.25 interface in this device.

Example:

```
li cugs
CUGS: 23 24 25 26 27
```

detailed

Lists the value of all the default parameters that the **national set** command modifies. Descriptions of the screen display are listed in the **national set** command described later in this chapter.

Example:

```
list detail

X.25 National Personality Configuration

Follow CCITT: on        OSI 1984:     on        OSI 1988:       off
Request Reverse Charges:  off   Accept Reverse Charges:     off
Frame Extended seq mode:  off   Packet Extended seq mode:   off
Incoming Calls Barred:    off   Outgoing Calls Barred:      off
Throughput Negotiation:   on    Flow Control Negotiation:   off
Suppress Calling Addresses: off DDN Address Translation:    off
Truncate Called Addresses:  off
Number of digits to truncate called address to:  2
CUG Support: off                BI-CUG Support: off
CUG Outgoing Access: off        CUG Incoming Access : off
BI-CUG Outgoing Access: off     CUG 0 Override: off
CUG Isertion: off               CUG deletion: off
T21 (Call Request Timer):     20 decaseconds
T23 (Clear Request Timer):    18 decaseconds (1 retries)
T22 (Reset Request Timer):    18 decaseconds (1 retries)
T20 (Restart Request Timer):  18 decaseconds (1 retries)
Min Recall Timer:       10 seconds
Min Connect Timer:      90 seconds
Collision Timer:        8 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  0.00 seconds     DP Timer:    500 milliseconds
Standard Version:     1984      Network Type: CCITT
Disconnect Procedure: active
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 256    Maximum: 256
```

protocols

Lists all the defined protocol configurations. See “Add” on page 263 for a description of the parameters.

Example:

```
list protocols

X.25 protocol configuration

Protocol       Window         Packet-Size        Idle    Max
 Number         Size          Default Maximum    Time    VCs

 0(IP)           2              128   256         30      4
              CUGS: 11 12 13 14 15         BI-CUGS: 21 22
QLLC Protocols

Protocol     Packet        Idle    Response    Reverse_Charges   Max       Station
 Number    Window MaxSize  Time   Timer Count  Accept Request   Message     Type

26(DLSW)     7      256     30     15    255      N      N        2048       PEER
           CUD : [C3 01 00 00 52 54 50 ]
           CUGS: 11 12 13 14 15      BI-CUGS: 21 22
```

pvc Lists all the defined PVCs.

Example:

```
list pvc

X.25 PVC configuration

Prtcl    X.25 Address    Active Enc    Window    Pkt_len   Pkt_chan
0          8383838383        CC           4      1024       3 - 3
```

summary

Lists all the values established by the **set** and **enable** commands. These values modify the X.25 configuration.

Example:

```
list summary

X.25 Configuration Summary

Node Address:       313131
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
```

```
Speed:          64000         Clocking:  Internal
MTU:             2048         Cable:     V.35 DCE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC             low: 1    high: 1
Inbound         low: 0    high: 0
Two-Way         low: 2    high: 64
Outbound        low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400
```

Accessing the Interface Monitoring Process

To monitor information related to the X.25 network interface, access the interface monitoring process as follows:

1. At the OPCON prompt, enter **talk 5**. For example:

   ```
   * talk 5
   +
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.

2. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

   ```
   + configuration
   ```

   See page “Configuration” on page 114 for sample output of the **configuration** command.

3. Enter the **network** command and the number of the X.25 interface.

   ```
   + network 2
   X.25>
   ```

   The X.25 monitoring prompt is displayed on the console. You can then view information about the X.25 interface by entering the X.25 monitoring commands.

X.25 Monitoring Commands

This section summarizes and explains all the X.25 monitoring commands. The X.25 monitoring commands allow you to view the parameters and statistics of the interfaces and networks that transmit X.25 packets. Monitoring commands display configuration values for the physical, frame, and packet levels. You also have the option of viewing the values for all three protocol levels at once.

Enter the X.25 monitoring commands at the `X.25>` prompt. Table 36 shows the commands.

Table 36. X.25 Monitoring Command Summary

Monitoring Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
List	Lists individual PVC or SVC statistics and general information.
Parameters	Displays the current parameters for any level of the X.25 configuration.
Statistics	Displays the current statistics for any level of the X.25 configuration.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

List

Use the **list** command to display the current active PVCs and SVCs.

Syntax:

list pvcs
svcs

pvc Displays the configured permanent virtual circuits.

svc Displays the active switched virtual circuits.

Example:

```
list svc

LCN/  Destination  Originate Transmits  Protocol    Totals
State      Address     Call   Queued  Encapsulated Xmts Rcvs Resets

13 D   898280077113   YES     0          IP      8943  261    1
20 D   898280077114    NO     0          IP       943   43    0
42 P   898280077116   YES     6          IP         0    0    0
23 C   898280077117   YES     0          IP      3054  110    0


D  - Data Transfer      P  - Call Progressing
C  - Call Clearing
```

Parameters

Use the **parameters** command to display the current parameters for any level of the X.25 configuration.

Syntax:

parameters all
frame
packet
physical

all Displays the parameters for the packet, frame, and physical levels.

frame Displays the parameters for the frame level.

Example:

```
parameters frame
Frame Layer Parameters:
Maximum Frame Size  = 262 Maximum Window Size  =     7
Protocol Enabled    = YES Equipment Type       =   DTE
T1 Retransmit Timer =   4 T2 Acknowledge Timer =     2
N2 Retry Counter    =  20 Disconnect Procedure =   PASSIVE
Disconnect Timer    = 500 Network Type         =   GTE
Protocol Options: Inhibit Idle RRs No   MOD 128 NO   Enable SARM  NO
```

packet

Displays the parameters for the packet level.

Example:

```
parameters packet
Packet Layer Parameters:
Default Packet Size = 128  Maximum Packet Size =   256
Log 2 Packet size   =   2  Acknowledge Delay   =     0
Layer Enabled       = YES  Default Window Size =     2
Lowest SVC          =   1  Highest SVC         =    64
Lowest PVC          =   0  Highest PVC         =     0
T20 (Restart)       =  18  R20 (Retry)         =     1
T21 (Call)          =  20
```

```
T22 (Reset)         =  18  R22 (Retry)         =     1
T23 (Clear)         =  18  R23 (Retry)         =     1
Network Type        = GTE  Equipment Type      =   DTE
```

physical

Displays the parameters for the physical level.

Example:

```
parameters physical
Physical Layer Parameters:
Interface Type        =    V.35

Maximum Frame Size    =    264   InterFrame Delay    =         2
Configured Speed      =      0   Clocking            =  External
Encoding              =    NRZ
Protocol Enabled      =    Yes
```

Statistics

Use the **statistics** command to display the current statistics of any level of the X.25 configuration.

Syntax:

statistics

all

frame

packet

physical

all Displays the statistics for the packet, frame, and physical levels.

frame Displays the statistics for the frame level.

Example:

```
statistics frame
Frame Layer Counters:      Received            Transmitted
Information Frames              0                     0
RR Command                      0                     0
RR Response                     0                     0
RNR Command                     0                     0
RNR Response                    0                     0
REJ Command                     0                     0
REJ Response                    0                     0
SABM                            0                    71
SABME                           0                     0
UA                              0                     0
DISC                            0                     0
DM                              0                     0
FRMR                            0                     0
Total Bytes                     0                     0
Frame Layer Miscellaneous:
Queued Output Frames = 0 Protocol Layer State = Link Setup
Send Sequence N(S)   = 0 Receive Sequence N(R)= 0
```

packet

Displays the statistics for the packet level.

Example:

```
statistics packet
Packet Counters:           Received            Transmitted
Call Request                    0                     0
Call Accepted                   0                     0
Clear Request                   0                     0
Clear Confirm                   0                     0
Interrupt Request               0                     0
Interrupt Confirm               0                     0
RR Packet                       0                     0
RNR Packet                      0                     0

Reset Request                   0                     0
Reset Confirm                   0                     0
Restart Request                 0                     0
```

```
Restart Confirm               0                    0
Diagnostic                    0                    0
Data Packet                   0                    0
Data Bytes                    0                    0
Buffers Queued                0                    0
Invalid Packets Received =    0
Switched Circuits Opened =    0
```

physical

Displays the statistics for the physical level.

Example:

```
statistics physical
 X.25 Physical Layer Counters:
  Rx Bytes                      0   Tx Bytes                   0

  Adapter cable:          V.35 DTE

   Nicknames:    RTS CTS DSR DTR DCD
   PUB 41450:    CA  CB  CC  CD  CF
   State:        ON  ON  ON  ON  ON

  Line speed:             unknown
  Last port reset:        12 minutes, 21 seconds ago

 Input frame errors:
  CRC error                     0   alignment (byte length)         0
  missed frame                  0   too long (>     0 bytes)        0
  aborted frame                 0   DMA/FIFO overrun                0
Output frame counters:
  DMA/FIFO underrun errors      0   Output aborts sent          0
```

X.25 Network Interfaces and the GWCON Interface Command

While X.25 interfaces have their own monitoring processes for monitoring purposes, the router also displays complete statistics for installed network interfaces when you use the **interface** command from the GWCON environment. (For more information on the **interface** command, refer to Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands).

Statistics Displayed for X.25 Interfaces

The following statistics display when you run the **interface** command from the GWCON environment for X.25 interfaces:

```
+interface 11
                                                Self-Test  Self-Test  Maintenance
Nt Nt'  Interface  Slot-Port                    Passed     Failed     Failed
11 11   X25/0      Slot: 8  Port: 1                 1          0          0

  X.25 MAC/data-link on V.35/V.36 interface
Interface State:  DCD  CTS   Packet Layer    Frame Layer
                  ON   ON        UP            UP
  Packet Counters:           Received            Transmitted
  Data Packet                     0                   353
  Data Bytes                      0                 18888
  Buffers Queued                  0                     0
  Invalid Packets Received =      0
  Switched Circuits Opened =      0

   Frame Layer Counters:      Received            Transmitted
   Information Frames            354                   354

   X.25 Physical Layer Counters:
   Rx Bytes                     3316   Tx Bytes               22204

     Adapter cable:               V.35 DTE

     V.24 circuit: 105 106 107 108 109
     Nicknames:    RTS CTS DSR DTR DCD
     PUB 41450:    CA  CB  CC  CD  CF
     State:        ON  ON  ON  ON  ON

   Line speed:              64.000 Kbps
```

```
   Last port reset:         1 hour, 20 minutes, 25 seconds ago

   Input frame errors:
    CRC error                          0   alignment (byte length)            0
    missed frame                       0   too long (>  2057 bytes)           0
    aborted frame                      0   DMA/FIFO overrun                   0
   Output frame counters:
    DMA/FIFO underrun errors           0   Output aborts sent                 0
 Interface buffer pool: Total = 57, Free = 56
```

The following list describes the interface statistics:

Nt Global interface number

Nt ' Reserved for future dial circuit use

Interface
Interface name and number (within interfaces of the same type)

Slot Slot number of interface

Port Port number of interface

Self-Test Passed
Number of times self-test succeeded

Self-Test Failed
Number of times self-test failed

Maintenance Failed
Number of maintenance failures

Interface state
Display the current state of the input modem control signals, the packet layer (X.25 layer 3), and the frame layer (X.25 layer 2).

Packet Counters
Provides statistics on packets received and transmitted.

Data Packets
Displays the number of data packets the interface transmits receives on the network

Data Bytes
Displays the number of data bytes the interface transmits receives on the network.

Buffers Queued
Displays the number of buffers currently queued for transmission over the network. These may be frame or packet layer supervisory messages as well as forwarder packets.

Invalid Packets Received
Displays the number of invalid X.25 packets received from the network.

Switched Circuits Open
Displays the number of switched circuits currently open.

Frame Layer Counters
Provides statistics generated from Frame Layer counters.

Information Frames
Displays the number of X.25 Information frames the interface has transmitted and received.

X.25 Physical Layer Counters
Provides statistics generated from Physical Layer counters.

RX Bytes
Display the number of bytes received by the Physical layer.

TX Bytes
Displays the number of bytes transmitted by the Physical layer.

Line speed
The transmit clock rate.

Last port reset
The length of time since the last port reset.

Input frame errors:

CRC error
The number of packets received that contained checksum errors and as a result were discarded.

Alignment
The number of packets received that were not an even multiple of 8 bits in length and as a result were discarded.

Too short
The number of packets that were less than 2 bytes in length and as a result were discarded.

Too long
The number of packets that were greater than the configured size, and as a result were discarded.

Aborted frame
The number of packets received that were aborted by the sender or a line error.

DMA/FIFO overrun
The number of times the serial interface card could not send data fast enough to the system packet buffer memory to receive them from the network.

Missed frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the `L & F bits not set` counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the `L & F bits not set` counter will be affected by traffic.

Output frame counters:

DMA/FIFO underrun errors
The number of times the serial interface card could not retrieve data fast enough from the system packet buffer memory to transmit them onto the network.

Output aborts sent
The number of transmissions that were aborted as requested by upper-level software.

Chapter 23. Using XTP

This chapter describes the X.25 Transport Protocol (XTP) for transporting X.25 traffic over TCP/IP. Included are the following sections:

The X.25 Transport Protocol

X.25 Transport Protocol (XTP) provides you with the services of a "protocol forwarder." A protocol forwarder is the focal point for inbound and outbound protocol packet processing. Forwarders receive packets on one network interface and send them to another interface.

XTP is designed to work with X.25 devices that are situated at multiple remote sites. In such environments, XTP can eliminate the use of X.25 packet-switched networks for communicating with servers at one or more centralized locations.

To enable this, you use routers at the server and remote locations to encapsulate the data and deliver the X.25 packets between the clients and server via TCP/IP.

Figure 16 on page 284 illustrates a network configuration before and after using XTP.

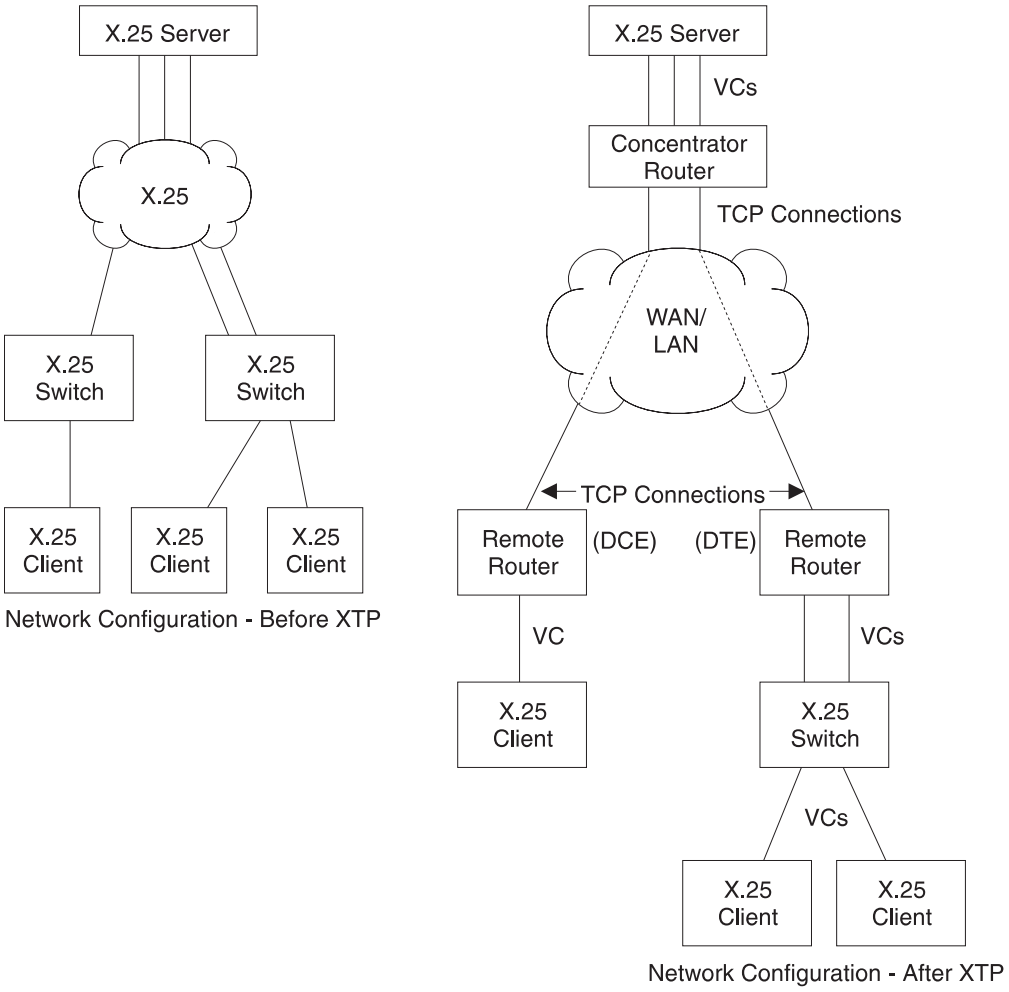

Figure 16. Configuration Before and After XTP

Configuration Information

X.25 recognizes an incoming call for XTP based on the node addresses configured for XTP. Therefore, in order to transport X.25 traffic between the X.25 nodes, you must configure X.25 to map to the data terminal equipment (DTE) address and IP addresses of the routers to which the nodes are connected.

For example, in Figure 16, you configure X.25 clients on remote routers and on the concentrator router. *Remote routers* in this example are the routers that connect the X.25 clients to the TCP/IP network that is used to access the X.25 server; the *concentrator router* connects the X.25 server to the TCP/IP network that is used to access the remote routers.

Note: When you configure XTP, if a router is connected to an X.25 switch, it is considered to be DTE. If it is not connected to a switch, it is considered to be DCE (Data Circuit-Terminating Equipment).

To configure a router for XTP, define the following information from the `XTP config>` prompt and then restart the router:

- Local DTEs
- Peer routers

- Remote DTEs
- PVCs
- CUGs

Local DTEs
X.25 nodes connected to the X.25 interfaces on the router

To configure local DTEs, use the X.121 address that is assigned to the local DTE. Multiple local DTEs can be configured on an interface.

Peer Routers
Routers with which you communicate over TCP/IP

Peer routers can differ depending on "point of view". For example, in Figure 16 on page 284, the *two remote routers* are the peer routers from the perspective of the concentrator router. However, the *concentrator router* is the peer router from the perspective of the two remote routers.

You designate the peer router by its internal IP address.

Remote DTEs
Remote X.25 nodes to which the local X.25 nodes open connections and exchange data. Use the X.121 address that is assigned to the remote DTE.

Configure a *unique* IP address for each peer router. For example, in Figure 16 on page 284, the concentrator router must know the unique IP address of each remote router, and each remote router must know the IP address of the concentrator router.

PVC A permanent channel that remains connected after X.25 restarts.

PVCs, because they are constant channels, are similar to leased telephone lines. A PVC, in the XTP context, is a PVC from a local X.25 DTE node to a remote X.25 DTE.

When you configure a router for PVCs, map the IP address of the peer router and the PVC number of the remote and local DTE. A PVC is identified by four pieces of information which are the:

- Logical channel numbers of the local PVCs
- X.121 address of the local DTE
- Logical channel numbers of the PVCs on the remote (peer) router
- X.121 address of the remote DTE

CUGS The closed user groups for the XTP protocol. See "Understanding Closed User Groups" on page 245.

Additional configuration information can be found at "Configuring XTP" on page 288 and at "XTP Configuring Commands" on page 297.

DTE Address Wildcards

The "*" wildcard is available for DTE address configuration. This is in addition to the "?" character that can be specified in a DTE address to represent any one digit in that position in the address. For example, a specification of "1?2?3" can match address 18243 where the first, third, and fifth digits are 1, 2, and 3, respectively.

The "*" wildcard character can represent any string of zero or more digits. Its use is limited to the end of a DTE address specification. For example: "123*", "5555*", "9*"

or "*". The special case of a DTE address of "*" represents any DTE address, even a null address. The null address is useful for handling incoming calls with no calling address in the X.25 Call Request packet.

Use of the "*" wildcard increases the chances for adding a local or a remote DTE address that conflicts with an existing address. The **add local-dte** and **add remote-dte** commands are enhanced to provide the conflicting address when the user attempts to add a DTE address that conflicts with an existing address.

Example: `xtp config>` **`add local-dte`**

```
Interface number [0]? 1
DTE address [ ] 123456
DTE address [ ]?

XTP config>add local-dte
Interface number [0]?1
DTE address [ ]?1*
DTE address conflicts with existing DTE address 123456
```

XTP Backup Peer Function

The Backup Peer Function allows the association of multiple peer routers with a remote DTE. The user specifies a list of peer routers associated with a remote DTE.

Example:

```
XTP config>add rem
DTE address [ ]?123456
Peer router's internal IP Address [0.0.0.0]?10.0.0.2
Peer router's internal IP Address [0.0.0.0]?10.0.0.4
Peer router's internal IP Address [0.0.0.0]?11.0.0.1
Peer router's internal IP Address [0.0.0.0]?
```

When an incoming call for the remote DTE is received, a connection is attempted through each router in the list in the same order that they appear for the remote DTE.

Searching for a Remote DTE

When a DTE initiates a call for a remote DTE, both DTE addresses are inspected to determine if they are acceptable for X.25 transport. If they are acceptable, the X.25 Transport protocol forwarder determines through which peer router to attempt to complete the call. It starts with the first router in the remote DTE's list of peer routers in its search. The first condition that must be met is an active TCP connection to the peer router. If there is not an active TCP connection to the peer, the next router in the list is checked. When an active TCP connection is found, an attempt is made to complete the call. The Connection Request Timer is started to time the call connection process.

The remote DTE search is terminated by one of the following events:

- Successful completion of the call through the peer router

  This completes call setup processing and ends the search for the remote DTE.
- Rejection of the call by the peer router

  This causes the search for the remote DTE to proceed to the next router in the peer router list.
- Expiration of the Connection Request Timer

This causes the search for the remote DTE to proceed to the next router in the peer router list.

If a pass through the list of peer routers is completed without a successful connection through any of the peer routers, the call to the local DTE is cleared.

Connection Request Timer

The Connection Request Timer is used to ensure that no call setup procedure hangs for an indeterminable time. There is a timer configured for each peer router.

Example:

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?10.0.0.2
Connection setup timeout [230]?60
```

The Connection Request Timer can be configured from 10 to 480 seconds. The default is 230 seconds. This default was determined based on the fact that the default setting for the X.25 Call Request Timer is 200 seconds.

The timer is started when an attempt is made to complete a call through a peer router. It is stopped when the call attempt is either accepted or rejected by the peer router.

Local XTP

Local XTP allows you to route incoming X.25 traffic to the same or different interfaces on the current router. To configure local XTP, specify the router's internal IP address as a peer address on the **add peer** command.

XTP and Closed User Groups

XTP supports closed user groups through the local DTE address defined by the **add local** or the **add cug** command. To enable XTP to use closed user groups, you must:

- Enable CUG or BI-CUG on the appropriate X.25 interfaces.
- Supply the XTP protocol-specific CUGs using the **add cug** and **add bi-cug** commands, if desired.
- Supply the appropriate closed user group numbers in the **add local** command. These include:
  - Closed user group number
  - Preferred closed user group number
  - Bilateral closed user group number
  - Preferred bilateral closed user group number
- Enable CUG insertion or deletion for the interface in the **national enable cug_insertion** or **national enable cug_deletion** commands, if desired.
- Enable the CUG 0 override option on the **national enable cug 0 override** command, if desired.

Configuring XTP

XTP is a protocol forwarder used to transport X.25 traffic over TCP/IP. XTP allows existing X.25 devices to communicate over a TCP/IP backbone and migrate from an X.25 network to a network of your choice.

Configuration Procedures

This section defines the detail for configuring the network displayed in Figure 17.

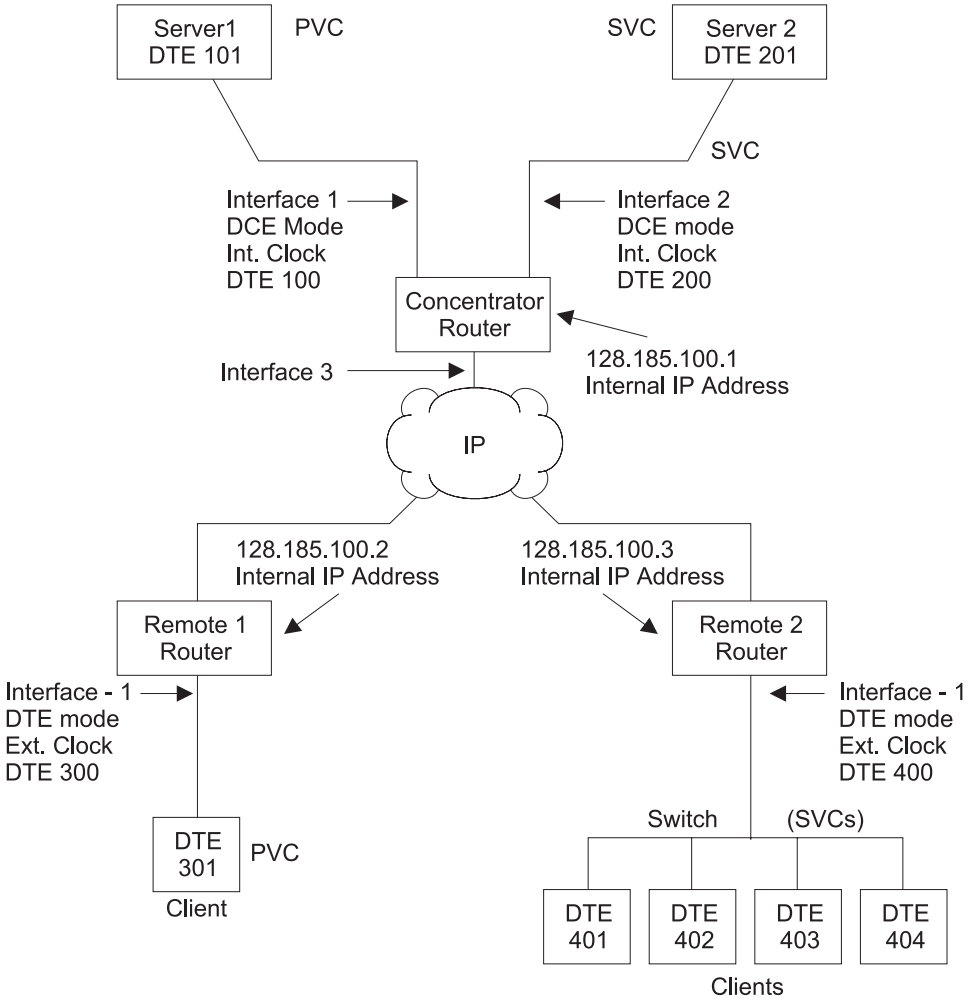

Figure 17. Sample XTP Configuration

This configuration shows three routers, the Concentrator router, Remote 1 router, and Remote 2 router. To make XTP operational on this network, perform the following steps for each of these routers:

- Set the data link
- Configure the IP interface
- Configure X.25
- Set the National Personality values
- Define the IP address

- Set the Internal IP address
- Configure XTP

Note: New configurations do not take effect until you restart the router.

Setting the Data Link

The data link defines the protocol you are using to send data packets over the network. Define the data link between the router you are configuring and each serial interface. The example in Figure 17 on page 288 configures a concentrator router with three serial interfaces, two for X.25 and one for PPP.

Set the data-link protocol for the serial interfaces:

```
Config>set data-link X25 1
Config>set data-link x25 2
Config>set data-link ppp 3
```

Configuring the IP Interface

In Figure 17 on page 288, the IP interface is PPP; enter **network 3** at the `Config>` prompt to configure this PPP interface:

```
Config>network 3
PPP interface configuration
```

Note: This procedure does not include details about the configuration of PPP. For details, refer to *Software User's Guide*

Configuring X.25

Before configuring XTP, configure the X.25 parameters for each interface. The following example configures the basic parameters for X.25 and is based on the topology in Figure 17 on page 288.

The parameters you need to configure depend on your network topology. For details about all the X.25 parameters, refer to *Software User's Guide*

Interface 1

Use the following instructions to configure *Interface 1* on the concentrator router as defined in Figure 17 on page 288.

1. At the `Config>` prompt, enter **network** followed by the number of the X.25 interface. In this example, it is interface 1.

   ```
   Config>network 1
   X.25 User Configuration
   X.25 Config>
   ```

2. Add the XTP protocol to the X.25 interface and define general interface values. Enter **add protocol xtp** at the X.25 `Config>` prompt. This command needs to be entered *one time only*.

   ```
   X.25 Config>add protocol xtp
   Window Size [2]?
   Default Packet Size [128]?
   Maximum Packet Size [256]?
   ```

3. Specify the network address by entering **set address** `X.25 node address`. In Figure 17 on page 288, the node address (DTE address) is 100.

   ```
   X.25 Config>set address 100
   ```

4. Enter **set clocking** followed by **internal** or **external** based on your router type.

```
X.25 Config>set clocking internal
```

5. Enter **set speed** followed by the access rate (line speed).

```
X.25 Config>set speed
Access rate in bps [9600]?19200
```

6. Enter **set equipment-type** and specify whether the frame and packet levels act as DCE or DTE.

```
X.25 Config>set equipment-type dce
```

7. Enter **set pvc** and define the lowest and the highest PVC you are using.

```
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
```

8. Enter **add pvc** to define individual PVCs.

```
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?
Destination X.25 Address [ ]?101
Window Size [2]?
Packet Size [128]
```

9. (Optional) Enter **national enable truncate-called-addresses**. If you want to truncate the called address size, enter **national set truncate-called-addr-size** followed by the number of digits to truncate the called DTE address to.
10. (Optional) Enable CUG support, CUG insertion, and CUG deletion as required.

Interface 2

Use the following instructions to configure interface 2.

1. At the Config> prompt, enter **network** followed by the number of the X.25 interface. In Figure 17 on page 288, it is 2.

```
Config>network 2
X.25 User Configuration
X.25 Config>
```

2. Use the same procedures as defined in “Interface 1” on page 289 to set the following parameters for interface 2:
   - address = 200
   - clocking = internal
   - speed = 19200
   - equipment = dce
3. Enter **set svc** and define the lowest and highest SVC you are using.

   There are three types of SVCs: two-way, inbound and outbound. The defaults are “svc low-two-way = 1” and “svc high-two-way = 64.” All other SVC types default to 0. For additional information on SVCs and PVCs, refer to *Software User’s Guide*

```
X.25 Config>set svc ?
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low outbound 0
X.25 Config>set svc high outbound 0
X.25 Config>set svc low-two-way 2
X.25 Config>set svc high-two-way 2
```

4. Exit the X.25 Config> prompt.

```
X25 Config>exit
Config>
```

Setting the National Personality

Each X.25 public network has its own standard configuration. The National Personality refers to a group of 28 variables that define the characteristics of the public data network. These variables provide the router with control information for packets transferred over the link and influence the X.25 facilities used between and XTP router and its local DTE.

All facilities contained in incoming call requests are passed on to the peer router, regardless of whether the local router was configured to support that facility. For example, when packet size negotiation is requested in the incoming call and flow control negotiation is not configured in the router.

The router will insure any packet size and window size being negotiated is within the range specified when defining the X.25 interface. For example, a packet window greater than 7 is negotiated down to 7 if packet-ext-seq-mode has not been defined for the X.25 interface.

To view the configuration values, enter **list detailed** at the `X.25 Config>` prompt. To set the default values for the national personality, enter **set national-personality** at the `X.25 Config>` prompt. For further information, refer to *Software User's Guide*

Defining the IP Address

Before you configure the Concentrator router (as displayed in Figure 17 on page 288) for XTP, define the IP address for this router. Enter **protocol ip** at the `Config>` prompt and enter **add address** at the `IP config>` prompt.

```
Config>protocol ip
IP config>add address
Which net is this address for [0]?3
New address [0.0.0.0]?128.185.100.7
Address mask [255.255.0.0]?255.255.255.0
```

Setting the Internal IP Address

Each router identifies its peer routers by the internal IP address of the peer routers.

To set the internal IP address of the peer router, enter **set internal IP address** at the `IP Config>` prompt.

```
IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.1
```

Configuring XTP

After you have configured X.25 and defined the IP address, you are ready to configure XTP for the router.

If you need further configuration information when configuring XTP, see "XTP Configuring Commands" on page 297.

Note: When configuring your network for XTP, remember that the peer routers are always the routers you are communicating with over TCP/IP. Therefore, the peer router can differ depending on the point of view. When configuring the routers defined as Remote 1 router and Remote 2 router in Figure 17 on page 288 , to them the peer router is the Concentrator router.

Using XTP

Implement the following steps to configure XTP for the router:

1. To access the `XTP config>` prompt, enter **protocol xtp** at the `Config>` prompt.
2. Add interface 1 to the XTP configuration. Enter **add local-dte** at the `XTP Config>` prompt.

```
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?101
Pref CUG []? 18
CUG (2) []? 2
CUG (3) []?
Pref BI-CUG [0]?
DTE address [ ]?
```

   Entering a null DTE address ends the command input.

3. Add interface 2 to the XTP configuration. Enter **add local-dte** at the `XTP Config>` prompt.

```
XTP config>add local-dte
Interface number [0]?2
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?201
DTE address [ ]?
```

   Entering a null DTE address ends the command input.

4. (Optional) Add XTP protocol-specific CUGs.

```
add cug
        Pref CUG  []? 11
        CUG (2)  []? 12
        CUG (3)  []? 13
        CUG (4)  []? 14
        CUG (5)  []? 15
add bi-cug
        Pref BI-CUG  []? 21
        BI-CUG (2)  []? 22
        BI-CUG (3)  []?
```

5. Add Remote 1 router as the peer router. Enter **add peer-router** and enter the IP address of this router.

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

6. Add the remote DTE for Remote 1 router. Enter **add remote-dte** and enter the IP and DTE address of this DTE.

```
XTP config>add remote-dte
DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

   Note: A remote DTE is *required* only if one of the following applies:

   - The Concentrator Router will be initiating XTP connections to the remote DTE due to incoming calls from its local DTEs.
   - The DTE is part of an XTP PVC definition.

7. Add Remote 2 router (as the peer router). Enter **add peer-router** and enter the IP address of this router.

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.3
Connection setup timeout [230]?
```

8. Add the remote DTEs for Remote 2 router. Enter add remote-dte and enter the IP and DTE addresses of this DTE.

```
XTP config>add remote-dte
DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?402
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?

XTP config>add remote-dte
DTE address [ ]?403
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?

XTP config>add remote-dte
DTE address [ ]?404
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

9. Add an XTP PVC to logically associate the local PVC to Server 1 with the remote DTE 301.

```
XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]?301
```

When entering DTE addresses, you can specify either of the following:

A '?' in place of any digit. The '?' means any single digit in this digit position.

An '*' as the last digit of an address to represent any combination of zero or more digits.

Sample Configuration of Remote Routers

The following is a sample configuration of Remote 1 router and Remote 2 router (see Figure 17 on page 288). The process is the same as that defined in the section at “Configuration Procedures” on page 288.

Remote 1 router

```
*talk 6

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

X.25 Config>set address 300
X.25 Config>set clocking internal
X.25 Config>set speed 19200
X.25 Config>set equipment-type dce
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?1
Destination X.25 Address [ ]?301

Window Size [2]?
Packet Size [128]?
X.25 Config>exit
Config>

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.8
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.2
IP Config>exit
Config>
```

```
Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?301
DTE address [ ]?

XTP config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?101
Peer router's internal IP Address ]0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?

XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]? 301
```

Remote 2 router

```
*talk 6

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

X.25 Config>set address 400
X.25 Config>set clocking external
X.25 Config>set speed 19200
X.25 Config>set equipment-type dte
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low-outbound 0
X.25 Config>set svc high-outbound 0
X.25 Config>set svc low-two-way 1
X.25 Config>set svc high-two-way 64
X.25 Config>add protocol
Protocol [IP]?xtp
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
X.25 Config>exit

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.9
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.3
IP Config>exit
Config>

Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?401
Pref CUG  []? 23
CUG (2)  []? 24
CUG (3)  []? 25
CUG (4)  []? 26
CUG (5)  []? 27

DTE address [ ]?402
Pref CUG  []?
DTE address [ ]?403
Pref CUG  []?
DTE address [ ]?404
Pref CUG  []?
DTE address [ ]?
```

```
XTP Config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?201
Peer router's internal IP Address [0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?
XTP config>exit

Config>
```

Chapter 24. Configuring and Monitoring XTP

This chapter describe the XTP configuring and monitoring commands. It includes the following sections:

- "XTP Configuring Commands"
- "XTP Monitoring Commands" on page 304

XTP Configuring Commands

This section describes the XTP configuring commands.

To access the XTP configuring environment, enter the **protocol xtp** command at the `Config>` prompt.

```
Config> p xtp
XTP config>
```

Enter the XTP configuring commands at the `XTP config>` prompt.

Table 37. XTP Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds an interface, peer router, closed user groups, remote DTE or PVC definitions.
Change	Changes a peer router, remote DTE or PVC definition.
Delete	Deletes a local DTE, peer router, closed user groups, remote DTE or PVC definition.
Enable-XTP	Activates the XTP forwarder.
Disable-XTP	Deactivates the XTP forwarder.
Set	Sets the value of the XTP Keepalive Timer.
List	Lists interfaces, peer routers, remote DTEs and PVC definitions.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Add

Adds a local X.25 node, a peer router, a remote X.25 node with corresponding routers, or a PVC from a local X.25 node to a remote X.25 node.

Wild card addressing is included in the XTP forwarder. When the local or remote DTE addresses are entered, they can contain a wild card character (? or *). For additional information on the use of wildcards, see "DTE Address Wildcards" on page 285 .

Syntax:

add bi-cug
cug
local-dte
peer-router

remote-dte

pvc

cug Specifies the closed user group numbers for the XTP protocol. The first CUG you are prompted for is the preferred cug.

Valid values: 0 to 9999

Default value: None

Example:

```
add cug
Pref CUG []? 114
CUG (2) []? 314
CUG (3) []? 478
CUG (4) []?
```

bi-cug Specifies the bilateral closed user group numbers for the XTP protocol. The first bi-cug you are prompted for is the preferred bi-cug.

Valid values: 0 to 9999

Default value: None

Example:

```
add bi-cug
Pref BI-CUG []? 50
BI-CUG (2) []? 51
BI-CUG (3) []? 52
BI-CUG (4) []? 53
BI-CUG (5) []? 54
```

local-dte

Adds the X.25 DTE addresses, or the X.25 nodes, that communicate with the router on the specified interface. The valid interface numbers for use with XTP are 0 to 255.

You can configure multiple local nodes. However, if the option to allow incoming calls without a calling DTE address has been selected and such a call is received, the *last* local DTE address added becomes the calling DTE address for that call.

Example:

```
add local-dte

Interface number [0]?4
Allow inbound calls without calling DTE address? (Y or N) [N]? y
DTE address [ ]?101
Pref CUG  []? 23
CUG (2)  []? 24
CUG (3)  []? 25
CUG (4)  []? 26
CUG (5)  []? 27
Pref BI-CUG []? 6
BI-CUG (2) []? 7
BI-CUG (3) []? 8
BI-CUG (4) []? 9
BI-CUG (5) []? 10
DTE address [ ]?
```

peer-router

Adds peer routers. Enter the internal IP addresses of the routers to which the remote X.25 nodes are connected. You can use these IP addresses to open TCP connections and transport X.25 packets that contain connection requests and X.25 data.

If the internal IP address you configure for the peer-router is this router's internal IP address, the software establishes a local XTP connection.

Example:

```
add peer-router

Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

remote-dte

Adds remote X.25 nodes and corresponding routers. You can connect remote nodes with local X.25 nodes so they can exchange data. You must configure an IP address for each remote X.25 node you configure. Any request or data sent to this remote node goes to the router. The router then uses one of its local X.25 interfaces to forward the data to the X.25 node.

Define a remote DTE if this router is to initiate XTP connections to the remote DTE due to incoming calls from its local DTEs, or if the remote DTE is part of an XTP PVC definition.

To use Local XTP, the peer router address must be the internal address of the local router and that DTE address must be previously defined using the **add local** command.

Example:

```
add remote-dte

DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc Adds a PVC from a local X.25 node to a remote X.25 node.

Three things need to exist in order to activate a PVC configuration:

- An X.25 PVC from the router to the local X.25 node
- An X.25 PVC from the peer router to the remote X.25 node
- A TCP connection to the peer router where the remote node is resident

Example:

```
XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]? 301
```

Notes:

1. When you add PVCs to the router configuration, you also must configure the PVC in X.25. For details on configuring X.25 interfaces, refer to *Software User's Guide*
2. For Local XTP, you must define the PVC in both directions. You need this definition because the router is performing both local and remote functions. For example, to define Local PVC 8 and Remote PVC 10 when you are using Local XTP, you would do the following:

```
XTP config>add pvc
Local PVC Range Start [1]? 8
Local PVC Range End [1]? 8
Local X.25 DTE address [ ]? 108
Remote PVC Range Start [1]? 10
Remote PVC Range End [1]? 10
Remote X.25 DTE address [ ]? 301

XTP config>add pvc
Local PVC Range Start [1]? 10
Local PVC Range End [1]? 10
Local X.25 DTE address [ ]? 310
Remote PVC Range Start [1]? 8
Remote PVC Range End [1]? 8
```

```
Remote X.25 DTE address [ ]? 108
```

3. A PVC range can be defined through the PVC range start and PVC range end parameters. The same number of circuits must be defined in the local PVC range as in the remote PVC range. For example, if one circuit is defined in the local PVC range, one circuit must be defined in the remote PVC range.
4. The PVCs defined must fall within the range of 1 to 255.

Note: When you add PVCs to the router configuration, you also must configure the PVC in X.25. For details on configuring X.25 interfaces, refer to the *Software User's Guide*

Change

Changes a peer router, remote DTE, or PVC from the XTP configuration.

Syntax:

change peer-router
remote-dte
pvc

peer-router
Changes specific peer routers from the XTP configuration.

Example:

```
change peer-router

Router IP Address [0.0.0.0]?128.185.100.2
```

remote-dte
Changes specific remote DTEs in the XTP configuration.

Example:

```
change remote-dte

DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc Changes PVC definitions for all PVCs in the range defined by the Local PVC Range Start parameter.

Example:

```
change pvc
Local PVC Range Start [1]?1
Local DTE address [ ]?301
```

Delete

Deletes a local DTE, peer router, remote DTE, or PVC from the XTP configuration.

Syntax:

delete bi-cug
cug
local-dte
peer-router

remote-dte

pvc

bi-cug Deletes a bilateral closed user group number used by this interface.

Valid values:

Y Deletes the current CUG.

N Does not delete the current CUG.

ALL Deletes all remaining CUGs.

Q Stops deleting any remaining CUGs.

Example:

```
delete bi-cug
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cug Deletes the closed user group numbers used by this interface. This command works similar to the **delete bi-cug** command.

Example:

```
del cug

Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

local-dte

Deletes specific local interfaces from the XTP configuration.

Example:

```
delete local-dte

Interface number [0]?1
DTE address [ ]?101
Record deleted
```

peer-router

Deletes specific peer routers from the XTP configuration.

Example:

```
delete peer-router

Router IP Address [0.0.0.0]?128.185.100.2
Record deleted
```

remote-dte

Deletes specific remote DTEs from the XTP configuration.

Example: `delete remote-dte`

DTE address [ ]?**401**

pvc Deletes PVC definitions for all PVCs in the range defined by the Local PVC Range Start parameter.

Example:

```
delete pvc

Local PVC Range Start [1]?1
Local DTE address [ ]?301
Record deleted
```

XTP Configuring Commands (Talk 6)

Enable

Activates the XTP forwarder.

Syntax: enable-xtp

Example: **`enable-xtp`**

Disable

Deactivates the XTP forwarder.

Syntax: disable-xtp

Example: **`disable-xtp`**

Set

Sets the XTP Keepalive Timer.

Syntax: keep-alive-timer

Example:

```
set keep-alive-timer
Keepalive timer in seconds [10]?60
```

List

Lists the interfaces, peer routers, remote DTEs, or PVCs.

Syntax:

list

all
cugs
keep-alive-timer
local-dtes
peer-routers
remote-dtes
pvcs
xtp-status

all Displays all the interfaces, peer routers, remote DTEs, and PVCs configured for XTP.

Example:

```
list all
STATUS: XTP-DISABLED
Local DTEs:
Interface      DTE Address
    1          44444                    Calling DTE address is optional
             Pref CUG     : 7777  Others : 9999 0
             Pref BI-CUG  : 0     Others :
```

```
    4          33333                    Calling DTE address is optional
             Pref CUG     : 1     Others : 2 3 4 5
             Pref BI-CUG  : 6     Others : 7 8 9 10


   Peer Routers    Connection Timeout

Remote DTEs:
      DTE Address    Peer Router(s)

PVCs:
Local PVC         Local DTE      Remote PVC        Remote DTE
LCN Range         Address        LCN Range         Address

Pref CUG     : 114   Others : 314 478
Pref BI-CUG  : 1     Others : 1 1 1 1111


KEEP-ALIVE-TIMER: 10 seconds
```

cugs Lists the CUG and BI-CUG numbers defined for the XTP protocol.

keep-alive-timer
Displays all the Keepalive time configured for XTP.

local-dtes
Displays all the local DTEs configured for XTP.

Example:

```
list local-dtes

Local DTEs:
Interface        DTE Addr
   1             101 Calling DTE address is required
   2             201 Calling DTE address is required
```

peer-routers
Displays all the peer routers configured for XTP.

Example:

```
list peer-routers

Peer Routers:
128.185.100.2
128.185.100.3
```

pvcs Displays all the PVCs configured for XTP.

Example-

```
list pvcs

PVCs:

Local PVC      Local DTE      Remote PVC      Remote DTE
LCN Range      Address        LCN Range       Address
    1 - 1            100           1 - 1             301
```

remote-dtes
Displays all the remote DTEs configured for XTP.

Example:

```
list remote-dtes

Remote DTEs:
DTE Address      Peer Router
    301         128.185.100.2
    401         128.185.100.3
    402         128.185.100.3
    403         128.185.100.3
    404         128.185.100.3
```

xtp-status
Displays the status of XTP indicating whether it is enabled or disabled.

Example:

```
list xtp-status

STATUS:  XTP-ENABLED
```

XTP Monitoring Commands

This section describes the XTP monitoring commands. These commands allow you to display the current active interfaces, peer routers, remote DTE, PVCs and SVCs. They also allow you to dynamically add or delete interfaces, DTEs, or peer routers.

To display the XTP> prompt, enter **protocol xtp** at the monitoring (+) prompt:

```
+protocol xtp
X.25 Transport Console
XTP>
```

Enter the XTP monitoring commands at the XTP> prompt.

Table 38. XTP Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Add	Dynamically adds local DTEs, remote DTEs, or peer routers
Delete	Dynamically deletes configurations for local DTEs, remote DTEs, or peer routers
List	Displays individual PVC or SVC statistics and general information
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Add

Adds an interface, peer router, or remote DTE to the XTP configuration.

Syntax:

add local-dtes
peer-router
remote-dtes

local-dtes

Adds a local interface to the XTP configuration.

Example:

```
add local-dtes

Interface number [0]?1
DTE address [ ]?101
```

peer-router

Adds a peer router to the XTP configuration.

Example:

```
add peer-router

Router's IP Address [0.0.0.0]?128.185.100.2
```

remote-dtes

Adds a remote DTE to the XTP configuration.

Example:

```
add remote-dtes

Peer router's IP Address [0.0.0.0]?128.185.100.2
DTE address [ ]?301
DTE address [ ]?
```

Delete

Deletes a local DTE, peer router, or remote DTE from the router configuration.

Syntax:

delete local-dtes
peer-router
remote-dtes

local-dtes
Deletes a local interface from the XTP configuration.

Example:

```
delete local-dtes

Interface Number [0]?1
DTE address [ ]?101
DTE address [ ]?
```

peer-router
Deletes a peer router from the XTP configuration.

Example: `delete peer-router`

```
Router's IP Address [0.0.0.0]?123.185.100.2
```

remote-dtes
Deletes a remote DTE from the XTP configuration.

Example:

```
delete remote-dtes

DTE address [ ]?401
DTE address [ ]?
```

List

Displays the current active interfaces, peer routers, remote DTEs, PVCs, and SVCs.

Syntax:

list all
xtp-status
local-dtes
peer-routers
remote-dtes
pvcs
pvc-detailed
pvcs-all-detailed
svcs
svc-detailed
svc-all-detailed

all Displays output of all list command options.

Example:

```
list all


STATUS:  XTP-ENABLED
KEEP-ALIVE TIMER = 20 seconds


LIST OF LOCAL DTES
------------------
Interface     Local
  No           DTE
  1            101     Calling DTE address is required
  2            201     Calling DTE address is required


LIST OF PEER ROUTERS
--------------------
 Router             CNN      Number        Received           Sent
                   State    of  Ckts     Pkts    Bytes     Pkts    Bytes
128.185.100.3     Active      15          60      1533      12      142
128.185.100.2     Active      12          63      1620      10      130


LIST OF REMOTE DTES
-------------------
      Remote         Router
       DTE             IP
       404           128.185.100.3
       403           128.185.100.3
       402           128.185.100.3
       401           128.185.100.3
       301           128.185.100.2


LIST OF PVCS
------------
Index     Int    PVC    Local       Local   Remote      Remote
 No        No   State    LCN         DTE      LCN         DTE
  1         1   Active               100                  301


LIST OF SVCS   (list svcs)
------------
Index   Int   Logical    SVC        Local     Remote         Peer
  No     No   Channel   State        DTE        DTE        Router
  1       2       5      ACT     333333333333 4444444444444 3.3.3.3


SVC  1 IN DETAIL   (list svc-detailed)
----------------
Int    Log     SVC        Received           Sent            Dropped
 No    Chn    State      Pkts   Bytes      Pkts   Bytes      Pkts   Bytes

  2      5     ACT          2     116         2     106         0       0


LIST OF SVCS   (svcs-all-detailed)
------------
Int    Log     SVC        Received           Sent            Dropped
 No    Chn    State      Pkts   Bytes      Pkts   Bytes      Pkts   Bytes

  2      5     ACT          1       7         1       2         0       0
```

xtp-status

Displays whether XTP is enabled/disabled, and the time specified for the Keepalive Timer.

Example:

```
list xtp-status

STATUS:  XTP-ENABLED
         KEEP-ALIVE-TIMER = 20 seconds
```

local-dtes

Displays all the interfaces configured for XTP.

Example:

```
list local-dtes

LIST OF LOCAL DTES
------------------
Interface     Local
```

```
 No           DTE
 1            101     Calling DTE address is required
 2            201     Calling DTE address is required
```

peer-routers

Displays all the peer routers configured for XTP.

Example:

```
list peer-routers

LIST OF PEER ROUTERS
--------------------
 Router             CNN      Number        Received            Sent
                   State    of  Ckts     Pkts    Bytes     Pkts    Bytes
128.185.100.3     Active      15          60      1533      12      142
128.185.100.2     Active      12          63      1620      10      130
```

remote-dtes

Displays all the remote interfaces configured for XTP.

Example:

```
 list remote-dtes

LIST OF REMOTE DTES
-------------------
      Remote         Router
       DTE             IP
       404           128.185.100.3
       403           128.185.100.3
       402           128.185.100.3
       401           128.185.100.3
       301           128.185.100.2
```

pvcs Displays all the PVCs configured for XTP.

Example:

```
list pvcs

LIST OF PVCS
------------
Index     Int    PVC   Local     Local    Remote      Remote
 No        No   State   LCN       DET      LCN         DTE
  1         1   Active            100                  301
```

pvc-detailed

Displays detailed information for a specific PVC definition. For a listing of Index numbers, enter **list all** at the `xtp>` prompt.

Example:

```
list pvc-detailed

PVC Index Number [1]?1

PVC  1 IN DETAIL
----------------
Int     PVC         Received            Sent             Dropped
 No    State      Pkts     Bytes    Pkts     Bytes    Pkts      Bytes
 1     ACTIVE      55       3220     35       2350     15        1870
```

pvcs-all-detailed

Displays detailed information for all PVC definitions.

Example:

```
list pvcs-all-detailed

LIST OF PVCS
------------
INT Local     PVC         Received            Sent             Dropped
 No  LCN     State      Pkts     Bytes    Pkts     Bytes   Pkts     Bytes
 1           ACTIVE      55       3220     35       2350    15       1870
```

svcs Displays all the SVCs definitions.

Example:

```
list svcs

LIST OF SVCS
------------
Index     Int LOG    SVC       Local      Remote  Peer
 No        No Chan  State       DTE         DTE   Router
  1         1       Active      200         401   3.3.3.3
  2         1       Active      200         402   3.3.3.3
  3         2       Active      200         403   3.3.3.3
  4         2       Active      200         404   3.3.3.3
```

svc-detailed

Displays information for specific SVC definitions.

Example:

```
list svc-detailed

SVC Index Number [1]?1
SVC  1 IN DETAIL
----------------
Int  LOG    SVC        Received            Sent            Dropped
 No  Chan  State     Pkts     Bytes    Pkts     Bytes   Pkts      Bytes
  1        ACTIVE     75       4220     55       3350    20        870
```

svcs-all-detailed

Displays information for all the SVC definitions.

Example:

```
list svcs-all-detailed

LIST OF SVCS
------------
Index     Int Log    SVC         Received          Sent           Dropped
No        No  Chn  State      Pkts    Bytes   Pkts     Bytes   Pkts    Bytes
1          1       ACTIVE     4220     55     550        20     870
2          1       ACTIVE     3220     40     2350        15     970
3          2       ACTIVE     4003     50     3892        20     870
4          2       ACTIVE     3967     58     4167        12     800
```

Chapter 25. Using Frame Relay Interfaces

This chapter describes how to use the Frame Relay interface and includes the following sections:

Frame Relay Overview

The Frame Relay (FR) protocol is a method of transmitting internetworking packets by combining the packet switching and port sharing of X.25 with the high speed and low delay of time division multiplexing (TDM) circuit switching. FR allows you to connect multiple LANs to a single high-speed (1.54 Mbps) WAN link with multiple point-to-point virtual circuits (VCs). FR offers the following features:

- *High throughput and low delay.* Utilizing the *core aspects* (error detection, addressing, and synchronization) of the Link Access Protocol, D-Channel (LAPD) datalink protocol, FR eliminates all network layer (Layer 3) processing. By using only the core aspects, FR reduces the delay of processing each frame.
- *Congestion detection.* Upon receiving Backward Explicit Congestion Notification (BECN) or a Forward Explicit Congestion Notification (FECN), the router initiates a controlled slowdown of traffic, thereby avoiding a complete FR network shutdown.

  The router can also initiate a slowdown of traffic when it receives a Consolidated Link Layer Management (CLLM) congestion message. CLLM is an optional part of the Frame Relay standards that provides additional management information about the operation of the frame relay network to attaching DTEs.
- *Circuit access and control.* As the router dynamically learns about the availability of non-configured circuits (orphan circuits), you can control access to those new circuits.
- *Network management option.* As your network requires, the FR protocol can operate with or without a local network management interface.
- *Multiplexing protocols.* Using one VC to pass multiple protocols.
- *Data compression* that supports the FRF.9 standard. See Using the Data Compression Subsystem in *Using and Configuring Features* for details.
- *Data encryption* using a proprietary encryption scheme. See Overview of Encryption in *Using and Configuring Features* for details.

FR provides no error correction or retransmission function. To provide error–free end-to-end transmission of data, FR relies on the intelligence of the host devices.

Frame Relay Network

The FR network consists of the FR backbone (consisting of FR switches provided by the FR carrier) providing the FR service. The router functions as the FR connection device. The router encapsulates FR frames and routes them through the network based on a Data Link Connection Identifier (DLCI). The DLCI is the medium access control (MAC) address that identifies the PVC or SVC between the router and the FR destination device. For example, in Figure 18, a packet destined to go from router B to router D would have a DLCI of 19 to reach router D; however, a packet destined to go from router D to router B would have a DLCI of 16.

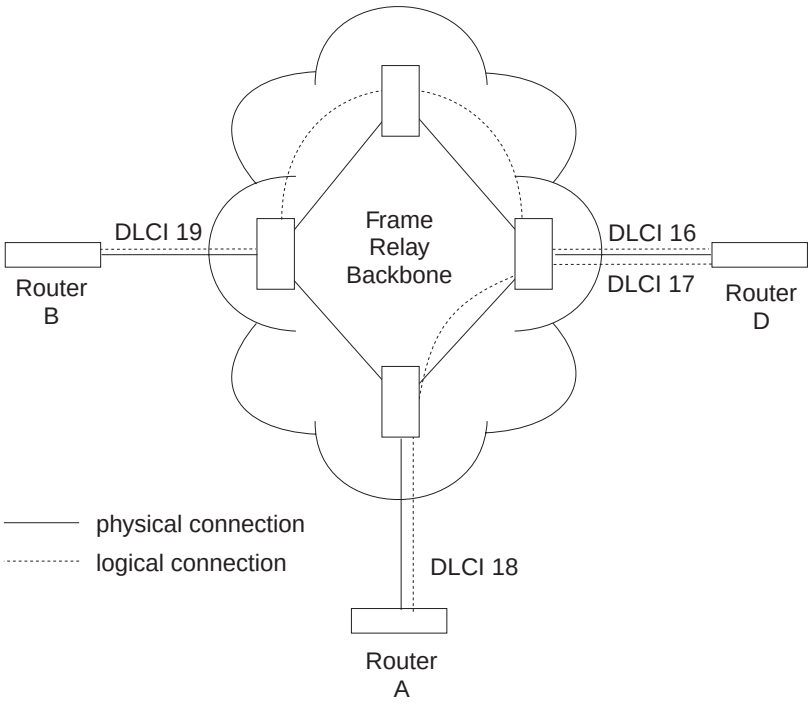

Figure 18. DLCIs in Frame Relay Network

A DLCI can have either local or global significance. Local DLCIs are significant at the point of entry to the network, but global DLCIs are significant throughout the network. To the user, however, the DLCI that the router uses to route a packet is the DLCI that the user associates with the frame's global or local destination. DLCIs are configured through the FR configuration process or learned through FR management.

FR PVCs are predefined connections used to route data through a FR network. The bandwidth allocated for a PVC within the network is a subscription option and must be allotted to the PVC whether or not the PVC uses it.

A Frame Relay network has the following characteristics:

- Transports frames transparently. The network can modify only the DLCI, congestion bits, and frame check sequence. High-Level Data Link Control (HDLC) flags and zero bit insertion provide frame delimiting, alignment, and transparency.
- Detects transmission, format, and operational errors (frames with an unknown DLCI)

- Preserves the ordering of frame transfer on individual VCs
- Does not acknowledge or retransmit frames

Frame Relay Switched Virtual Circuits

Frame Relay Switched Virtual Circuits (SVCs) provide the ability to implement ″cut-through″ routing in a Frame Relay network, minimizing or eliminating intermediate router hops between DTEs. Network complexity can be simplified and the DTE may experience improved performance.

SVCs may replace PVCs to conserve network bandwidth, reducing bandwidth cost.

FR SVC standards are a subset of ISDN standards and provide many of the same advantages as ISDN with less complexity.

The following protocols are supported over FR SVCs:

- AppleTalk 2
- ARP
- Bridging
- DECnet IV
- DLSw
- IP/OSPF/RIP/BGP4
- IPX

SVCs cannot be required and cannot belong to a required group.

Frame Relay Interface Initialization

Local Management Interface (LMI) is used to determine the status of PVCs on a Frame Relay interface. If an LMI is enabled, the FR interface is active when a successful exchange of LMI frames occurs between the router and the FR switch; however, no data can be received from or transmitted to another router until an LMI status message indicates that the PVC status for the DLCI to the other router is active. Also, there are instances where the FR interface state is tied to PVC states and the interface does not come up even if LMI or Q.922 exchanges are successfully occurring (for additional information, see “Configuring PVC States to Affect the Frame Relay Interface State” on page 313).

If LMI is not enabled and SVCs are enabled, the Frame Relay interface is active when a successful exchange of Q.922 frames occurs between the router and the adjacent device. All PVCs are considered active at this point. However, SVCs are active only after a successful Q.933 activation exchange.

PVC status appears for all PVCs as either active or inactive. An active PVC has a completed connection to an end system. An inactive PVC does not have a completed connection to an end system because either an end system or an FR switch is off-line.

For example, in Figure 19 on page 312 router B has a configured PVC to router D. Router B is successfully interacting with FR management through FR switch B. Because either another FR switch is down or the end system is down, the

end-to-end PVC connection is not established. Router B receives an inactive status for that PVC.

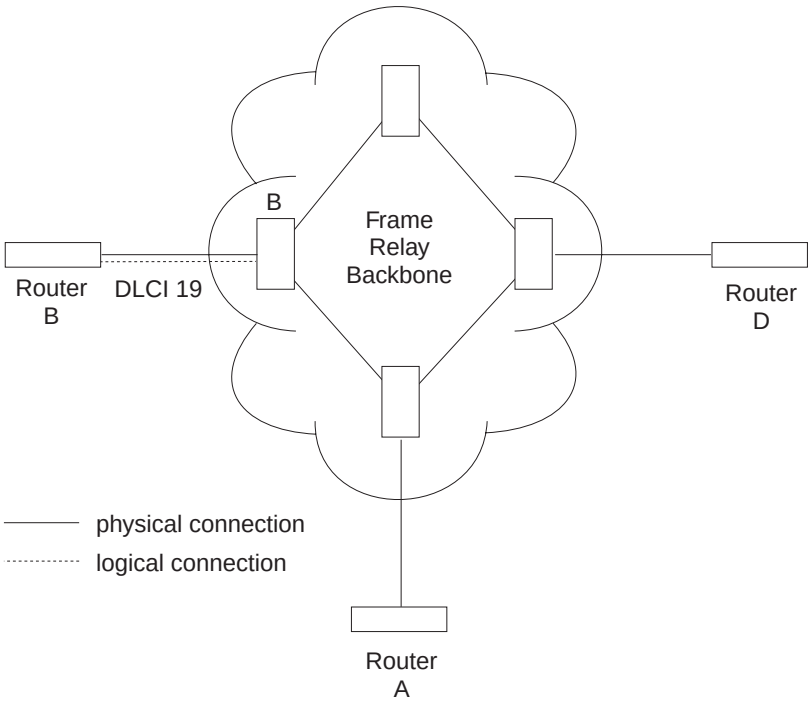

Figure 19. DLCIs in Frame Relay Network

When the LMI and SVCs are disabled, the FR interface is running on a serial line and a DTE cable is being used, the FR protocol asserts the DTR and RTS modem control signals. (The Control signal is asserted for X.21). The FR interface goes up once the DSR, CTS, and DCD modem control signals are on. (When X.21 is used, the FR interface goes up once the Indication modem control signal is on.) The FR interface is down or in the testing state if either DSR, CTS, or DCD are off or, when X.21 is used, the Indication signal is off. Therefore, you need to ensure that the modem, modem eliminator, or DSU that is used drops one or more of these signals when the physical connection to the FR switch or the other FR DTE (if configured for FR DTE to DTE connectivity) is lost.

Orphan Circuits

An orphan permanent virtual circuit is any PVC that is not configured for your router but is learned indirectly through the actions of the network management entity. For example, Figure 20 on page 313 assumes that router B has a configured PVC to router D, but none to router A. Router A configures a PVC to router B. Router B would then learn about the PVC to router A from LMI messages and classify it as an orphan.

Orphan PVCs are treated the same as configured circuits except that you may enable or disable their use with the **enable orphan-circuit** and **disable orphan-circuit** commands.

By disabling orphan circuits, you add a measure of security to your network by preventing any unauthorized entry into your network from a non-configured circuit.

By enabling orphan circuits, you allow the router to forward packets over circuits you did not configure. Packets that would normally be dropped are now forwarded.

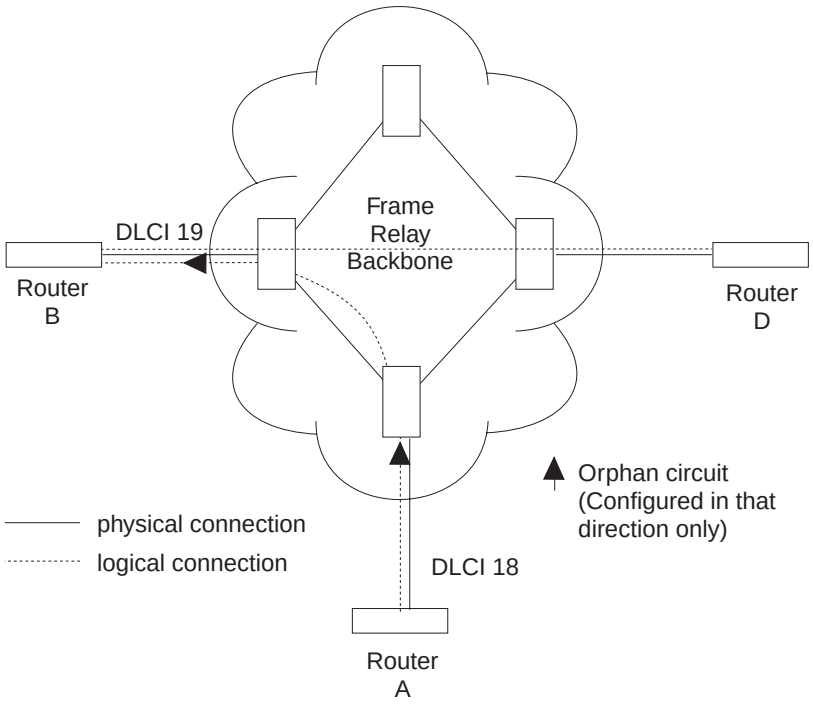

Figure 20. Orphan Circuit

An orphan switched virtual circuit is an SVC that is not configured for your router but is created when a call-in is received for it. This is similar to Figure 20. However, Q.933 messages are used instead of LMI to generate the circuit and associate the appropriate parameters with it. Orphan SVCs are treated the same as configured SVCs except that you may enable or disable their use with the call-in option of the **enable switched-virtual-circuit** command.

Configuring PVC States to Affect the Frame Relay Interface State

You can control the operation of your Frame Relay interface by

1. Enabling the “No-PVC” feature or
2. Configuring “required PVCs” or
3. Configuring “required PVC groups”.

By enabling the Frame Relay “No-PVC” feature, the Frame Relay interface becomes inactive when there are no active PVCs on the interface. If at least one PVC is active, the Frame Relay interface becomes active when a successful LMI exchange occurs between the router and the FR switch.

You can configure a PVC as a “required PVC”. If a PVC is required but not in a group, the Frame Relay interface becomes inactive when the PVC becomes inactive. When the PVC becomes active, the interface is activated following a successful exchange of LMI frames between the router and the Frame Relay switch.

Using Frame Relay

If multiple PVCs are required and are not in a PVC group, the interface is not activated until all required PVCs are active.

If a required PVC belongs to a PVC group, the Frame Relay interface becomes inactive when all PVCs in the PVC group are inactive. If at least one PVC in the group is active, the interface becomes active following a successful exchange of LMI frames between the router and the FR switch. If there are multiple PVC groups, the interface does not become active until at least one PVC *in each group* is active.

A “required PVC group” is a group of circuits associated by name, where “name” is the name of the required PVC group.

These features can be used with WAN Reroute so that an alternate link can be brought up if all PVCs, required PVCs, or a group of PVCs become inactive on the primary FR link.

Frame Relay Frame

An FR frame consists of a fixed size address field with variable sized encapsulated user data. Figure 21 illustrates a Frame-Relay frame format.

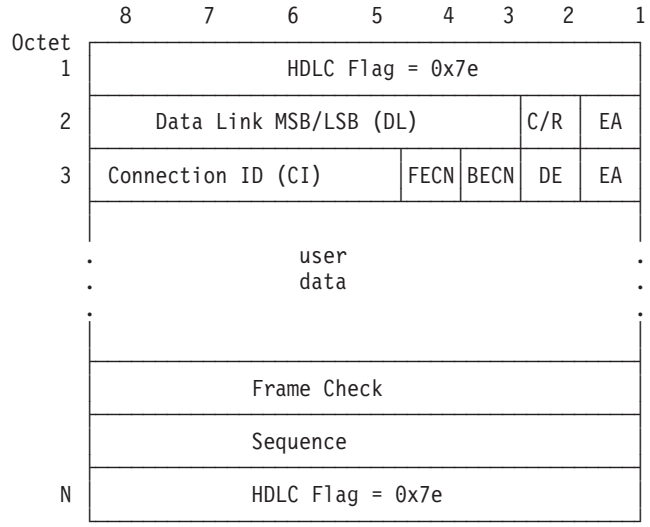

Figure 21. Frame-Relay Frame Format

HDLC Flags

Located in the first and last octet, these flags indicate the beginning and end of the frame.

Data Link Connection Identifier (DLCI)

This 10-bit routing ID resides in bits 3 to 8 of octet 2 and bits 5 to 8 of octet three. The DLCI is the MAC address of the circuit. The DLCI allows the user and network management to identify the frame as being from a particular PVC. The DLCI enables multiplexing of several PVCs over one physical link.

Command/Response (C/R)

This field's use is not defined within the Frame-Relay standards and the field is passed transparently across the network.

Extended Address

This version of FR does not support extended addressing.

Forward Explicit Congestion Notification (FECN)

The FR backbone network sets this bit to 1 to notify the user receiving the frame that congestion is occurring for the PVC in the direction the frame is being sent. You can configure the device to slow down data transmission in the direction from which it receives a FECN using the **enable throttle-transmit-on-fecn** command. You can also set the BECN bit in data frames sent to the originator of the FECN using the **enable notify-fecn-source** command.

APPN High Performance Routing (HPR) uses detection of this bit set to allow Rapid Transport Protocol's adaptive rate-based flow and congestion control algorithm to adjust the data send rate. This algorithm prevents traffic bursts and congestion, maintaining a high level of throughput.

Backward Explicit Congestion Notification (BECN)

The FR backbone network sets this bit to 1 to notify the user that the frames sent by this router for this PVC have encountered congestion. The router then initiates a *throttle down* to a rate equal to or less than the user-defined CIR when CIR or congestion monitoring are enabled. The CIR for a PVC is supplied by the FR service provider and is configured using the **add permanent-virtual-circuit** command.

Discard Eligibility (DE)

The Frame Relay network may discard transmitted data exceeding CIR on a PVC. The DE bit can be set by the router to indicate that some traffic should be considered discard eligible. If appropriate, the Frame Relay network will discard frames marked as discard eligible which may allow frames that are not marked discard eligible to make it through the network. To identify traffic that is discard eligible:

1. Configure BRS on the Frame Relay interface and any FR circuits that has traffic that you are making discard eligible.
2. Assign a protocol or filter to a BRS traffic class using the **assign** command. You specify whether the DE bit should be set on for this protocol or filter traffic.

User Data

This field contains the protocol packet being transmitted. This field can contain a maximum of 8188 octets; however, the frame check sequence (FCS) can effectively detect errors only on a maximum of 4096 octets of data. The protocol data is preceded by a Frame Relay encapsulation header as defined in RFC 1490.

Frame Check Sequence

This field is the standard 16-bit cyclic redundancy check (CRC) that HDLC and LAPD frames use. This field detects bit errors occurring in the bits of the frame between the opening flag and FCS.

Frame Forwarding over the Frame Relay Network

When the FR protocol receives a packet for encapsulation, it compares the packet's network address to the entries in the Address resolution Protocol (ARP) cache. If the ARP cache contains the DLCI number that matches the network address, the FR protocol encapsulates that packet into a frame and transmits the frame over its specified local DLCI. If the ARP cache does not contain a match, the FR protocol sends out an ARP request over all configured PVCs on the interface. When the appropriate end-point responds with an ARP response, the FR protocol adds its local DLCI that received the ARP response to the ARP cache. Subsequent data packets directed to the same network address are then encapsulated into a frame and sent out over its local DLCI.

Protocol Addresses

Protocol addresses can be either mapped statically to FR network PVC addresses or SVCs using locally configured names or discovered dynamically through Inverse ARP or ARP. (For more information on ARP and Inverse ARP, see the *Protocol Configuration and Monitoring Reference*.) Either method is protocol-dependent as illustrated in Table 39.

Note: Static protocol addresses are also referred to as static ARP entries. A static ARP entry is added to the configuration with the **add protocol-address** command.

Table 39. Protocol Address Mapping

Protocol Type	ARP and Inverse ARP Usage	Static Mapping	VC Configured at Protocol Configuration
AP2	Yes	Yes	No
IP	Yes	Yes	No
IPX	Yes	Yes	No
Banyan VINES**	No	No	No
DNA IV	Yes	Yes	No
OSI*, **	No	No	Yes

* You must configure OSI at the protocol level to map the protocol address to the FR PVC.
** Not supported using SVCs.

Multicast Emulation and Protocol Broadcast

Multicast emulation is an optional feature that allows protocols requiring multicast such as ARP to function properly over the FR interface. With multicast emulation, a multicast frame is transmitted on each active PVC. By using the **enable** and **disable multicast** commands, you can turn this feature on or off. Protocols that utilize multicast are AP2, ARP, Banyan VINES, DNA4, IP, and IPX.

Protocol broadcast is another optional feature that allows the IP RIP protocol to function properly over the FR interface. By using the **enable protocol-broadcast** and **disable protocol-broadcast** commands, you can turn this feature on or off.

For protocols that support ARP/InARP over Frame Relay, Frame Relay will only multicast a protocols packets over a circuit if a protocol address was either learned or configured for that circuit.

Multicast can also be enabled or disabled for an individual SVC. Use the multicast option on **add switched-virtual-circuit**.

Frame Relay Network Management

The supplier of the FR network backbone provides FR network management. It is management's responsibility to provide FR end-stations (routers) with status and configuration information concerning PVCs available at the interface.

For PVCs, the FR protocol supports the ANSI T1.617 Annex D, ITU-T Q.933 Annex A (also referred to as CCITT Q.933 Annex A), and the Interim Local Management Interface (LMI) management entities. You can turn these entities on or off using the **enable** and **disable** LMI configuration commands. Specifically, FR LMI provides the following information:

- Notification of additional PVCs (orphans) and whether they are active or inactive, or notification of any PVC deletions.
- Notification of the availability of a configured PVC. The availability of a PVC is indirectly related to the successful participation of the PVC end-point in the *heartbeat polling* process, which is detailed in "Link Integrity Verification Report" on page 318.
- Verification of the integrity of the physical link between the end-station and network by using a *keep alive* sequence number interchange.

Although the FR interface supports PVC network management, it is not necessary for management to run on the FR backbone for the interface to operate over the FR backbone. For example, you may want to disable management for back-to-back configurations.

For SVCs, the FR protocol supports FRF 4 (Frame Relay Forum Implementation Agreement 4). This includes an implementation of ANSI Q.922 and a subset of ANSI Q.933. Q.922 provides verification of the integrity of the physical link between the router and the network. Q.933 provides the means for establishing and disconnecting SVCs across the network. Q.922 and Q.933 are always enabled when SVCs are used.

Management Status Reporting

Upon request, FR LMI provides two types of status reports, a full status report and a link integrity verification report. A full status report provides information about all PVCs the interface knows about. A link integrity verification report verifies the connection between a specific end station and a network switch. All status inquiries and responses are sent over DLCI 0 for ANSI T1.617 Annex D and ITU-T Q.933 Annex A, or DLCI 1023 for interim LMI management.

Full Status Report

When the FR interface requires a full status report, the router's FR protocol sends a status enquiry message to the FR network backbone requesting a full status report. A status enquiry message is a request for the status of all PVCs on the interface. Upon receiving this request, FR management must respond with a full status report consisting of the link integrity verification element and a PVC status information element for each PVC. (See "Link Integrity Verification Report" on page 318.)

The PVC status information element contains the following information: the local DLCI number for the particular PVC; the state of the PVC (active or inactive); and whether the PVC is new or an existing PVC that management already knows about.

Note: The number of PVCs supplied at the FR interface is restricted by the network frame size and the amount of individual PVC information elements that can fit into a full status report. For example, 202 is the maximum number of PVCs for a network with a 1K frame size.

Link Integrity Verification Report

The link integrity verification report, sometimes referred to as *heartbeat polling*, contains the link integrity verification element. This element is where the exchange of the send and receive sequence numbers takes place. By exchanging sequence numbers, management and the end station can evaluate the integrity of the synchronous link. The send sequence number is the current send sequence number of the message originator. The receiver looks at this number and compares it to the last send sequence number to verify that this number is incrementally correct. The receive sequence number is the last send sequence number that the originator sent out over the interface. It is the receiver's responsibility to place a copy of the send sequence number into the receive sequence number field. This way the originator can ensure that the receiver receives and interprets the frames correctly.

When an end-station fails to participate in this polling process, all remote end-stations with logically attached PVCs are notified through management's full status report mechanism that the PVC is inactive.

Consolidated Link Layer Management (CLLM)

CLLM is an optional FR management function that is not widely supported by the industry but it has been adopted by some Frame Relay switch manufacturers. CLLM provides some of the same management information provided by LMI, in particular, outage notification. CLLM's main use is to provide asynchronous congestion notification of PVCs to attaching devices. A single CLLM message may indicate outage or congestion for multiple PVCs. The Frame Relay protocol supports the following standards for CLLM: ANSI T1.618, ITU-T (CCITT) Q.922 Annex A, and ITU-T (CCITT) X.36 Annex C.

Frame Relay Data Rates

This section introduces data rates for Frame Relay permanent virtual circuits (PVCs).

Committed Information Rate (CIR)

The CIR is the data rate that the network commits to support for the VC under normal, uncongested conditions. Any VC that is configured or is learned is provided a CIR (by the FR service provider). The CIR is a portion of the total bandwidth of the physical link of either 0 or between 300 bps and 2 Mbps * reserved for the VC. 64 Kbps or a single DS0 channel is most common.

You define the CIR with the **add permanent-virtual-circuit**, **change permanent-virtual-circuit**, **add switched-virtual-circuit**, or **change**

switched-virtual-circuit configuration command. You can also dynamically change the CIR with the **set circuit** console command. You can also set the default CIR for all Frame Relay circuits on this interface using the **set CIR-defaults** command.

Some Frame Relay switches allow a value of 0 to be configured for CIR. When CIR is equal to 0, little or no bandwidth is reserved in the Frame Relay network backbone for the VC, and the VC's traffic uses non-reserved bandwidth.

Orphan Permanent Virtual Circuit CIR

The router assigns a CIR to orphan circuits based on the CIR defaults configured at the interface level. If you are relying on the orphan circuit to route important data and the CIR, Bc, and Be values from the network provider are different from the values configured at the interface level, it is recommended that you define a PVC instead of an orphan circuit. Doing this, you can assign a CIR that the network commits to support.

Committed Burst (Bc) Size

The *committed burst (Bc) size* is the maximum amount of data (in bits) that the network commits to deliver during a *calculated time (Tc) interval*. The Tc is equal to the Bc divided by the CIR (Tc = Bc / CIR). If you configure 0 for CIR, Frame Relay uses a value of 1 second for Tc..

For example, if you set a VC's CIR to 9600 bps and the committed burst size to 14 400 bits, the time period is 1.5 sec. (14 400 bits / 9600 bps = 1.5 sec). This means that the VC is allowed to transmit a maximum of 14 400 bits in 1.5 seconds.

Note: The minimum Tc supported by FR is .1 second.

This parameter is important because of the relationship between the committed burst size and the maximum frame size. If the maximum frame size in bits is greater than the committed burst size, the network may discard frames whose size exceeds the committed burst size. Therefore, the committed burst size should be greater than or equal to the maximum frame size. It should also equal the burst size set up with the network provider.

Use the **add permanent-virtual-circuit**, **change permanent-virtual-circuit**, **add switched-virtual-circuit** or **change switched-virtual-circuit** configuration commands to set the committed burst size. The **set circuit** console command can be used to dynamically change the committed burst size. You can also set the default committed burst size for all Frame Relay circuits on this interface using the **set CIR-defaults** command.

The device assigns orphan circuits a committed burst size based on the default you set with the **set CIR-defaults** command. If you configure 0 for CIR, then the committed burst (Bc) size also equals 0.

Excess Burst (Be) Size

The *excess burst (Be) size* is the maximum amount of uncommitted data the router can transmit on a PVC in excess of the Bc during the Tc (Tc = Bc / CIR) when CIR and Bc are nonzero. When CIR = 0, Frame Relay used a value of 1 second for Tc.

The network delivers this excess data with a lower probability of success than committed burst size data. Set the Be to a value greater than zero only if you are willing to accept the risk of discarded data and its effect on higher-layer protocol performance. The Be should equal the value set up with the network provider.

Use the **add permanent-virtual-circuit**, **change permanent-virtual-circuit**, **add switched-virtual-circuit** or **change switched-virtual-circuit** commands during frame-relay configuration to set the excess burst size. You can also use the **set circuit** console command to dynamically change the excess burst size. Orphan circuits will receive a default excess burst size equal to the value set in the **set CIR-defaults** command. If you configure 0 for CIR, then you must configure a nonzero value for the excess burst (Be) size. You can also set the default excess burst size for all Frame Relay circuits on this interface using the **set CIR-defaults** command.

Line Speed

The *line speed* is the interface's line speed.

The FR interface's line speed is configured using the **set line-speed** configuration command. The line speed must be configured when internal clocking is used. However, it is recommended that you configure a line speed for external clocking since the router uses the line speed as the maximum information rate when congestion monitoring is enabled. Also some of the protocols use an interface's configured line speed when calculating a route's cost.

The line speed is not configurable on a Frame Relay dial circuit interface. If the dial circuit is mapped to an ISDN base interface, 64 Kbps is used as the line speed.

For dial circuits using Channelized T1/E1 as the base net, the line speed is 64 Kbps times the number of timeslots assigned or 56 Kbps if you set the bandwidth of the Channelized circuit to 56 Kbps. For example, if you set the number of timeslots for a Channelized circuit to 3, the line speed is 192 Kbps (3 * 64 Kbps).

If the dial circuit is mapped to a V.25bis base interface, the line speed of the V.25bis interface is used for the FR dial circuit.

Minimum Information Rate

The *minimum information rate (IR)* is the minimum data rate for a VC that the router throttles down to when it is notified of congestion. You set the minimum IR as a percentage of CIR using the **set ir-adjustment** configuration command. It can be dynamically changed using the **set ir-adjustment** console command. If you configure CIR equal to 0, the minimum IR is 1500 bps.

Maximum Information Rate

The *maximum information rate* is the maximum data rate at which the router transmits for a VC. If the CIR monitoring feature is enabled and CIR and Bc are nonzero, the maximum information rate is calculated using CIR, Bc, and Be as follows:

```
( Bc + Be ) per Tc interval
```

If the CIR monitoring feature is enabled and CIR and Bc are configured equal to 0, the maximum information rate is equal to the excess burst size (Be) per second.

If the CIR monitoring feature is not enabled the maximum information rate is equal to the line speed.

Variable Information Rate

The *variable information rate* (VIR) ranges from the configured minimum IR to the calculated maximum IR when the CIR monitoring or congestion monitoring features are enabled. The VIR is gradually decreased down to the minimum information rate when the router is notified of congestion on a circuit and is gradually increased to the maximum information rate when the router stops receiving congestion notifications. Using the **set ir-adjustment** configuration command, you configure the percentage of the information rate by which the VIR should decrease when the router is notified of congestion. You also use this command to configure the percentage of the information rate by which the VIR should be gradually increased when the congestion ends.

To avoid impulse loading of the network, the router initially sets the VIR to CIR when the VC becomes active. If you configure 0 for CIR, VIR is initially set to excess burst (Be) times the MIR adjustment percentage. For example, if Be is set to 64 000 and the MIR adjustment percentage is set to 25%, then the initial VIR would be equal to 16 000 bps.

The VIR can actually exceed the maximum value in one case. If the length of a frame in bits is greater than the maximum IR, Frame Relay transmits the frame anyway.

Circuit Congestion

Circuit congestion occurs for one of the following reasons:

- The sender is transmitting faster than the allowable throughput
- The receiver is too slow when processing the frames
- An intermediate backbone link is congested, resulting in the sender transmitting faster than the available throughput allows.

When circuit congestion happens, the network must drop packets and/or shut down.

In response to circuit congestion, the router implements a *throttle down*, which is a step-wise slowing of packet transmission to the configured minimum IR. Throttle down occurs during the following conditions:

- Circuit congestion is occurring.
- The router is the sender of frames.
- CIR monitoring or congestion monitoring is enabled.

This section discusses monitoring of Frame Relay data rates and circuit congestion.

CIR Monitoring

CIR monitoring is an optional Frame Relay feature that you can set for each interface to prevent the router from creating congestion conditions in the FR network. CIR monitoring allows the VIR for a VC to range between the configured minimum and maximum IR.

CIR monitoring is configured with the **enable cir-monitor** configuration command and is disabled by default. CIR monitoring, when enabled, overrides congestion

monitoring. You can also dynamically enable and disable CIR monitoring using the **enable cir-monitor** and **disable cir-monitor** console commands.

Congestion Monitoring

Congestion monitoring is an optional feature, set per interface, that allows the VIR of VCs to vary in response to network congestion. The VIR assumes values between the minimum IR and a maximum IR of the line speed. Congestion monitoring is enabled by default. It can be disabled with the **disable congestion-monitor** configuration command and re-enabled with the **enable congestion-monitor** command. You can also dynamically enable and disable congestion monitoring using the **enable congestion-monitor** and **disable congestion-monitor** console commands.

CIR monitoring, if enabled, overrides congestion monitoring. If both CIR monitoring and congestion monitoring are disabled, the VIR for each VC on the interface is set to the line speed and does not decrease in response to network congestion.

Note: Even with compression enabled, the device uses the uncompressed size of frames to determine if the VIR is being exceeded.

Congestion Notification and Avoidance

When congestion occurs, the FR backbone network is responsible for notifying the sender and receiver by sending out a FECN or a BECN signal. FECN and BECN are bits that are set in a frame to notify the DTEs at each end of a VC that congestion is occurring. FECN indicates that congestion is occurring in the same direction from which the frame was received; the sender is causing the congestion. BECN indicates that the frames sent by this DTE are causing network congestion.

Optionally, the network can use CLLM messages to convey congestion information for PVCs. CLLM messages are sent only to the congestion source and should be treated similarly to BECN messages by the DTE.

The example in Figure 22 on page 323 shows a congestion condition at switch B when frames are sent from router X to router Y. The FR backbone network notifies router X that frames it sends are encountering congestion by setting the BECN bit in frames sent to router X. The FR backbone network also notifies router Y that frames it receives encountered congestion by setting the FECN bit.

When the router receives a frame containing BECN, it is the router's responsibility to throttle down the VC's VIR (variable information rate) if either CIR monitoring or congestion monitoring is enabled. The router does this gradually as it receives consecutive frames with BECN until either the minimum IR is reached or a frame without BECN arrives. FR switches often set BECN in multiple frames after reaching a congestion threshold. In order for FR to avoid overreacting to network congestion when the network is setting multiple frames with BECN, FR will decrease a VC's VIR at most once every second. This allows the VIR to decrease gradually. As the router receives consecutive frames without BECN, the VIR gradually rises to the maximum IR.

Depending on the operation of the FR network, it may be necessary for the device to throttle down the VC's VIR when the device receives a FECN to minimize the overall amount of traffic being offered to the network as quickly as possible. Reducing the overall load on the network reduces the number of packets discarded

for all VCs to relieve congestion. Enabling the ***throttle-transmit-on-fecn*** parameter, along with either the CIR or congestion monitoring options, causes the device to treat a FECN like a BECN thus reducing overall FR network congestion when any congestion notification is received. Use the throttle-transmit-on-fecn parameter only in FR networks whose queuing methods do not provide dedicated buffers for both input and output. If the ***throttle-transmit-on-fecn*** is enabled, FR will decrease a VC's VIR at most once every second for each BECN or FECN received.

Some FR network switches set FECN to indicate congestion but do not set BECN. To provide congestion notification to the source of the congestion, enable the ***notify-fecn-source*** parameter allowing the device to set BECN in frames that it transmits over a VC on which it has received a FECN. This action provides a signal to the device that is causing the network congestion to throttle down its VC's VIR.

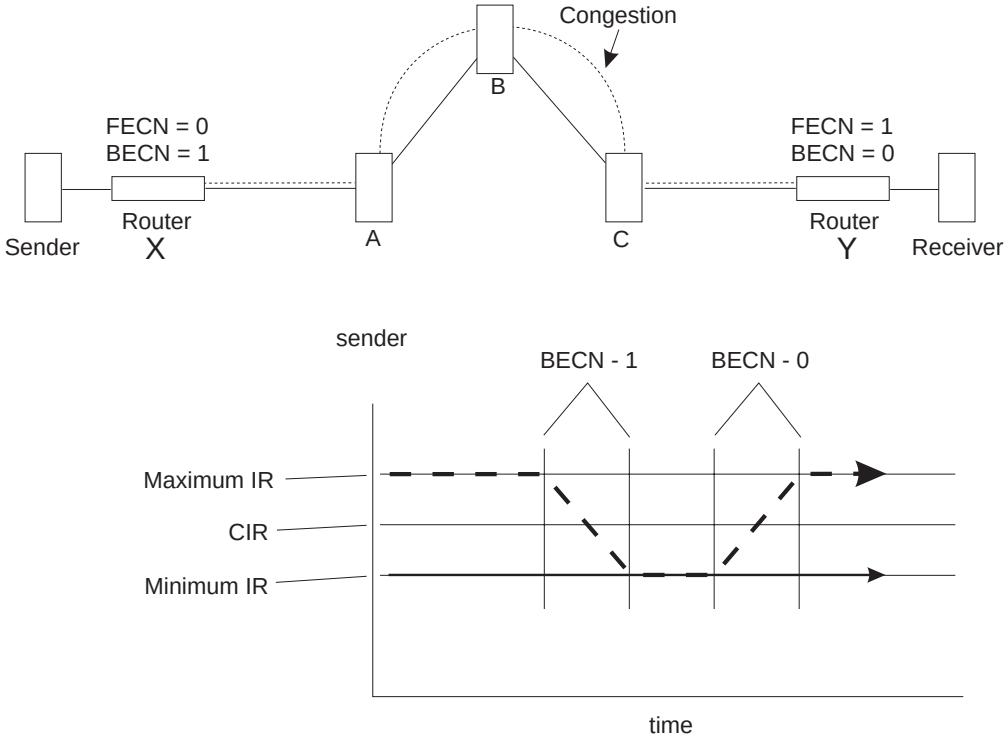

Figure 22. Congestion Notification and Throttle Down

Note: If multiple DLCIs are configured between two end-stations when congestion occurs, it is possible that a second DLCI may be used to transmit data at a higher throughput until the congestion condition on the first DLCI is corrected.

Similarly, if the network provider supports CLLM, you can configure Frame Relay to *throttle down* its transmit rate for PVCs contained in a CLLM message. CLLM messages contain a cause code that indicates the type and severity of the problem being reported. The device reacts differently depending on the cause code and the CIR configured for each PVC contained in the CLLM message. When the device receives a CLLM message that indicates:

- A short-term condition, and the configured CIR for the PVC is nonzero, the Frame Relay protocol will throttle the transmit rate for the affected PVCs by the configured IR decrement percentage.

- A long-term condition, the Frame Relay protocol will set the transmit rate for the affected PVCs to the calculated minimum information rate.
- Facility or equipment failure or maintenance action, or if the CIR was configured as zero, the FR protocol will continue to transmit any queued data for the affected PVCs but will not accept any more outgoing packets from the upper layer protocols until the congestion condition is cleared.

Once a CLLM message for a PVC has been received, if the device does not receive any CLLM messages or BECNs within the *Ty* timer period or if a frame without a BECN is received, the device will consider the congestion condition cleared and gradually return the PVC to its configured transmission rates. If you are using CLLM to control congestion, you must not configure DLCI 1007 for any other use.

Bandwidth Reservation over Frame Relay

For information on bandwidth reservation over Frame Relay, refer to Using Bandwidth Reservation and Priority Queuing and Configuring and Monitoring Bandwidth Reservation in *Using and Configuring Features*.

Displaying the Frame Relay Configuration Prompt

To access the Frame Relay configuration environment:

1. At the OPCON prompt (*), type **talk 6**.
2. At the configuration prompt (Config>), enter the **list devices** command to see a list of interfaces configured on the router.
3. Enter the **network** command to display the Frame Relay configuration prompt. The network number is the number of the Frame Relay interface.

```
Config>network
What is the network number [0] 2
Frame Relay user configuration
FR 2 Config>
```

4. At the Frame Relay interface configuration prompt (FR Config>), use the commands discussed in this chapter to configure Frame Relay parameters.

Frame Relay Basic Configuration Procedure

This section outlines the minimum configuration steps that you are required to perform to get the Frame Relay protocol up and running. If you desire any further configuration information and explanation, refer to the configuration commands described in this chapter.

Note: You must restart the router for new configuration changes to take effect.

- **Select FR management.** The FR Local Management Interface (LMI) protocol defaults to ANSI. You have the option of connecting to a network using the Interim LMI (REV1), ANSI T1.617 Annex D management, or ITU-T/CCITT Q.933 Annex A management. Use the **enable** and **set** commands to enable and set the required management.
- **Add a PVC.** Add any required PVCs that are needed if FR management is disabled or orphan circuits are disabled. If you want to bridge over a FR PVC, or if you want to run APPN over a FR PVC, you also must configure that PVC. Use the **add permanent-virtual-circuit** command.

- **Configure FR destination addresses.** If you are running a protocol such as IP or IPX over the FR interface, and are interconnecting with devices not supporting the Address Resolution Protocol (ARP) or Inverse ARP on FR, use the **add protocol-address** command to add the static protocol and address mapping.
- **Configure Bandwidth Reservation over Frame Relay.** In addition to the basic Frame Relay configuration, which must be done, you can also configure Bandwidth Reservation (an optional feature) over Frame Relay. For information on configuring Bandwidth Reservation, refer to Using Bandwidth Reservation and Priority Queuing in *Using and Configuring Features*.
- **Configure Discard Eligibility.** You can configure Discard Eligibility (DE) congestion control using Bandwidth Reservation. For information on configuring Discard Eligibility, refer to Using Bandwidth Reservation and Priority Queuing in *Using and Configuring Features* .
- **Configure Data Compression.** You can configure data compression for Frame Relay. For information on configuring data compression, refer to Using Data Compression in *Using and Configuring Features* .

Enabling Frame Relay PVC Management

There are three management options under Frame Relay:

- Interim Local Management Interface Revision 1
- ANSI T1.617 Annex D management
- ITU-T/CCITT Q.933 Annex A management.

Frame Relay defaults to ANSI enabled. If you want to change management types, or if you want to re-enable ANSI management, use the following procedure. Enabling management over Frame Relay is a two-step process:

1. Enter the **enable lmi** command at the `FR Config>` prompt to enable management activity.
2. Enter the **set lmi-type** command to select the type of management for the interface.

   See Table 40 for details of the management types available using the **set** command.

   An example of how to set these management types is shown after the table. Also, refer to the **enable** and **set** command sections in this chapter for more information.

Table 40. Frame Relay Management Options

Command	Options	Description
set	lmi-type rev1	Conforms to LMI Revision 1 (Stratacom s Frame Relay Interface Specification)
set	lmi-type ansi	Conforms to ANSI T1.617 ISDN-DSS1-Signalling Specification for Frame Relay Bearer Service (known as Annex D)
set	lmi-type ccitt	Conforms to Annex A of ITU-T/CCITT Recommendation Q.933 - DSS1 Signalling Specification for Frame Mode Basic Call Control.

Example:

```
enable lmi

set lmi-type ansi
```

Enabling Frame Relay SVC Management

Frame Relay SVC management is automatically enabled when SVCs are enabled.

Chapter 26. Configuring and Monitoring Frame Relay Interfaces

This chapter describes the Frame Relay configuration and operational commands and includes the following sections:

- "Frame Relay Configuration Commands"
- "Accessing the Frame Relay Monitoring Prompt" on page 354
- "Frame Relay Monitoring Commands" on page 355
- "Frame Relay Interfaces and the GWCON Interface Command" on page 367

Note: For information on monitoring bandwidth reservation over Frame Relay, refer to Configuring and Monitoring Bandwidth Reservation in *Using and Configuring Features*.

Frame Relay Configuration Commands

This section describes the Frame Relay configuration commands. Enter all commands at the `Frame Relay>` prompt.

You must restart the router for new configuration changes to take effect. Table 41 lists the commands.

Table 41. Frame Relay Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds PVCs, Required PVC groups, SVCs, and destination protocol addresses to the Frame Relay interface.
Change	Modifies a PVC, SVC or Required PVC group previously defined by the **add** command.
Disable	Disables any enabled Frame Relay features.
Enable	Enables Frame Relay features such as circuit monitoring, management options, multicast, protocol-broadcast, and orphans.
List	Displays the current configuration of the LMI, PVCs, Required PVC groups, SVCs, HDLC information, and protocol addresses.
LLC	Configures LLC parameters on the Frame Relay interface. These LLC parameters are required when running APPN over the Frame Relay interface.
Remove	Deletes any previously added PVCs, SVCs, or required PVC groups (if empty), or protocol addresses.
Set	Configures the Frame Relay management options and parameters (N1-parameter, N2-parameter, N3-parameter, P1 parameter, and T1-parameter). Configures the physical-layer parameters for FR serial interfaces. Sets the maximum frame size.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Note: In this section, the terms *circuit number* and *PVC* are synonymous with the term DLCI (Data Link Circuit Identifier).

Add

Use the **add** command to add a PVC, Required PVC group, or destination protocol address supported by the Frame Relay interface.

Syntax:

add permanent-virtual-circuit . . .

protocol-address . . .

pvc-group . . .

switched-virtual-circuit . . .

permanent-virtual-circuit

Adds a PVC to the Frame Relay interface beyond the reserved range 0 through 15. The maximum number of PVCs that can be added is approximately 992, but the actual number of PVCs that the interface can support depends on the throughput required for each PVC, the line speed, the type of protocols running on the interface, and the number of local management interface PVC information elements that can fit in the maximum frame size.

Example:

```
add permanent-virtual-circuit
Circuit Number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign Circuit name []?
Is circuit required for interface operation [N]?
Does the circuit belong to a required PVC group [N]?
What is the group name []?
Do you want to have data compression performed [Y]?
Do you want to have data encryption performed [N]? y

Data encryption requires a key that is 16 hexadecimal characters long
You will be asked to enter the key twice for security reasons

Please enter the key for the first time now

A valid encryption key has been entered

Please confirm the key by entering it again

The encryption keys match - the key has been accepted
```

Circuit Number

Indicates the circuit number for this PVC.

Valid Values: 16 to 1007.

Committed Information Rate

Indicates the committed information rate (CIR). The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps. For more information, see “Committed Information Rate (CIR)” on page 318. The maximum is the value of the default CIR configured for the interface.

Note: The default value is determined according the CIR-defaults set at the interface level.

Committed Burst Size

The maximum amount of data in bits that the network agrees to deliver during a measurement interval equal to committed burst (Bc)

size / CIR seconds. The range is 300 to 2048000 bits. The maximum value is value of the default committed burst configured for the interface.

Notes:

1. The default value is determined according the Bc defaults set at the interface level.
2. If CIR is configured as 0 then the committed burst size is set to 0 and you are not prompted for a value. For additional information, see “Committed Burst (Bc) Size” on page 319.

Excess Burst Size

The maximum amount of uncommitted data in bits in excess of committed burst size that the network attempts to deliver during a measurement interval equal to (Committed Burst Size/CIR) seconds. Range is 0 to 2 048 000 bits. The maximum value is the value configured for excess burst size for the interface. For additional information, see “Excess Burst (Be) Size” on page 319.

Note: The default value is determined according the Be defaults set at the interface level.

Assign Circuit Name

Indicates the ASCII string that is assigned to describe the circuit. The default is unassigned.

Is the circuit required for operation

Specify Y or N to indicate whether the circuit is required for interface operation.

Does the circuit belong to a required PVC group

This prompt is displayed only for circuits that are required. Specify Y or N to indicate whether the circuit should belong to a required PVC group.

What is the group name

Enables you to specify the name of the required PVC group when the PVC is defined as belonging to a required group. Enter a question mark (?) for a list of currently defined groups.

Do you want to have compression performed

Enables you to specify whether or not the circuit will compress data packets. This question appears only if compression is enabled on the interface.

Note: If you enable compression on a PVC and exceed the interface’s compression circuit limit, you will get a message. Compression will be performed on the circuit, if possible – that is, the active compression limit has not been exceeded when the circuit becomes active. Compression limit includes the number of compression contexts allocated to SVCs as well as PVCs.

Do you want to have data encryption performed

Enables you to specify whether or not the circuit will encrypt data packets. This question appears only if encryption is enabled on the interface. The prompts for the encryption key will only appear if you respond “yes” (or “y”) to this question.

Specifying the Encryption Key: The encryption key is 16 hexadecimal characters long. You must specify the encryption key as a value between X'0000000000000000' and X'FFFFFFFFFFFFFFFF'.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95 .

protocol-address

This command adds statically configured destination protocol (protocol-name) addresses to the Frame Relay interface. Statically configured destination protocol addresses are useful if neither Inverse ARP nor ARP is an option, or for other reasons such as security. Adding protocol name and address mappings (static ARP) is less efficient than Inverse ARP or ARP.

- Inverse ARP is the preferred, efficient method because of dynamic address mapping with no broadcasts.
- ARP is recommended if Inverse ARP is not an option. It is less efficient than Inverse ARP because it uses address broadcast and mappings are relearned at regular intervals.

This parameter prompts you for different information depending on the type of protocol that you are adding.

Example:

```
add protocol-address
Protocol name or number [0]?
```

IP protocol:

```
IP Address [0.0.0.0]?
Circuit Number or name [16]?
```

IPX protocol:

```
Host Number (in hex)[]?
Circuit Number or name [16]?
```

AppleTalk Phase 2 protocol:

```
Network Number (1-65279) []?
Node Number (1-253) []?
Circuit Number or name[16]?
```

DN protocol:

```
Node address [0.0]?
Circuit Number or name[16]?
```

Protocol name or number

Defines the name or number of the protocol that you are adding. If you should specify an unsupported protocol, the system will prompt you with the error message:

```
Unknown protocol name, try again
```

For example, you may have erroneously specified one of the following:

```
Prot#  Name
0      IP
4      DN
7      IPX
22     AP2
```

To see a list of supported protocol types, type ? at the `Protocol name or number [IP]?` prompt.

IP Address
Defines the 32-bit Internet address in dotted-decimal notation of the remote IP host.

Host Number
Defines the 48-bit IPX node address of the remote IPX host.

Network Number
Defines the AppleTalk Phase 2 network number of the remote AppleTalk host.

Node Number
Defines the node number of the interface attached to the remote AppleTalk host.

Node address
Defines the DECnet node address of the remote DECnet host. Configure the node address in the format *x.y*, where *x* is a 6-bit area address and *y* is a 10-bit node number.

Circuit Number or name
Defines the PVC by DLCI or name or SVC by name that this remote protocol address is associated with.

pvc-group *groupname*
Adds a required PVC group name.

Note: SVCs may not belong to a required PVC group.

switched-virtual-circuit
Adds a switched virtual circuit (SVC). The SVC will act similar to a PVC except that the SVC's bandwidth will be allocated for it dynamically by the FR network only when the SVC is active. The number of SVCs that can be added is similar to the number of PVCs that can be added in that the number depends on the throughput required for each circuit, the line speed, etc. However, since the bandwidth for an SVC is only reserved when the SVC is active, it may be possible to support more SVCs over an interface than PVCs.

```
FR 4 Config>add switched-virtual-circuit
Circuit name []? svc01
Remote party number []? 12345
Remote party number numbering plan (E.164 or X.121) [E.164]?
Remote party number type (Unknown or International) [International]?
Remote party subaddress in hexadecimal []? 01
Remote party subaddress format (private or NSAP) [private]ı?
Requested outgoing Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable outgoing Committed Information Rate (CIR) in bps [64000]?
Requested incoming Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable incoming Committed Information Rate (CIR) in bps [64000]?
Requested outgoing Committed Burst size (Bc) in bits [64000]?
Requested incoming Committed Burst size (Bc) in bits [64000]?
Requested outgoing Excess Burst size (Be) in bits [0]?
Requested incoming Excess Burst size (Be) in bits [0]?
Idle timer in seconds [60]?
Establish circuit to learn remote protocol addresses [Y]?
Is multicast required for this circuit [Y]?
Are call-ins allowed for this circuit [Y]?
```

Circuit name
Specifies the circuit name for the SVC. This name will be used to associate the call with both a protocol and a BRS definition and will be used to identify a connection instead of a circuit number.

Valid Values: A 1 - 32 character ASCII string

Default Value: The name is required and must be unique for this interface

Remote party number
Specifies the remote destination's Frame Relay address.

Valid Values: A 1 - 20 character string of decimal digits

Default Value: None

Remote party numbering plan
Specifies the format of the remote party number. The numbering plan must match that used by the FR network.

Valid Values: E.164 (ISDN) or X.121 (Data)

Default Value: E.164

Remote party number type
Specifies the destination Frame Relay party number type. The number type must match that used by the FR network.

Valid Values: International or Unknown

Default Value: International

Remote party subaddress
Specifies the party entity (for example, protocol) within the destination node. If the subaddress is used, it will be matched to the remote device's subaddress. The subaddress at both ends of the connection must be the same.

The format of the **remote party subaddress** can be:

- NSAP

  The number of digits entered must be even and in the range of X'0' - X'F'.

- Private

  If the encoding is BCD, then an odd number of digits in the range of 0 - 9 can be entered.

  If the encoding is not BCD, then an even number of digits in the range of X'0' - X'F' can be entered.

The combination of **remote party number** and **remote party subaddress** must be unique on this interface. If parallel connections between two router interfaces is required, the subaddress must be used to uniquely identify each switched virtual connection definition.

Valid Values: 1 - 40 character hexadecimal string

Default Value: None

Requested outgoing throughput (CIR)
Specifies the requested outgoing CIR. The network will provide this bandwidth, if available.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps.

Default Value: Default value is determined according to CIR-defaults at the interface level

Minimum acceptable outgoing Committed Information Rate (CIR)
Specifies the minimum CIR that will be accepted if the network cannot provide the requested CIR.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps with a maximum of the **requested outgoing throughput (CIR)**.

Default Value: Default value is determined according to CIR-defaults at the interface level

Requested incoming CIR
Specifies the requested incoming CIR.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps.

Default Value: Value of the **requested outgoing CIR**

Minimum acceptable incoming Committed Information Rate (CIR)
Specifies the minimum CIR that will be accepted if the network cannot provide the requested CIR.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps with a maximum of the **requested incoming CIR**.

Default Value: Same as **minimum acceptable outgoing CIR**

Requested outgoing committed burst size (Bc)
Specifies the requested outgoing committed burst size.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps.

Default Value: Value determined according to CIR-defaults at the interface level

Requested incoming committed burst size (Bc)
Specifies the requested incoming committed burst size.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps.

Default Value: Value equal to **requested outgoing Bc**

Outgoing excess burst size (Be)
Specifies the requested outgoing burst size.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps.

Default Value: Value determined according to CIR-defaults at the interface level

Requested incoming excess burst size (Be)
Specifies the requested incoming excess burst size.

Valid Values: The CIR can be either 0 or a value in the range 300 bps to 2 048 000 bps.

Default Value: Same as **requested outgoing excess burst size (Be)**

Idle timer

Specifies the time period that a SVC will remain active in the absence of traffic. Specifying 0 designates this SVC as a fixed circuit that will be established the first time data arrives for it and will not be disconnected even if no traffic flows over it.

Valid Values: 0 - 65535 seconds

Default Value: 60

Establish circuit to learn remote protocol addresses

Specifies whether this SVC should be established when the interface comes up to learn the protocol addresses of the adjacent node. This option can be used in place of statically configured destination protocol names and addresses for protocols that support dynamic address discovery, such as IP, IPX, Appletalk2, and DECnet IV to force the router to learn the protocol addresses associated with the remote device via directed InARP. Using this option may help reduce ARP broadcasts. The idle timer will be used to disconnect the SVC once the protocol addresses are learned.

Valid Values: yes or no

Default Value: yes

Is multicast required for this circuit

Specifies whether or not this SVC should be used to transmit multicast packets on this interface even if it means setting the SVC up just to do so. You may use static routes to keep from requiring multicast over SVCs so that the SVCs will not be established just to exchange routing information.

Valid Values: yes or no

Default Value: Defaults according to the multicast emulation setting at the interface level

Are call-ins allowed

Specifies whether or not a call-in from this remote DTE should be accepted. Specifying no can be used to block call-ins from specific users and help eliminate call-in/call-out race conditions.

Valid Values: yes or no

Default Value: yes

Compression capable

Specifies whether Frame Relay compression is supported

Valid Values: yes or no

Default Value: yes, if compression is enabled for the interface. Otherwise, no.

Encryption capable

Specifies whether encryption is supported for this SVC.

Valid Values: yes or no

Default Value: yes, if encryption is enabled for the interface. Otherwise, no.

Change

Use the **change permanent-virtual-circuit** command to change any previous PVCs that were added with the **add permanent-virtual-circuit** command.

Syntax:

change permanent-virtual-circuit . . .

switched-virtual-circuit . . .

Example:

```
change permanent-virtual-circuit
Circuit Number [16]?
Committed Information Rate in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign Circuit Name: []?
Is the circuit required for interface operation [N]?
Does the circuit belong to a required group [N]?
What is the group name []?
Do you want to have data compression performed []?
Do you want to have data encryption performed []?
```

permanent virtual circuit

See page 328 for a description of the parameters.

switched-virtual-circuit

```
FR 4 Config>change switched-virtual-circuit
Circuit name []? svc01
Remote party number []? 12345
Remote party number numbering plan (E.164 or X.121) [E.164]?
Remote party number type (Unknown or International) [International]?
Remote party subaddress in hexadecimal []? 01
Remote party subaddress format (private or NSAP) [private]ı?
Requested outgoing Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable outgoing Committed Information Rate (CIR) in bps [64000]?
Requested incoming Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable incoming Committed Information Rate (CIR) in bps [64000]?
Requested outgoing Committed Burst size (Bc) in bits [64000]?
Requested incoming Committed Burst size (Bc) in bits [64000]?
Requested outgoing Excess Burst size (Be) in bits [0]?
Requested incoming Excess Burst size (Be) in bits [0]?
Idle timer in seconds [60]?
Establish circuit to learn remote protocol addresses [Y]?
Is multicast required for this circuit [Y]?
Are call-ins allowed for this circuit [Y]?
```

See page 331 for a description of the parameters.

Disable

Use the **disable** command to disable those features previously enabled using the **enable** command.

Syntax:

disable cir-monitor

cllm

compression

congestion-monitor

dn-length-field

encryption

lmi

lower-dtr

multicast-emulation

no-pvc

notify-fecn-source

orphan-circuits

protocol-broadcast

switched-virtual-circuits

throttle-transmit-on-fecn

cir-monitor
Disabling this feature allows the circuit's information rate to exceed the maximum information rate that is calculated using the parameters configured with the **add permanent-virtual-circuit** or **add switched-virtual-circuit**command. The default setting for this feature is disabled. See "Circuit Congestion" on page 321 for more information.

cllm Disables the device from *throttling down* in response to a CLLM message. The default is disabled. See "Circuit Congestion" on page 321 for details.

compression
Disables compression on the interface. Compression will not be performed for any VC.

congestion-monitor
Disables the congestion monitoring feature. Disabling this feature prevents a circuit's information rate from varying in response to congestion between the minimum information rate and the line speed. See "Circuit Congestion" on page 321 for more information. The default setting for this feature is enabled.

dn-length-field
Prevents inter-operation with implementations of DECnet Phase IV over Frame Relay that require a length field to precede DECnet packets in Frame Relay frames, but allows inter-operation with DECnet Phase IV Frame Relay software that does not use a length field before the DECnet packet. Disabling dn-length-field causes Frame Relay not to insert a length field into transmitted frames containing DECnet packets and not to attempt to remove the length field from received frames containing DECnet packets.

Note: This option is presented as a configuration option only

encryption
Disables encryption on the interface. Even though the PVCs on this interface may be encryption capable, encryption will not take place.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See "Load" on page 95.

lmi Disabling this parameter allows for normal operation or end-to-end Frame Relay testing in the absence of a real network or management interface. With end-to-end Frame Relay testing, it is necessary to add like PVCs (the same PVC number, such as 16 and 16) on both ends of the link.

lower-dtr
This parameter determines how the data terminal ready (DTR) signal is

handled for leased serial-line interfaces on the router. It is not supported on Frame Relay dial circuit interfaces. See the **enable lower-dtr** command for a more complete description of the lower-dtr parameter.

The following cable types are supported:

EIA 232 (RS-232)

V.35

V.36

The default setting is **disable lower-dtr**.

multicast-emulation
Disables multicast emulation on each active VC. The default setting for this feature is enabled. If you disable this feature, you are required to add protocol static address maps.

Some protocols, such as IPX RIP, will not function on the Frame Relay interface if multicast-emulation is disabled. The protocol-broadcast feature also requires multicast-emulation in order to function properly. For more information, see “Multicast Emulation and Protocol Broadcast” on page 316.

no-pvc
Controls whether the interface is considered active or inactive. If no-pvc is disabled, the presence of active PVCs on the interface does not affect whether the Frame Relay interface is considered active or inactive.

notify-fecn-source
Disables setting a BECN bit on the first packet destined to a device from which the router received a packet with the FECN bit set. See “Circuit Congestion” on page 321 for more information.

orphan-circuits
Prohibits the use of all non-configured PVC orphan circuits at the interface. The default setting for orphan circuits is enabled. Disabling orphan circuits adds a measure of security to your network by preventing unauthorized entry from a non-configured circuit. However, if you disable orphan circuits, you are required to add PVCs that will be used on the interface.

protocol-broadcast
Prohibits protocols such as IP RIP from functioning over the Frame Relay interface. For more information, see “Multicast Emulation and Protocol Broadcast” on page 316. The default setting for this feature is enabled.

switched-virtual-circuits
Prohibits the use of SVCs.

throttle-transmit-on-fecn
Prohibits the device from *throttling down* the transmission of packets in response to a packet with a FECN bit set on. The default is disabled. See “Circuit Congestion” on page 321 for more information.

Enable

Use the **enable** command to enable Frame Relay features.

Syntax:

enable cir-monitor
cllm

compression

congestion-monitor

dn-length-field

encryption

lmi

lower-dtr

multicast-emulation

notify-fecn-source

no-pvc

orphan-circuits

protocol-broadcast

switched-virtual-circuits

throttle-transmit-on-fecn

cir-monitor

Enables the circuit monitoring feature. The circuit monitoring feature ensures that the circuit's information rate varies between the minimum information rate and the maximum information rate, calculated using the parameters configured with the **add permanent-virtual-circuit** command or the **change permanent-virtual-circuit** command

Note: The circuit monitoring feature overrides the congestion monitoring feature if there is a conflict when both are enabled. The default setting for this feature is disabled.

For additional information on CIR monitoring, see "CIR Monitoring" on page 321 .

Note: To maximize throughput for circuits running data compression, you should not enable CIR monitoring on the same interface on which you have enabled compression. Because the device uses the uncompressed size of frames to determine if the VIR of a PVC is being exceeded and compressed frames will require less bandwidth, the CIR of a PVC will be under-utilized if the device strictly monitors and does not exceed the configured CIR. Instead, congestion monitoring can be used to allow the device to react to congestion indications sent by the FR network to avoid frame loss.

cllm Enables the device to *throttle down* in response to a CLLM message. Contact your FR network provider to see whether this support is available. See "Circuit Congestion" on page 321 for more information.

compression

Enables compression on the interface. All compression-capable VCs on the interface can compress data packets, provided that contexts are available and the active compression circuit limit has not been exceeded. (See Using the Data Compression Subsystem in *Using and Configuring Features* for details.)

Note: To maximize throughput for circuits running data compression, you should not enable CIR monitoring on the same interface on which

you have enabled compression. Because the device uses the uncompressed size of frames to determine if the VIR of a VC is being exceeded and compressed frames will require less bandwidth, the CIR of a VC will be under-utilized if the device strictly monitors and does not exceed the configured CIR. Instead, congestion monitoring can be used to allow the device to react to congestion indications sent by the FR network to avoid frame loss.

congestion-monitor
Enables the congestion monitoring feature. This feature allows a circuit's information rate to vary in response to congestion between the minimum information rate and the line speed.

Note: The circuit monitoring feature overrides the congestion monitoring feature if there is a conflict when both are enabled. The default setting for this feature is enabled.

For additional information on congestion monitoring, see "Congestion Monitoring" on page 322.

dn-length-field
Supports inter-operation with implementations of DECnet Phase IV over Frame Relay that require a length field to precede DECnet packets in Frame Relay frames. Enabling dn-length-field causes Frame Relay to insert a length field into transmitted frames containing DECnet packets and to remove the length field from received frames containing DECnet packets. This option is disabled by default. By default, Frame Relay will neither insert nor attempt to remove the length field.

Note: This option is presented as a configuration option only when the router software contains the DECnet Phase IV protocol.

encryption
Enables encryption on the interface. All VCs that are configured as encryption enabled, will encrypt all transmitted data.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See "Load" on page 95.

lmi Enables management activity.

After issuing the **enable lmi** command, use the **set lmi-type** command to select the management mode for your Frame Relay interface. See "Enabling Frame Relay PVC Management" on page 325. The system defaults to ANSI T1.617 Annex D management.

Use the **enable lmi** command to resume LMI management if you have previously disabled Frame Relay management.

LMI only provides information about PVCs on an interface, so it does not need to be enabled if only SVCs are used unless it is required by the network. Q.922 determines the usability of all SVCs on an interface and is an indicator of the state of the interface itself. When both PVCs and SVCs are on an interface, LMI and Q.922 may be active at the same time.

lower-dtr
This parameter determines how the data terminal ready (DTR) signal is handled for leased serial-line interfaces that are disabled. It is not supported

on Frame Relay dial circuit interfaces. If this parameter is set to “disabled” (the default), the DTR signal will remain raised when the interface is disabled.

When lower-dtr is enabled, DTR will be lowered when the interface is disabled. This behavior may be desirable in situations where the interface has been configured as an alternate link for WAN Reroute and the interface is connected to a dial-out modem which maintains its dial connection based on the state of the DTR signal.

If this feature is enabled and the interface is disabled, the DTR signal is low and the modem keeps the dial connection down. When the interface is enabled, due to a WAN Reroute backup scenario, DTR is raised and the modem dials a stored number to the backup site. When the primary interface is restored, the alternate interface is disabled, DTR is lowered, and the modem hangs up the dial connection.

The following cable types are supported:

EIA 232 (RS-232)

V.35

V.36

The default setting is **disable lower-dtr**.

multicast-emulation
Enables multicast emulation. This allows a multicast/broadcast frame to be transmitted on each active VC. Protocols such as ARP, IPX RIP, and IP RIP require multicast emulation to be enabled to function correctly over a Frame Relay interface. For more information, see “Multicast Emulation and Protocol Broadcast” on page 316. The default for this parameter is enabled.

no-pvc
Controls whether the interface is considered active or inactive. When this feature is enabled, the Frame Relay interface becomes inactive when there are no active PVCs on the interface. If at least one PVC is active, the Frame Relay interface becomes active when a successful LMI exchange occurs between the router and the FR switch.

notify-fecn-source
Enables setting a BECN bit on the first packet destined to a device from which the router received a packet with the FECN bit set. Use this parameter to enhance the congestion control mechanisms of the device in a network whether the FR switches do not themselves set BECN but set FECN. See “Circuit Congestion” on page 321 for more information.

orphan-circuits
Enables the use of all non-configured orphan circuits. The default for this feature is enabled. See “Orphan Permanent Virtual Circuit CIR” on page 319 for information about the default CIR values.

protocol-broadcast
Allows protocols such as IP RIP to function correctly over the Frame Relay interface. The multicast emulation feature must be enabled for the protocol-broadcast feature to function correctly. The default setting for this feature is enabled.

switched-virtual-circuits
Allows the use of SVCs and prompts you for the local SVC network number, the numbering plan, whether call-ins from orphan SVCs are allowed, the number of dial-out retries performed for all SVCs on the

interface, and whether network emulation mode, which is used in back-to-back (for example, dial circuit) router configurations, is required.

You can also use the **enable switched-virtual-circuits** command to change configured SVC interface parameters if SVCs have already been enabled.

Example:

```
FR 1 Config> enable switched
Local party number []? 4141990
Local party number numbering plan (E.164 or X.121) [E.164]?
Local party number type (Unknown or International) [International]?
Are call-ins allowed on this interface [Y]?
Call-out redial attempts [2]?
Network emulation mode [N]?
```

Local party number
Specifies the destination's Frame Relay address.

Valid Values: A 1 - 20 character string of decimal digits

Default Value: None

Local party numbering plan
Specifies the format of the party number. The numbering plan must match that used by the FR network.

Valid Values: E.164 (ISDN) or X.121 (Data)

Default Value: E.164

Local party number type
Specifies the destination Frame Relay party number type. The number type must match that used by the FR network.

Valid Values: International or Unknown

Default Value: International

Call-ins allowed
Specifies whether calls from unconfigured (orphan) SVCs are allowed on this interface.

Call-out redial attempts
Specifies the number of call-out redial attempts that will be performed for each SVC in case of a call-out timeout on this interface.

Default Value: 2

Network emulation mode
Specifies whether this SVC is in network emulation mode. It is used for a back-to-back router configuration.

throttle-transmit-on-fecn
Enables the device to *throttle down* the transmission of packets in response to a packet with a FECN bit set on. Use this parameter to minimize overall FR network congestion whenever a congestion indication is received. It causes the device to react to a FECN in the same way that it reacts to a BECN.

List

Use the **list** command to display currently configured management and PVC information.

Syntax:

list all
hdlc
lmi
permanent-virtual-circuits
protocol-address
pvc-groups
switched-virtual-circuits

all Displays the Frame Relay configuration. The display is a combination of the **list hdlc,** the **list lmi**, and the **list permanent virtual circuits** commands.

See **list hdlc** and **list lmi** for descriptions of the parameters.

hdlc Displays the Frame Relay High-Level Data Link Control (HDLC) configuration.

Example:

```
list hdlc
                        Frame Relay HDLC Configuration


 Maximum frame size     = 2048
 Encoding               = NRZ
 Idle state             = Flag
 Clocking               = External
 Cable type             = V.35 DTE
 Line speed (bps)       = 64000
 Transmit delay         = 0
 Lower DTR              = Enabled
```

Encoding
The transmission encoding scheme for the serial interface. Encoding is NRZ (non-return to zero) or NRZI (non-return to zero inverted).

Idle The data link idle state: flag or mark.

Clocking
The type of clocking: internal or external.

Cable type
The serial adapter cable type: RS-232, V.35, V.36, or X.21.

Line Speed (bps)
Indicates the physical data rate for the Frame Relay interface.

Maximum frame size
Indicates the maximum frame size that can be transmitted or received over the network at any given time.

Transmit delay
Indicates the number of additional flag bytes sent between frames.

Lower DTR
Indicates whether the router will drop the DTR signal when a WAN Reroute alternate link is no longer needed. Dropping the DTR signal causes the modem to terminate the leased-line connection for the alternate link. Lower DTR does not appear when the cable type is X.21.

Notes:

1. For a FR dial circuit interface, only the maximum frame size is displayed.

lmi Displays logical management and related configuration information about the Frame Relay interface.

Example:

```
list lmi
                        Frame Relay Configuration


  LMI enabled            =  Yes   LMI DLCI                      =    0
  LMI type               =  ANSI  LMI Orphans OK                =  Yes
  CLLM enabled           =   Yes  Timer Ty seconds    = 10

  SVC network number     =   4141990
  SVC Number type        =   International
  SVC Numbering plan     =   E.164  SVC Call-out redial attempts =  2
  SVC Call-ins allowed   =     Yes  SVC Network emulation mode   = No

  Protocol broadcast     =   Yes  Congestion monitoring         =  Yes
  Emulate multicast       =   Yes  CIR monitoring                =   No
  Notify FECN Source     =   Yes  Throttle Transmit on FECN     =  Yes

  Data compression       =   Yes  Orphan compression            =   No
  Compression circuit limit=  10  Number of compression circuits=    5 1
  Data encryption        =  Yes   Number of encryption circuits  =   1 2

  PVCs P1 allowed        =    64  Interface down in no PVCs     =   No
  Timer T1 seconds       =    10  Counter N1 increments         =    6
  LMI N2 error threshold =     3  LMI N3 error threshold window =    4
  MIR % of CIR           =    25  IR % Increment                =   25
  IR % Decrement         =    25  DECnet length field           =   No
  Default CIR            = 64000  Default Burst Size             = 64000
  Default Excess Burst   =     0
```

1 This line appears only when data compression is on (yes).

2 This line appears only when data encryption is on (yes).

LMI enabled
Indicates whether the management features are enabled on the Frame Relay interface, yes or no.

LMI DLCI
Indicates the management circuit number. This number reflects the LMI type: 0 for ANSI and ITU-T/CCITT and 1023 for REV1.

LMI Type
Indicates the LMI type: REV1, ANSI, or CCITT.

LMI Orphans OK
Indicates if non-configured circuits are available for use, yes or no.

CLLM Enabled
Indicates whether CLLM is enabled on the Frame Relay interface.

Timer Ty seconds
Indicates the amount of time that must elapse without the device receiving any CLLM messages or BECNs before the device considers a congestion condition cleared and gradually return the PVC to its configured transmission rate.

SVC network number
Specifies the network number for the SVCs on this interface.

SVC number type
Specifies the SVC number type, unknown or international.

SVC numbering plan
Specifies whether the numbering plan is E.164 or X.121.

SVC call-out redial attempts
Specifies the number of call-out redial attempts on this interface.

SVC network emulation mode
Specifies whether this interface operates in network emulation mode for SVCs.

SVC call-ins allowed
Specifies whether call-ins are allowed on this interface.

Protocol Broadcast
Indicates whether protocols such as IP RIP can function over the Frame Relay interface, yes or no.

Emulate multicast
Indicates whether the multicast emulation feature is enabled on each active PVC, yes or no.

Congestion Monitoring
Indicates whether the congestion monitoring feature that responds to network congestion is enabled, yes or no.

CIR monitoring
Indicates whether the circuit monitoring feature that enforces the transmission rate is enabled, yes or no.

Notify FECN Source
Indicates whether this device sets a BECN bit on the first packet destined to a device from which the router received a packet with the FECN bit set.

Throttle Transmit on FECN
Indicates whether the device will *throttle down* the transmission of packets in response to a packet with a FECN bit set on.

Data compression
Indicates whether this interface has data compression enabled.

Data encryption
Indicates whether this interface has data encryption enabled and the number of circuits that are encryption capable.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95 .

Orphan compression
Indicates whether orphan circuits on this interface will have data compression enabled.

Note: Enabling compression on orphan circuits will decrease the number of available compression contexts available for the native PVCs on the device.

Orphan compression applies to both PVCs and SVCs.

Compression circuit limit
Indicates the maximum number of circuits that can participate in data compression.

Number of compression VCs
Indicates the current number of VCs supporting data compression.

P1 allowed
Indicates the number of allowable PVCs and SVCs for use with this interface.

Timer T1 seconds
Indicates the frequency with which the Frame Relay interface performs a sequence number exchange with the Frame Relay switch LMI entity.

Counter N1 increments
Indicates the number of T1 timer intervals which must expire before a complete PVC LMI status enquiry is made.

LMI N2 error threshold
Indicates the number of management event errors occurring within the N3 window that will cause a reset of the Frame Relay interface.

LMI N3 error threshold window
Indicates the number of monitored management events used to measure the N2 error threshold.

MIR % of CIR
Minimum IR, expressed as a percentage of CIR.

IR % Increment
Percentage by which the router increments the IR each time it receives a frame without BECN until it reaches the maximum IR.

IR % Decrement
Percentage by which the router decrements the IR each time it receives a frame that contains BECN until it reaches the minimum IR.

Default CIR
The committed information rate, in bits per second, used as the default for VCs on this interface.

Default Burst Size
The committed burst size, in bits, used as the default for VCs on this interface.

Default Excess Burst Size
The excess burst size, in bits, used as the default for VCs on this interface.

permanent-virtual-circuits
Displays all the configured PVCs on the Frame Relay interface.

Example:

```
FR Config>li perm

  Maximum circuits allowable =      64
  Total circuits configured  =       9
  Total PVCs configured      =       7

            Circuit              Circuit   Circuit   CIR     Burst  Excess
             Name                Number     Type    in bps   Size   Burst
 ------------------------------- ------- ---------- ------- ------- -------
 cir16                             16 $@#Permanent   64000   64000       0
 cir244                           244   #Permanent   64000   64000       0
 cir33                             33   #Permanent   64000   64000       0
 cir1005                         1005   #Permanent   64000   64000       0
 cir55                             55   #Permanent   64000   64000       0
 cir22                             22   @Permanent   64000   64000       0
 cir66                             66  @*Permanent   64000   64000       0
```

```
* = circuit is required
# = circuit is required and belongs to a Required PVC group
@ = circuit is data compression capable
$ = circuit is data encryption capable
```

Maximum circuits allowable
Indicates the number of PVCs and SVCs that can exist for this interface. This number includes any PVCs that you added with the **add permanent-virtual-circuit** command and any SVCs that you added with the **add switched-virtual-circuit** command and dynamically learned through the management interface.

Total circuits configured
Indicates the total number of currently configured PVCs and SVCs that can exist for this interface.

Circuit Name
Indicates the ASCII designation of the configured PVC.

Circuit Number
Indicates the DLCI of a currently configured PVC.

Circuit Type
Indicates the type of virtual circuit currently configured. This release of Frame Relay only supports permanent virtual circuits.

Committed Information Rate
Indicates the information rate at which the network agrees to transfer data under normal conditions.

Committed Burst Size
The maximum amount of data in bits that the network agrees to deliver during a measurement interval equal to (Committed Burst Size/CIR) seconds.

Excess Burst Size
The maximum amount of uncommitted data in bits in excess of Committed Burst Size that the network attempts to deliver during a measurement interval equal to (Committed Burst Size/CIR) seconds.

pvc-groups
Displays all the Required PVC groups on the Frame Relay interface.

Example:

```
list pvc-groups
    Required PVC group = group1

          Circuit # 16
```

protocol-addresses
Displays all the statically configured protocol addresses of circuit mappings at the Frame Relay interface.

Example:

```
list protocol-addresses
                Frame Relay Protocol Address Translations

  Protocol Type              Protocol Address      Circuit Number or Name
  -------------              ----------------      ----------------------
       IP                     125.2.29.4                  21
       IPX                    000000004503                16
```

Protocol Type
Displays the name of the protocol running over the interface.

Protocol Address
Displays the protocol address of the device at the other end of the circuit.

Circuit Number or Name
Displays the DLCI of the PVC or the name of the SVC that is handling the protocol.

switched-virtual-circuits

```
FR 4 Config>list s

  Maximum circuits allowable =      64
  Total circuits configured  =       9
  Total SVCs configured      =       2

 Circuit                          Opt-  Idle             Outgoing    Incoming
  Name                            ions  Timer              Value       Value
 -------------------------------- ----- ------          ----------  ----------
 circ01                           ILM       60     CIR:      64000       64000
   Remote party number: IE12345                   Min CIR:      64000       64000
   Remote subaddress:   None                        Burst:      64000       64000
                                                   Excess:          0           0

 svc01                            ILM       60     CIR:      64000       64000
   Remote party number: IE12345                   Min CIR:      64000       64000
   Remote subaddress:                               Burst:      64000       64000
      P01                                          Excess:          0           0

 Options: I - call-ins allowed, L - learn protocols, M - Multicast required
          c - compression capable, e - Encryption capable
 Address type: I - International, U - Unknown
 Numbering plan: E - E.164, X - X.121
 Subaddress format: N - NSAP, P - private
FR 4 Config>
```

Maximum circuits allowable
Indicates the number of circuits that can exist for this interface.

Total circuits configured
Indicates the total number of currently configured circuits for this interface.

Circuit Name
Indicates the ASCII designation of the configured circuit.

Committed Information Rate
Indicates the information rate at which the network agrees to transfer data under normal conditions.

Committed Burst Size
The maximum amount of data in bits that the network agrees to deliver during a measurement interval equal to (Committed Burst Size/CIR) seconds.

Excess Burst Size
The maximum amount of uncommitted data in bits in excess of Committed Burst Size that the network attempts to deliver during a measurement interval equal to (Committed Burst Size/CIR) seconds.

Idle Timer
Time period that the SVC will remain active in the absence of traffic.

Options
Indicates the options configured for the circuit.

Remote party number
Remote destination FR address. This address is prefixed by the address type and numbering plan used.

Remote subaddress
Remote party subaddress assigned to this connection. The subaddress is prefixed by the subaddress format.

LLC

Use the **LLC** command to access the LLC configuration environment. See "LLC Configuration Commands" on page 217 for an explanation of each of these commands.

Note: The **LLC** command is supported only if APPN is in the software load.

Syntax:

llc

Remove

Use the **remove** command to delete any PVC, Required PVC group, or protocol-address previously added using the **add** command.

Syntax:

remove permanent-virtual-circuit . . .
protocol-address
pvc-group
switched-virtual-circuit *circuit-name*

permanent-virtual-circuit *pvc#*

Deletes any configured PVC in the range 16 to 1007.

Notes:

1. When you delete a PVC that is running compression, the interface decreases the count of active compression PVCs. If this action brings the count of compression PVCs below the limit, you will receive a message to that effect.
2. When you delete a PVC that is running encryption, the interface decreases the count of active encryption PVCs.

   Note: Encryption support is optional and must be added to your software load using the **load add** command. See the CONFIG process **load** command in *Access Integration Services Software User's Guide*.

protocol-address
Deletes any configured protocol addresses (static ARP entries). This parameter prompts you for different information depending on the type of protocol that you are adding.

Example:

```
remove protocol-address
Protocol name or number [IP]?
```

IP protocol:

```
IP Address [0.0.0.0]?
Circuit Name or Number [16]?
```

IPX protocol:

```
Host Number (in hex)[]?
Circuit Name or Number [16]?
```

AppleTalk Phase 2 protocol:

```
Network Number (1-65279) []?
Node Number (1-253) []?
Circuit Name or Number [16]?
```

DN protocol:

```
Node address [0.0]?
Circuit Name or Number [16]?
```

Protocol name or number
Defines the name or number of the protocol that you are deleting. If you try to delete an unsupported protocol the system will display the error message:

```
Unknown protocol name, try again
```

To see a list of supported protocols, type `?` at the `Protocol name or number [IP]?` prompt.

IP Address
Defines the 32-bit internet address of the remote IP host in dotted-decimal notation.

Host Number
Defines the 48-bit node address of the remote IPX host.

Network Number
Defines the AppleTalk Phase 2 network number.

Node Number
Defines the node number of the interface attached to the remote AppleTalk host.

Node address
Defines the DECnet node address of the remote DECnet host. Configure the node address in the format *x*,*y*, where *x* is a 6-bit area address and *y* is a 10-bit node number.

Circuit Number
Defines the name of a PVC or SVC that the protocol runs over.

pvc-group *groupname*
Deletes any configured PVC group by name. The group is removed only if it has no member circuits.

Example: remove pvc-group PVC group name [IP]?

switched-virtual-circuit
Deletes any configured SVC by circuit name.

Set

Use the **set** command to configure the interface to run the Frame Relay protocol.

Set Command Considerations

Two parameters, the n2-parameter and the n3-parameter, require further explanation before you configure them. The n2-parameter sets the error threshold for management events, and the n3-parameter sets the number of events that are monitored in the event window. If the number of management errors in the event window equals n2, the Frame Relay interface resets. For example:

set n3-parameter 4
set n2-parameter 3

You now have a window size of 4 (n3 = 4) and an error threshold of 3 (n2 = 3). That means the system is monitoring 4 management events and checking to determine if any of those are in error. If the number of events in error equals 3 (the n2 parameter), the Frame Relay interface is reset and the status of the network is considered *network down*.

For the status of the network to be considered *network up*, the number of events in error within the window must be less than n2 prior to any change in status.

Syntax:

set
- cable*
- cir-defaults
- clocking*
- encoding*
- frame-size
- idle . . .*
- ir-adjustment . . .
- line-speed*
- lmi-type n1-parameter
- n2-parameter
- n3-parameter
- p1-parameter
- t1-parameter
- transmit-delay . . .*
- ty-parameter

*** Note:** The commands with an * following them are not available for FR dial circuit interfaces.

cable *physical-interface-link-type data-connection-type*
Sets the cable type for the network physical link.

A DTE cable is used when you are attaching the router to some type of DCE device (for example, a modem or a DSU/CSU). A DCE cable is used when the router is acting as the DCE and providing the clocking for direct attachment.

The available options are:

Physical Interface Link Type	Data Connection Type
EIA 232 (RS-232)	DTE, DCE

Physical Interface Link Type	Data Connection Type
V35	DTE, DCE
V36	DTE
X21	DTE, DCE

cir-defaults

Sets the default values for the circuit congestion parameters. The parameters are:

cir Sets the default value of *cir* to the value provided by a Frame Relay network provider.

Valid Values: 0 or 300 to 204 800 bps

Default Value: 64 000

bc Sets the default value of *bc* to the value provided by a Frame Relay network provider.

Valid Values: See “Committed Burst (Bc) Size” on page 319

Default Value: 64 000

be Sets the default value of *be* to the value provided by a Frame Relay network provider.

Valid Values: See “Excess Burst (Be) Size” on page 319

Default Value: 0

Example:

```
FR 6 config> set cir-default
Default Committed Information Rate (CIR) in bps [64000]? 48000
Default Committed Burst Size (Bc) in bits [64000]? 40000
Default Excess Burst Size (Be) in bits [0]? 52000
```

clocking [external or internal]

To connect to a modem or DSU, configure clocking as external. To connect directly to another DTE device, use a DCE cable and set the clocking to internal. For internal clocking, you must enter the **set line-speed** command to configure a clock speed between 2400 and 2048000 bps.

- interface 1.
- port 1 of a 4-port WAN concentration adapter.
- ports 1 and 5 of an 8-port WAN concentration adapter.

If you want to use a line speed greater than 2048000, you can only do this on port 1 of the system card’s integrated WAN ports and all other integrated WAN ports must be clocked at 64 Kbps or less.

For external clocking the maximum line speed is 6 312 000 bps.

encoding [NRZ or NRZI]

Sets the HDLC transmission encoding scheme as NRZ (non-return to zero) or NRZI (non-return to zero inverted). Most configurations use NRZ, which is the default.

frame-size *#*

Sets the maximum size of the network layer portion of the frames transmitted and received on the interface. This maximum size includes the

2-byte DLCI address and the user data shown in figure 39-4. The size you configure must be consistent with the maximum frame size supported by the Frame Relay switch and by the other FR DTEs in the Frame Relay network. Values are 262 to 8190. The default is 2048. Since the configured frame size includes the DLCI address and the FR RFC 1490 multi-protocol encapsulation header, the maximum protocol packet size that can be transmitted is less than the configured frame size and is protocol dependent. The following table shows how many bytes to subtract from the configured frame size to determine the maximum protocol packet size that can be transmitted and received on the interface.

IP	4 bytes
IPX	10 bytes
Appletalk Phase 2	10 bytes
DECnet Phase IV (DNA IV)	12 bytes
Banyan Vines	10 bytes
OSI	10 bytes
Bridging	10 bytes
APPN	58 bytes (see note)

Note: Assumes worst case for APPN BAN where a T/R MAC address header and LLC header are added in addition to the FR header bytes.

If FR data encryption is enabled then you must subtract up to an additional 12 bytes.

When using Frame Relay SVCs, the maximum information field size must be the same at both ends of the virtual circuit. To determine the maximum information field size, subtract 16 bytes from the frame size if encryption is enabled on the SVC and subtract 4 bytes if encryption is not enabled on the SVC.

idle [flag or mark]

Sets the transmit idle state for HDLC framing. The default value is **flag**, which provides continuous flags (7E hex) between frames. The mark option puts the line in a marking state (OFF, 1) between frames.

ir-adjustment *increment-% decrement-% minimum-IR*

Sets the minimum information rate (IR) and the percentages for incrementing and decrementing the IR in response to network congestion.

The minimum IR, expressed as a percentage of CIR, is the lower limit of the information rate. The minimum percentage is 1 and the maximum percentage is 100. The default is 25.

When network congestion clears, the information rate is gradually incremented by the IR adjustment increment percentage until the maximum information rate is reached. The minimum percentage is 1 and the maximum percentage is 100. The default is 12.

When network congestion occurs, the information rate is decremented by the IR adjustment decrement percentage each time a frame containing BECN is received until the minimum information rate is reached. The minimum percentage is 1, and the maximum percentage is 100. The default is 25.

Example:

```
set ir-adjustment
IR adjustment % increment [12]?
IR adjustment % decrement [25]?
Minimum IR as % of CIR [25]?
```

line-speed *rate*

For internal clocking, this command specifies the speed of the transmit and receive clock lines. The range is 2400 to 2 048 000 bps.

For external clocking, this command does not affect the hardware (in other words, the actual speed of the line) but it sets the speed of some protocols, such as IPX, used to determine routing cost parameters. Congestion monitoring also uses the configured line speed to determine the maximum information rate. Therefore, it is recommended that you set the speed to match the actual line speed. If the speed is not configured, the protocols and congestion monitoring assume a speed of 1 000 000 bps.

Notes:

1. When using external clocking, the maximum line speed is 6 312 000.
2. When using internal clocking, the maximum line speed is 2 048 000.

- interface 1.
- port 1 of a 4-port WAN concentration adapter.
- ports 1 and 5 of an 8-port WAN concentration adapter.

If you want to use a line speed greater than 2048000, you can only do this on port 1 of the system card's integrated WAN ports and all other integrated WAN ports must be clocked at 64 Kbps or less.

lmi-type [rev1 or ansi or ccitt]

Sets the management type for the interface. See "Enabling Frame Relay PVC Management" on page 325 for details on setting Frame Relay management. The default is type **ansi** enabled.

Table 42. Frame Relay Management Options

Command	Management Type	Description
set	lmi-type rev1	Conforms to LMI Revision 1, (Stratacom's Frame Relay Interface Specification)
set	lmi-type ansi	Conforms to ANSI T1.617 ISDN-DSS1-Signalling Specification for Frame Relay Bearer Service (known as Annex D)
set	lmi-type ccitt	Conforms to Annex A of ITU-T/CCITT Recommendation Q.933 - DSS1 Signalling Specification for Frame Mode Basic Call Control.

n1-parameter *count*

Configures the number of T1 timer intervals which must expire before a complete PVC status enquiry is made. *Count* is the interval in the range 1 to 255. The default is 6.

n2-parameter *max#*

Configures the number of errors that can occur in the management event window monitored by the n3-parameter before the Frame Relay interface resets. Max# is a number in the range 1 to 10. The default is 3. This parameter must be less than or equal to the n3-parameter or you will receive an error message.

n3-parameter *max#*

Configures the number of monitored management events for measuring the n2-parameter. Max# is a number in the range 1 to 10. The default is 4.

p1-parameter *max#*

Configures the maximum number of PVCs supported by the Frame Relay interface. This includes active, inactive, removed, and congested PVCs. Max# is a number in the range 0 to 992. The default is 64. 0 (zero) implies that the interface supports no PVCs.

t1-parameter *time*

Configures the interval (in seconds) between sequence number exchanges with Frame Relay management. The management's T2 timer is the allowable interval for an end station to request a sequence number exchange with the manager. The T1 interval must be less than the T2 interval of the network. *Time* is a number in the range 5 to 30. The default is 10.

transmit-delay *#*

Allows the insertion of a delay between transmitted packets. The purpose of this command is to slow the serial line so that it is compatible with older, slower serial devices at the other end. It can also prevent the loss of serial line hello packets between the lines. *#* is between 0 and 15 extra flags. The default is zero (0). Setting this parameter provides 0 to 15 extra flags between transmit frames. Table 43 lists the units and range values for serial interfaces.

Table 43. Transmit Delay Units and Range for the 2212 Serial Interface

Unit	Minimum	Maximum
Extra Flags	0	15

ty-parameter *time*

Configures the interval after which the device considers an existing congestion condition indicated by the receipt of a CLLM message to be cleared. If the device receives a CLLM message before the timer expires, the device resets this timer.

Valid Values: 5 to 30 seconds.

Default Value: 11 seconds.

Accessing the Frame Relay Monitoring Prompt

To access the Frame Relay operating commands and to monitor Frame Relay on your router, perform the following steps:

1. At the OPCON prompt (*), type **talk 5**.
2. At the GWCON prompt (+), enter the **interface** command to see a list of interfaces configured on the router.
3. Enter the **network** command followed by the network number of the frame relay interface. For example:

```
+ net 2
Frame Relay Monitoring
FR 2 >
```

Frame Relay Monitoring Commands

This section summarizes and then explains the Frame Relay Monitoring commands. Use these commands to gather information from the database. Table 44 shows the commands.

Table 44. Frame Relay Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Clear	Clears statistical information on the Frame Relay interface.
Disable	Disables CIR monitoring and congestion monitoring on the Frame Relay interface.
Enable	Enables CIR monitoring and congestion monitoring on the Frame Relay interface.
List	Displays statistics specific to the data-link layer and Frame Relay management.
LLC	Displays the LLC monitoring prompt.
Notrace	Disables packet tracing capability for individual circuits or for the entire interface.
Set	Sets CIR, Committed Burst Size, and Excess Burst Size for a Frame Relay VC.
Trace	Enables packet tracing capability for individual circuits or for the entire interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Note: In this section, the terms *circuit number* and *PVC* are equivalent to the term *data link circuit identifier (DLCI)*.

Clear

Use the **clear** command to zero statistical counters on the Frame Relay interface.

Note: Statistics can also be cleared by using the OPCON **clear** command.

Syntax:

clear

Disable

Use the **disable** command to disable the Frame Relay CIR monitoring and congestion monitoring features.

The **disable** command dynamically changes the router configuration. These changes will be lost when the router is restarted.

Syntax:

disable

cir-monitor

cllm

congestion-monitor

notify-fecn-source

throttle-transmit-on-fecn

Enable

Use the **enable** command to enable the Frame Relay CIR monitoring and congestion monitoring features.

The **enable** command dynamically changes the router configuration. These changes will be lost when the router is restarted.

Syntax:

enable

cir-monitor

cllm

congestion-monitor

notify-fecn-source

throttle-transmit-on-fecn

List

Use the **list** command to display statistics specific to the data-link layer and the Frame Relay interface.

Syntax:

list

all

circuit . . .

lmi

permanent-virtual-circuits

pvc-groups

switched-virtual-circuit

svcs

virtual-circuits

all Displays circuit, management, and VC statistics on the Frame Relay interface. The output displayed for this command is a combination of the **list lmi** and **list permanent-virtual-circuit** commands.

circuit *name or number*
Displays detailed virtual circuit configuration and statistical information for the specified VC using the input circuit name or DLCI.

Example:

```
list circuit 347

 Circuit name = Valencia

 Circuit state        =    Active  Circuit is orphan   =     No
 Frames transmitted   =         0  Bytes transmitted   =      0
 Frames received      =         0  Bytes received      =      0
 Total FECNs          =         0  Total BECNs         =      0
 Times congested      =         0  Times Inactive      =      0
 CIR in bits/second   =     64000  Potential Info Rate =  56000
 Committed Burst (BC) =      1200  Excess Burst (Be)   =  54800
 Minimum Info Rate    =     16000  Maximum Info Rate   =  64000
 Required             =       Yes  PVC group name      = group1
```

```
Compression capable  =       Yes  Operational         =    Yes
R-Rs received        =         0  R-Rs transmitted    =      0
R-As received        =         0  R-As transmitted    =      0
R-R mode discards    =         0  Enlarged frames     =      0
Decompress discards  =         0  Compression errors  =      0
Compression ratio    = 1.72 to 1  Decompression ratio = 1.10 to 1

Encryption capable   =        Yes  Operational         =          Yes
Encryption errors    =          0  Decryption errors   =            0
Rcv error discards   =          0

Current number of xmit frames queued                  =      0
Xmit frames dropped due to queue overflow             =      0
```

Circuit state
Indicates the state of the circuit: inactive, active, or congested. Inactive indicates that the circuit is not available for traffic because either the Frame Relay interface is down or the Frame Relay management entity has not notified the Frame Relay protocol that the circuit is active. Active indicates that data is being transferred. Congested indicates that data flow is being controlled.

Circuit is orphan
Indicates if the circuit is a non-configured PVC learned through LMI management or a callin-in for a non-configured SVC.

Frames/Bytes transmitted
Indicates how many frames and bytes this VC has transmitted.

Frames/Bytes received
Indicates how many frames and bytes this VC has received.

Total FECNS
Indicates the number of times that this VC has been notified of inbound or downstream congestion.

Total BECNS
Indicates the number of times that this VC has been notified of outbound or upstream congestion.

Times congested
Indicates the number of times that this VC has become congested.

Times inactive
Indicates the number of times that this VC was inoperable.

CIR in bits/sec
Indicates the information rate of the VC between the range 300 bps to 2048000 bps. A value of 0 is also supported.

Potential Info Rate
Indicates the current maximum rate in bits per second at which data will be transmitted for the circuit. The actual data rate will depend on the queue depths and priorities associated with the circuit.

If this field has a value of “Line Speed”, then the maximum data rate is the actual line speed even if the line speed was not configured or was configured incorrectly for this interface.

Committed Burst (BC)
Maximum amount of data, in bits, that the router can transmit during the *time interval* (Tc). (Tc=Bc/CIR.)

Excess Burst (Be)
Maximum amount of uncommitted data in bits the router can transmit on a VC in excess of the Bc during the time interval (Tc).

Minimum Info Rate
Minimum Information Rate. The minimum data rate for a VC that the router throttles down to when it is notified of congestion.

Maximum Info Rate
Maximum Information Rate. The maximum data rate at which the router transmits for a VC.

Required
Yes or No. If yes, the PVC is a Required PVC.

PVC group name
If the PVC is a member of a required PVC group, the name appears here; otherwise, “Unassigned” appears.

Compression capable
Indicates whether the circuit can compress data packets.

Operational
Indicates whether compression is active on the circuit. When this is yes, data is being compressed on this link.

R-Rs received
Indicates the number of Reset-Request packets sent by the peer decompressor. A peer decompressor sends a Reset-Request whenever the peer detects that it is out of synch with its peer compressor. If this number increases rapidly, packets are being lost or corrupted on this circuit.

R-Rs transmitted
Indicates the number of Reset-Request packets sent since compression started on the circuit. If this number increases rapidly, packets are being lost or corrupted on this circuit.

R-As received
Indicates the number of Reset-Acknowledgements received in response to Reset-Requests. The compressor also sends out this packet to signal that it has reset its compression history.

R-As transmitted
This is the number of Reset-Acknowledgements sent to the peer.

R-R mode discards
Indicates the number of compressed data frames that were discarded while waiting for an R-A after sending out an R-R.

Enlarged frames
This is a count of the frames that could not be compressed. Usually an incompressible frame is sent in its uncompressed format within a special compression frame type allowing the compressor and decompressor to remain synchronized.

Decompress discards
Indicates the number of compressed frames that were discarded because of decompression errors.

Compression errors
Indicates the number of frames that had compression errors which were transmitted in an uncompressed form.

Compression ratio
Indicates the approximate effectiveness of the compressor.

Decompression ratio
Indicates the approximate effectiveness of the decompressor.

Encryption capable
Indicates whether this circuit is encryption enabled.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95 .

Operational
Indicates whether encryption is active on the circuit. When this is yes, data is being encrypted on this link.

Encryption errors
Indicates the number of frames that had encryption errors.

Decryption errors
Indicates the number of frames that had decryption errors.

Rcv error discards
Indicates the number of compressed frames that were discarded because of reception problems.

Current number of xmit frames queued
Indicates the number of frames currently queued for this circuit by FR. These frames are waiting for space to become available on the serial device handler transmit queue for this interface.

Xmit frames dropped due to queue overflow
Indicates the number of frames that could not be transmitted for this VC due to output queue overflow.

lmi Displays statistics relevant to the logical management on the Frame Relay interface.

Example:

```
list lmi
   Management Status:
  ------------------
    LMI enabled           =     Yes  LMI DLCI                   =       0
    LMI type              =    ANSI  LMI Orphans OK             =     Yes
    CLLM enabled          =      No

    SVC local net number  =   12345678
    SVC Number type       =   International
    SVC Numbering plan    =   E.164  SVC Call-out retries       =       2
    SVC Call-ins allowed  =     Yes  SVC Network emulation mode =      No

    Protocol broadcast    =     Yes  Congestion monitoring      =     Yes
    Emulate multicast     =     Yes  CIR monitoring             =      No
    Notify FECN source    =      No  Throttle transmit on FECN  =      No
    Number VCs P1 allowed =      64  Interface down if no PVCs  =      No
    Line speed (bps)      = 1000000  Maximum frame size (bytes) =    2048
    Timer T1 seconds      =      10  Counter N1 increments      =       6
    LMI N2 threshold      =       3  LMI N3 threshold window    =       4
    MIR % of CIR          =      25  IR % Increment             =      12
    IR % Decrement        =      25  DECnet length field        =      No
    Default CIR           =   64000  Default Burst Size         =   64000
       Default Excess Burst  =       0
   Current receive sequence  =       0
   Current transmit sequence =       1
   Total status enquiries    =       9  Total status responses   =       0
   Total sequence requests   =       0  Total responses          =       0

   Data compression enabled  =      No

   Data encryption enabled   =      No

 Virtual Circuit Status:
 -----------------------
 Total allowed       =      64  Total configured       =       2
```

```
Total active        =       0  Total congested        =       0
Total PVCs left net =       0  Total PVCs join net    =       0
```

Management Status:

LMI enabled
Indicates if Frame Relay management is active (yes or no).

LMI DLCI
Indicates the management circuit number. This number is either 0 (ANSI default or ITU-T/CCITT) or 1023 (interim LMI REV1).

LMI type
Indicates the type of frame relay management being used, ANSI, ITU-T/CCITT, or LMI Revision 1.

LMI orphans OK
Indicates if all non-configured circuits learned from Frame Relay LMI management are available for use (yes or no).

CLLM enabled
Specifies whether this circuit will throttle transmission on receiving CLLM frames.

Timer Ty seconds
Indicates the value of the CLLM Ty timer. This field is only displayed if CLLM is enabled.

Last CLLM cause code
Indicates the congestion cause code given in the last CLLM message received or ***None*** if no CLLM messages have been received. This field is only displayed if CLLM is enabled.

SVC network number
Specifies the network number for the SVCs on this interface.

SVC number type
Specifies the SVC number type, unknown or international.

SVC numbering plan
Specifies whether the numbering plan is E.164 or X.121.

SVC call-out redial attempts
Specifies the number of call-out redial attempts on this interface.

SVC network emulation mode
Specifies whether this interface operates in network emulation mode for SVCs.

SVC call-ins allowed
Specifies whether call-ins are allowed on this interface.

Protocol broadcast
Indicates if protocols such as IP RIP are able to operate over the Frame Relay interface.

Congestion monitoring
Indicates whether the congestion monitor feature that responds to network congestion is enabled (yes or no).

Emulate multicast
Indicates whether the multicast emulation feature is enabled on each active PVC (yes or no).

CIR monitoring
Indicates whether the circuit monitoring feature that enforces the transmission rate is enabled (yes or no).

PVCs P1 allowed
Indicates the number of allowable VCs for use with this interface. This number is the maximum number of active, congested, inactive, and removed VCs that can be supported on the interface.

Interface down if no PVCs
Indicates whether the router considers the interface unavailable when there are no active PVCs.

Line speed (bps)
Indicates the configured data rate of the Frame Relay interface.

Timer T1 seconds
Indicates the frequency with which the Frame Relay interface performs a sequence number exchange with the Frame Relay switch LMI entity.

Counter N1 increments
Indicates the number of T1 timer intervals which must expire before a complete PVC LMI status enquiry is made.

LMI N2 error threshold
Indicates the number of management event errors occurring within the N3 window that will cause a reset of the Frame Relay interface.

LMI N3 error threshold window
Indicates the number of monitored management events used to measure the N2 error threshold.

MIR % of CIR
Minimum IR, expressed as a percentage of CIR.

IR % Increment
Percentage by which the router increments the IR each time it receives a frame without BECN until it reaches the maximum IR.

IR % Decrement
Percentage by which the router decrements the IR each time it receives a frame that contains BECN until it reaches the minimum IR.

DECnet length field
Indicates whether or not the DECnet length field feature is enabled. Some Frame Relay DECnet Phase IV implementations require a length field between the Frame Relay multiprotocol encapsulation header and the DECnet packet. A length field is inserted if the DECnet length field feature is enabled.

Default CIR
Specifies the default CIR for this interface.

Default Burst Size
Specifies the default burst size for this interface.

Default Excess CIR
Specifies the default excess burst size for this interface.

Current receive sequence
Indicates the current receive sequence number that the Frame Relay interface has received from the Frame Relay management entity.

Current transmit sequence
Indicates the current transmit sequence number that the Frame Relay interface has sent to the Frame Relay management entity.

Total status enquiries
Indicates the total number of status enquiries that the Frame Relay interface has made of the Frame Relay management entity.

Total status responses
Indicates the total number of responses that the Frame Relay interface has received from the Frame Relay management entity in response to status enquiries.

Total sequence requests
Indicates the total number of sequence number requests that the Frame Relay interface has sent to the Frame Relay management entity.

Total responses
Indicates the total number of sequence number responses that the Frame Relay interface has received from the Frame Relay management entity.

Data compression enabled
Indicates whether data compression is enabled on this interface.

Orphan compression
Indicates whether orphan circuits on this interface will have data compression enabled.

Note: Enabling compression on orphan circuits will decrease the number of available compression contexts available for the native VCs on the device.

Orphan compression applies to both PVCs and SVCs.

Compression circuit limit
Specifies the maximum number of VCs that can compress data on this interface.

Active compression circuits
Specifies the number of VCs currently compressing data on this interface.

Data encryption enabled
Indicates whether data encryption is enabled on this interface.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95 .

Active encryption circuits
Indicates the number of VCs that are currently encrypting data.

Virtual Circuit Status:

Total allowed
Indicates the number of allowable VCs (including orphans) whose state is active, congested, removed, or inactive for use with this interface.

Total configured
Indicates the total number of currently configured VCs for this interface.

Total active
Indicates the number of active VCs on this interface.

Total congested
Indicates the number of VCs that are throttled down because of congestion within the network.

Total PVCs left net
Indicates the total number of PVCs that have been removed from the network.

Total PVCs joined net
Indicates the total number of PVCs that have been added to the network.

permanent-virtual-circuit
Displays general link-layer statistics and configuration information for all configured PVCs on the Frame Relay interface.

Example:

```
list permanent-virtual-circuit
                                Orphan   Type/    Frames       Frames
 Circuit#     Circuit Name     Circuit  State  Transmitted   Received
 --------  -----------------   -------  -----  -----------   ---------
     16    Valencia               No   %@*P/A            2         1
     17    Raleigh                No    @#P/A           15        14
     18    Boston                 No    &#P/A            0         0
     19    Orlando                No     *P/A            0         0
     20    Port Royal             No     $P/A            0         0
     21    New York               No     @P/A            2         0

    A - Active     I - Inactive   R - Removed   P - Permanent  C - Congested
    * - Required                  # - Required and belongs to a PVC group
    @ - Data compression capable but not operational
    & - Data compression capable and operational
    $ - Data encryption capable but not operational
    % - Data encryption capable and operational
```

Circuit#
Indicates the DLCI of the PVC.

Circuit Name
Name of the circuit, an ASCII string.

Orphan Circuit
Indicates whether the PVC is a non-configured circuit (yes or no).

Type/State
Indicates the state of the circuit, A (active), I (inactive), P (permanent), C (congested), or R (removed).

Frames Transmitted
Indicates how many frames this PVC has transmitted.

Frames Received
Indicates how many frames this PVC has received.

pvc-groups
Displays required PVC group information for all required PVC groups. For

each group this consists of the group name, the circuits in the group and the state (active, inactive, or removed) of each circuit.

Example:

```
list pvc-groups
Group name              Circuits in group    Circuit status
----------              -----------------    --------------

group1                            16             active
                                  44             inactive
                                 240             removed
```

svcs Displays all SVCs, either configured or orphaned, on the interface regardless of state.

Example:

```
FR 1>list svcs
                                                          Circuit  Call
          Circuit Name             Remote party number     State   State  DLCI
 -------------------------------  --------------------  -------  -----  -----
 flotsam                          911                      R       N       0
 jetsam                           666                      R       N       0
    Circuit states: A - Active   I - Inactive   R - Removed   C - Congested
    Call states: N - Null   I - Call Initiated   O - Outgoing call proceeding
                 A - Active   D - Disconnect request   R - Release request
```

switched-virtual-circuit

The following example displays configuration and operational information for a single SVC by name.

Example:

```
FR 1>list switched-virtual-circuit flotsam
 Circuit                          Opt-   Idle             Outgoing   Incoming
  Name                            ions   Timer              Value      Value

 -------------------------------- -----  ------          ----------  ----------

 flotsam                          ILM        60     CIR:         0           0
   Call state: Null                                 Burst:       0           0
   Call Initiated by: None        DLCI: 0         Excess:       0           0
   Remote party number: IE911
   Remote subaddress:   None

 Options: I - call-ins allowed, L - learn protocols, M - multicast required
          C - compression capable and operational, c - compression capable
          E - encryption capable and operational,  e - encryption capable

 Address type: I - International, U - Unknown
 Numbering plan: E - E.164, X - X.121
 Subaddress format: N - NSAP, P - private
```

virtual-circuits

Displays all PVCs and all active SVCs with associated information that is identical to the **list permanent-virtual-circuit** command.

```
FR 1>list virtual-circuits

 Circuit                                  Orphan  Type/   Frames      Frames
 Number           Circuit Name            Circuit State Transmitted  Received
 ------ -------------------------------- ------- ----- ----------- ----------
     16  circ16                             No     P/A           4          8
     17  Unassigned                         Yes  @ P/I           0          0
     18  flotsam                            No     S/A          12         10
     19  Unassigned                         Yes  @ P/A           7          2
     24  circ24                             No     P/R           0          0

    P - PVC   S - SVC   A - Active   I - Inactive   R - Removed   C - Congested
```

```
* - Required        # - Required and belongs to a PVC group
@ - Data compression capable but not operational
& - Data compression capable and operational
```

LLC

Use the **LLC** command to access the LLC monitoring prompt. LLC commands are entered at this new prompt. See “LLC Monitoring Commands” on page 221 for an explanation of each of these commands.

Syntax:

llc

Note: The LLC command is supported only if APPN is in the software load.

Notrace

Use the **notrace** command to disable packet tracing for individual circuits or the entire interface. This command can be used as a filter when tracing specific circuits or interfaces is required. The default setting is to trace all circuits.

Syntax:

notrace	circuit#
	circuitname
	all

Example:

```
notrace 16
     Disables packet tracing on circuit (PVC or SVC) with DLCI 16.
 notrace circuit phoenix
    Disables packet tracing on circuit (PVC or SVC) named phoenix.
 notrace circuit all
    Disables packet tracing on all circuits on this interface.
```

Set

Use the **set** command to set the values for Committed Information Rate (CIR), Committed Burst Rate, and Excess Burst Rate for the specified VC. You also can set values for IR adjustment rates.

Changes made with this command do not affect the configuration data. They are in effect only until the router is restarted.

Syntax:

set	circuit . . .
	ir-adjustment . . .

circuit *circuit# or name cirvol bcval beval*

Sets the values for Committed Information Rate (CIR), Committed Burst Rate, and Excess Burst Rate for the specified VC and can be used to change the operational outgoing CIR, Bc, and Be for a PVC or an active SVC.

Example:

```
set circuit
Circuit number [16]?
Committed Information Rate (CIR) in bps [1200]?
Committed Burst Size (Bc) in bits [1200]?
Excess Burst Size (Be) in bits [56000]?
```

Circuit Number

Indicates the circuit number in the range 16 to 1007.

Committed Information Rate

Indicates the committed information rate (CIR). The CIR can be either 0 or a value in the range 300 bps to 2048000 bps. The default is 64000 bps. For more information, see “Committed Information Rate (CIR)” on page 318.

Committed Burst Size

The maximum amount of data in bits that the router will send during a measurement interval equal to committed burst (Bc) size / CIR seconds. The range is 300 to 2048000 bits. The default value is 64000 bits.

Note: If CIR is configured as 0 then the committed burst size is set to 0 and you are not prompted for a value. For additional information, see “Committed Burst (Bc) Size” on page 319.

Excess Burst Size

The maximum amount of uncommitted data in bits in excess of committed burst size that the router attempts to deliver during a measurement interval equal to (Committed Burst Size/CIR) seconds. Range is 0 to 2048000 bits. Default is 0. For additional information, see “Excess Burst (Be) Size” on page 319.

ir-adjustment *increment-% decrement-% minimum-IR*

Sets the minimum information rate (IR) and the percentages for incrementing and decrementing the IR in response to network congestion.

The minimum IR, expressed as a percentage of CIR, is the lower limit of the information rate. The minimum percentage is 1 and the maximum percentage is 100. The default is 25.

When network congestion clears, the information rate is gradually incremented by the IR adjustment increment percentage until the maximum information rate is reached. The minimum percentage is 1 and the maximum percentage is 100. The default is 12.

When network congestion occurs, the information rate is decremented by the IR adjustment decrement percentage each time a frame containing BECN is received until the minimum information rate is reached. The minimum percentage is 1, and the maximum percentage is 100. The default is 25.

Example:

```
set ir-adjustment
    IR adjustment % increment [12]?
    IR adjustment % decrement [25]?
    Minimum IR as % of CIR [25]?
```

Trace

Use the **Trace** command to enable packet tracing for individual circuits or the entire interface and to list the tracing capability of all circuits on this interface. This command can be used as a filter when tracing specific circuits or interfaces is required. The default setting is to trace all circuits.

Syntax:

trace	all
	circuitname
	circuit#
	list

Example:

```
trace 16
     Enables packet tracing on circuit (PVC or SVC) with DLCI 16.
trace circuit phoenix
    Enables packet tracing on circuit (PVC or SVC) named phoenix.
trace circuit all
    Enables packet tracing on all circuits on this interface.

trace list
 The following circuits are available for packet trace
 Circuit Name                    Circuit Number
 -------------------------------     --------------
 Unassigned                             16
 phoenix                                25
 jetsam                                  0

 Lists the packet tracing capability of all circuits on this
 interface.
```

Frame Relay Interfaces and the GWCON Interface Command

While Frame Relay interfaces have a monitoring process for monitoring purposes, the router also displays complete statistics for installed interfaces when you use the **interface** command from the GWCON environment. (For more information on the **interface** command, refer to “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 111)

Statistics Displayed For Frame Relay Interfaces

Statistics similar to the following are displayed when you execute the **interface** command from the GWCON environment for Frame Relay interfaces:

Nt Indicates the interface number as assigned by software during initial configuration.

Nt’ Indicates the interface number as assigned by software during initial configuration.

Note: For FR dial circuit interfaces, Nt’ is different from Nt. Nt’ indicates the base interface (ISDN) that the dial circuit is running over.

Interface
Indicates the type of interface and its instance number. Frame relay has a FR designation.

Slot Indicates the slot of the interface running Frame Relay

Port Indicates the port of the interface that is running Frame Relay

Self-test Passed
Indicates the total number of times the Frame Relay interface passed self-test.

Self-test Failed
Indicates the total number of times the Frame Relay interface failed self-test.

Maintenance Failed
Indicates the total number of times the interface was unable to communicate with Frame Relay management.

V.24 circuit, Nicknames, and State
The circuits, control signals, pin assignments and their state (ON or OFF). Note: The symbol - - - in monitoring output indicates that the value or state is unknown.

Line speed
The transmit clock rate.

Last port reset
The length of time since the last port reset.

Input frame errors:

CRC error
The number of packets received that contained checksum errors and as a result were discarded.

Alignment
The number of packets received that were not an even multiple of 8 bits in length and a result were discarded.

Too short
The number of packets that were less than 2 bytes in length and as a result were discarded.

Too long
The number of packets that were greater than the configured size, and as a result were discarded.

Aborted frame
The number of packets received that were aborted by the sender or a line error.

DMA/FIFO overrun
The number of times the serial interface could not send data fast enough to the system packet buffer memory to receive them from the network.

Missed frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the

buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the `L & F bits not set` counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the `L & F bits not set` counter will be affected by traffic.

Output frame counters:

DMA/FIFO underrun errors
The number of times the serial interface could not retrieve data fast enough from the system packet buffer memory to transmit them to the network.

Output aborts sent
The number of transmissions that were aborted as requested by upper-level software.

Statistics similar to the following are displayed for Frame Relay dial circuits when you execute the interface command from the GWCON environment:

```
+interface 3

                                                  Self-Test  Self-Test  Maintenance
Nt Nt'  Interface                          Passed      Failed      Failed
3   2    FR/1                                    1             0              0

    Frame Relay MAC/data-link on ISDN Primary Rate interface
```

Chapter 27. Using Point-to-Point Protocol Interfaces

This chapter describes how to use the Point-to-Point Protocol for interfaces on the device. Sections in this chapter include:

See "Chapter 29. Using the Multilink PPP Protocol" on page 431 and "Chapter 30. Configuring and Monitoring Multilink PPP Protocol (MP)" on page 437 for information about using the Multilink PPP Protocol.

PPP Overview

PPP provides a method for transmitting protocol datagrams at the Data Link Layer over serial point-to-point links. PPP provides the following services:

- Link Control Protocol (LCP) to establish, configure, and test the link connection.
- Encapsulation protocol for encapsulating protocol datagrams over serial point-to-point links.
- Authentication protocols (APs) to validate the identity of a peer (remote) unit, and to submit your own identity to the peer for validation.
- Network Control Protocols (NCPs) for establishing and configuring different network layer protocols. PPP allows the use of multiple network layer protocols.

Figure 23 on page 372 shows some examples of point-to-point serial links.

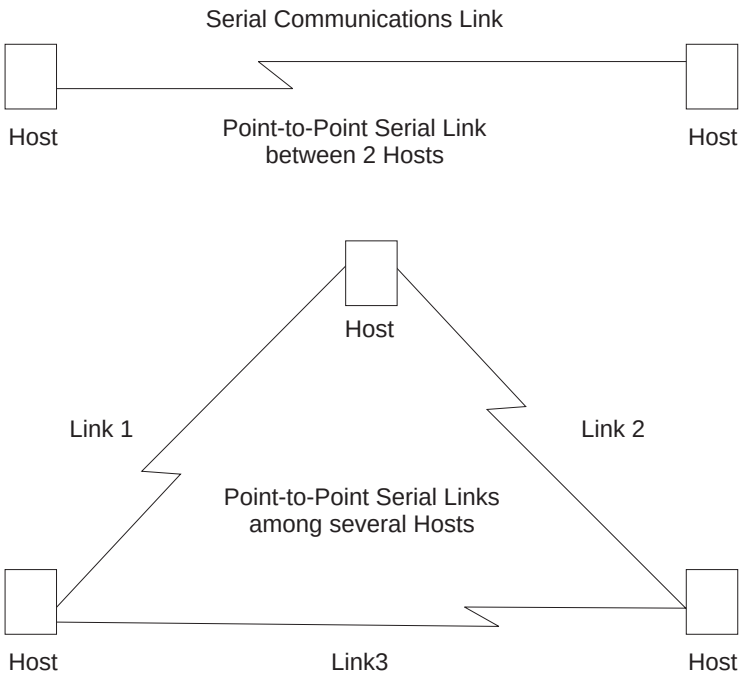

Figure 23. Examples of Point-to-Point Links

PPP currently supports the following control protocols:

- AppleTalk Control Protocol (ATCP)
- DECnet Protocol Control Protocol (DNCP)
- Banyan VINES Control Protocol (BVCP)
- Bridging protocols (BCP, NBCP, and NBFCP)
- Internet Protocol Control Protocol (IPCP)
- Internet Protocol Version 6 Control Protocol (IPv6CP)
- IPX Control Protocol (IPXCP)
- APPN HPR Control Protocol (APPN HPRCP)
- APPN ISR Control Protocol (APPN ISRCP)
- OSI Control Protocol (OSICP)

Each end starts by sending LCP packets to configure and test the data link. After the link has been established, PPP sends NCP packets to choose and configure one or more network layer protocols. After network layer protocols have been configured, datagrams from each network layer can be sent over the link. The next sections explain these concepts in more detail.

PPP Data Link Layer Frame Structure

PPP transmits data frames that have the same structure as High-level Data Link Control (HDLC) frames. PPP uses a byte-oriented transmission method with a single-frame format for all data and control exchanges. Figure 24 on page 373 illustrates the PPP frame structure and is followed by a detailed description of each field.

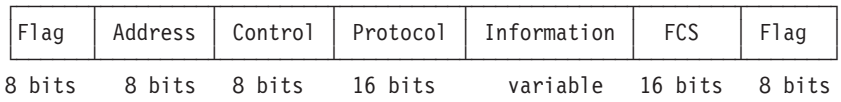

Figure 24. PPP Frame Structure

Flag Fields
The flag field begins and ends each frame with a unique pattern of 01111110. Generally a single flag ends one frame and begins the next. The receiver attached to the link continuously search for the flag sequence to synchronize the start of the next frame.

Address Field
The address field is a single octet (8 bits) and contains the binary sequence 11111111 (0xff hexadecimal). This is known as the All-Station Address. PPP does not assign individual station addresses.

Control Field
The control field is a single octet and contains the binary sequence 00000011 (0x03 hexadecimal). This sequence identifies the Unnumbered Information (UI) command with the P/F bit set to zero.

Protocol Field
The protocol field is defined by PPP. The field is 2 octets (16 bits) and its value identifies the protocol datagram encapsulated in the Information field of the frame.

Protocol field values in the range '0xC000'–'0xFFFF' indicate Layer 3 data (protocol datagrams) such as LCP, PAP, CHAP,

Information Field
The information field contains the datagram for the protocol specified in the protocol field. This is zero or more octets.

When the protocol type is LCP, exactly one LCP packet is encapsulated in the information field of PPP Data Link Layer frames.

Frame Check Sequence (FCS) Field
The frame check sequence field is a 16-bit cyclic redundancy check (CRC).

PPP links can negotiate the use of various options which may modify the basic frame format; the description below applies to the frame format prior to any such modifications. PPP LCP packets are always sent in this format as well, regardless of negotiated options, so that LCP packets can be recognized even when there is a loss of synchronization on the line.

The router supports two such options: Address and Control Field Compression (ACFC) and Protocol Field Compression (PFC). These are described in detail in a later section.

The PPP Link Control Protocol (LCP)

PPP's Link Control Protocol (LCP) establishes, configures, maintains, and terminates the point-to-point link. This process is carried out in four phases:

1. Before exchanging any network layer datagrams, PPP first opens the connection through an exchange of LCP configuration packets. As part of this negotiation process, the PPP processes at each end of the link agree on

various basic link level parameters such as the maximum packet size that can be transferred and whether the ends must use an authentication mechanism to identify themselves to their peers before carrying network traffic.

If this negotiation is unsuccessful, the link is considered to be “down” and incapable of carrying any network traffic. If the negotiation is successful, LCP goes to an “Open” state and PPP goes on to the next phase.

2. After LCP successfully reaches an Open state, the next step in establishing the link is to perform authentication where each end of the link identifies itself to the other end using the “authentication protocol” that the other end dictated as part of the LCP negotiation.

   If authentication fails, the link is marked “down” and cannot carry any network traffic. If authentication succeeds or if authentication is not required, the PPP link moves to the next phase.

3. After authentication is negotiated, the peers negotiate encryption for the link. After authentication phase is complete, the router negotiates the use of encryption using Encryption Control Protocol (ECP) packets where each end of the link negotiates which encryption algorithm will be used to encrypt the data over this PPP link. If ECP did not reach “Open” state then the link is marked “down” and cannot carry any network traffic. If ECP successfully reaches “Open” state, or if encryption is not required, the PPP link moves to the next phase, NCP negotiation (except ECP, which is technically also an NCP). The link is considered to be “open” or “up” at this time, though it cannot yet carry layer-3 protocol datagrams.

4. Once the link is open, the router negotiates the use of various layer-3 protocols (for example, IP, IPX, DECnet, Banyan Vines) using Network Control Protocol (NCP) packets. Each layer-3 protocol has its own associated network control protocol. For example IP has IPCP and IPX has IPXCP. The basic format and mechanisms for all these NCP packets is the same for all protocols, and is basically a superset of the LCP mechanisms as described later in this section.

   Each layer-3 protocol is negotiated independently. When a particular NCP successfully negotiates, the link is “up” for that protocol’s traffic. As with LCP, configuration information can be exchanged as part of this negotiation; for example, IPCP can exchange IP addresses or negotiate the use of ″Van Jacobson IP header compression″.

   As with LCP, it is possible for an NCP to fail to negotiate successfully with its peer. This might happen because the peer does not support a particular protocol or because some configuration option was unacceptable. If an NCP fails to reach the “Open” state, no layer-3 protocol packets can be exchanged for that protocol even though other layer-3 protocols are successfully passing traffic across the PPP link.

5. Finally, LCP has the ability to terminate the link at any time. This is usually done at the request of the user but may occur for other reasons such as: an administrative closing of the link, idle timer expiration, or failure to re-authenticate on a CHAP rechallenge.

For complete details about PPP LCP, authentication, and the general NCP negotiation mechanisms, consult RFCs 1331, 1334, 1570, and 1661.

LCP Packets

LCP packets are used to establish and manage a PPP link and can be loosely divided into three categories:

- *Link establishment packets* that exchange configuration information and establish the link.
- *Link termination packets* that shut down the link or signal that a link is not accepting connections at a particular time. They also can be used to signal that a particular protocol is unrecognized (for example, during NCP negotiations).
- *Link maintenance packets* that monitor and debug a link.

Exactly one LCP packet is encapsulated in the information field of PPP Data Link Layer frames. In the case of LCP packets, the protocol field reads “Link Control Protocol” (C021 hexadecimal). Figure 25 illustrates the structure of the LCP packet and is followed by a detailed description of each field.

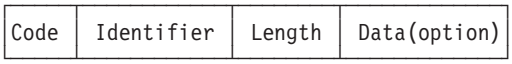

Figure 25. LCP Frame Structure (in PPP Information Field)

Code The code field is one octet in length and identifies the type of LCP packet. The codes in Table 45 distinguish the packet types. They are described in more detail in later sections.

Table 45. LCP Packet Codes

Code	Packet Type
1	Configure-Request (Link Establishment)
2	Configure-Ack (Link Establishment)
3	Configure-Nak (Link Establishment)
4	Configure-Reject (Link Establishment)
5	Terminate-Request (Link Termination)
6	Terminate-Ack (Link Termination)
7	Code-Reject (Link Establishment)
8	Protocol-Reject (Link Establishment)
9	Echo-Request (Link Maintenance)
10	Echo-Reply (Link Maintenance)
11	Discard-Request (Link Maintenance)

Identifier
The identifier field is one octet in length and is used to match packet requests to replies.

Length
The length field is two octets in length and indicates the total length (that is, including all fields) of the LCP packet.

Data (Option)
The data field is zero or more octets as indicated by the length field. The format of this field is determined by the code.

NCP packets are structured identically to LCP packets and are distinguished by having different PPP “Protocol” values. Each LCP packet type (distinguished by the code field) has the same meaning for each NCP, though an individual NCP may not implement all possible LCP packet types. NCPs normally implement all of the link establishment type packets that LCP defines. They may implement some of the additional LCP packet types, and they also may define additional packet types beyond what LCP uses. Unlike LCP packets, the structure of an NCP frame may be modified according to options negotiated by LCP during the link establishment phase.

Link Establishment Packets

Link Establishment Packets establish and configure a point-to-point link including the following packet types:

Configure-Request
LCP packet code field is set to 1. LCP transmits this packet type when it wants to open a point-to-point link. Upon receiving a Configure-Request, a peer station's LCP entity sends an appropriate reply, depending on whether it is ready to process packets.

Configure-Ack
LCP packet code field is set to 2. The peer transmits this packet type when every configuration option in a Configure-Request packet is acceptable. Upon receiving the Configure-Ack (ack = acknowledgment), the originating station checks the Identifier field. This field must match the one from the last-transmitted Configure-Request or the packet is invalid.

Both ends send Configure-Request and both ends must receive a Configure-Ack before the link opens. Options negotiated for one direction may differ from that negotiated for the other direction. There is no "master-slave" relationship. Rather, each end works symmetrically.

Configure-Nak
LCP packet code field is set to 3. The peer transmits this packet type when some part of the configuration option in a Configure-Request packet is unacceptable. The Identifier field is copied from the received Configure-Request and the Data (option) field is filled with the received unacceptable configuration options. The Identifier field must match the one from the last-transmitted Configure-Request or the packet is invalid and is discarded.

When the originator receives a Configure-Nak packet, a new Configure-Request packet is sent that includes modified, acceptable configuration options.

Configure-Reject
LCP packet code field is set to 4. The peer transmits this packet type when some part of the configuration options in a Configure-Request packet is unacceptable. The Identifier field is copied from the received Configure-Request and the Data (option) field is filled with the received unacceptable configuration options. The Identifier field must match the one from the last-transmitted Configure-Request or the packet is invalid and is discarded.

When the originator receives a Configure-Reject packet, a new Configure-Request packet is sent that does not include any of the configuration options received in the Configure-Reject packet.

Code-Reject
LCP packet code field is set to 7. The transmission of this packet type indicates that the LCP "code" field on a received packet is not recognized as a valid value. While this can indicate an error, it also can indicate that the peer does not implement some feature that you are trying to use.

Protocol-Reject
LCP packet code field is set to 8. The transmission of this packet type indicates that a PPP frame has been received that contains an unsupported or unknown protocol (the PPP "protocol" field was unrecognized for some packet). This usually occurs if you try to negotiate some NCP for a protocol

that the other end doesn't support. For example, if DECnet CP (DNCP) sends a Config-Request and the other end does not know about DECnet, the other end replies with an LCP Protocol-Reject on DNCP. Upon receiving a Protocol-Reject packet, the link stops transmitting the incorrect protocol.

Note: NCP packet types and structure are the same as LCP, although there are a few additional "code" fields associated with some NCPs.

Link Termination Packets

Link Termination Packets terminate a link and include the following packet types:

Terminate-Request
LCP packet code field is set to 5. LCP transmits this packet type when a point-to-point link needs to be closed. These packets are sent until a Terminate-Ack packet is sent back, or until a retry counter is exceeded while waiting for an Ack.

Terminate-Ack
LCP packet code field is set to 6. Upon receiving a Terminate-Request packet, this packet type must be transmitted with the code field set to 6. Reception of an Terminate-Ack packet that was not expected indicates that the link has been closed.

Link Maintenance Packets

Link Maintenance Packets manage and debug a link, and include the following packet types:

Echo-Request and Echo-Reply
LCP packet code fields are set to 9 and 10 respectively. LCP transmits these packet types in order to provide a Data Link Layer loopback mechanism for both directions on the link. This feature is useful, for example, in debugging a faulty link to determine link quality. These packets are sent only when the link is in the Open state.

Discard-Request
LCP packet code field is set to 11. LCP transmits this packet type to provide a data sink for Data link Layer testing. A peer that receives a Discard-Request ***must*** throw away the packet. This is useful in debugging a link. These packets are sent only when the link is in the Open state.

PPP Authentication Protocols

PPP authentication protocols provide a form of security between two nodes connected via a PPP link. If authentication is required on a box, then immediately after the two boxes successfully negotiate the use of the link at the LCP layer (LCP packets are exchanged until LCP goes into an "open" state), they go into an "authentication" phase where they exchange authentication packets. A box is neither able to carry network data packets nor negotiate the use of a network protocol (NCP traffic) until authentication negotiation completes successfully.

There are different authentication protocols in use: Password Authentication Protocol (PAP) and Challenge/Handshake Authentication Protocol (CHAP). Microsoft PPP CHAP (MS-CHAP) is also available to authenticate Windows workstations and peer routers. PAP and CHAP are described in detail in RFC 1334, and briefly described later in this section. MS-CHAP is described in RFC 1994.

On remote dial-in access ports, a third authentication protocol is available. This is Shiva Password Authentication Protocol (SPAP), which is a Shiva proprietary protocol. See “Shiva Password Authentication Protocol (SPAP)” on page 379 for more information.

Whether a box requires the other end to authenticate itself (and if so, with what protocol) is determined during the LCP negotiation phase. Authentication could be considered to “fail” even at the link establishment phase (LCP negotiation), if one end does not know how, or refuses to use, the authentication protocol the other end requires.

Each end of a link sets its own requirements for how it wants the other end to authenticate itself. For example, given two routers “A” and “B”, connected over a PPP link, side A may require that B authenticate itself to A using PAP, and side B may require that A similarly identify itself using CHAP. It is valid for one end to require authentication while the other end requires none.

In addition to initial authentication during link establishment, with some protocols an authenticator may demand that the peer reestablish its credentials periodically. With CHAP, for example, a rechallenge may be issued at any time by the authenticator and the peer must successfully reply - or lose the link.

If more than one authentication protocol is enabled on a link, the router initially attempts to use them in the following priority order:

1. MS-CHAP
2. CHAP
3. PAP
4. SPAP

Note: SPAP is only available on interfaces that have IBM DIALs Dial-In circuits configured.

If the remote side responds to the authentication request with NAK and suggests an alternative, the router uses the alternative, provided that it is enabled on the link. If the remote side continues responding to the router’s suggestions with NAK but does not provide an alternative that the router has enabled, the link is terminated.

Password Authentication Protocol (PAP)

The Password Authentication Protocol (PAP) provides a simple method for the peer to establish its identity using a two-way handshake. This is done only upon initial link establishment. Following link establishment, the peer sends an ID/Password pair to the authenticator until authentication is acknowledged or the connection is terminated. Passwords are sent over the circuit “in the clear,” and there is no protection from playback or repeated trial and error attacks. The peer controls the frequency and timing of the attempts.

Challenge-Handshake Authentication Protocol (CHAP)

The Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a three-way handshake. This is done upon initial link establishment, and *may* be repeated anytime after the link has been established. After the initial link establishment, the authenticator sends a “challenge” message to the peer. The peer responds with a value calculated using a “one-way

hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection is terminated.

Microsoft PPP CHAP Authentication (MS-CHAP)

MS-CHAP is an extension to PPP CHAP that is used to authenticate remote Windows workstations and peer routers. Both MS-CHAP and CHAP use PPP's Link Control Protocol (LCP) to negotiate the desired authentication protocol in one or both directions; both use the CHAP protocol identifier as the PPP protocol; and each protocol uses a random challenge which is encrypted as part of the response.

MS-CHAP can be used with the internal PPP user Local List database, but ***not*** with the external AAA authentication server that is described in the chapter "Using Local or Remote Authentication" in *Using and Configuring Features*. If you plan to use Microsoft PPP Encryption (MPPE) on a PPP interface, you must enable MS-CHAP on that interface before you configure MPPE. Use the talk 6 command **enable mschap** to enable MS-CHAP.

Shiva Password Authentication Protocol (SPAP)

Note: SPAP is only available on interfaces that have IBM DIALs Dial-In circuits configured.

The Shiva Password Authentication Protocol (SPAP) provides a simple method for the peer to establish its identity using a 2-way handshake similar to PAP. After the Link Establishment phase is complete, an Id/Password is repeatedly sent by the peer to the authenticator until authentication is acknowledged, the connection is terminated, or a retry counter expires.

SPAP is a moderately strong authentication protocol that uses a proprietary encryption algorithm for the password. In addition to authentication, SPAP offers:

- The ability to change a password.

  Note: SPAP change password support is not available on the 2212.
- The ability for the router to send a configurable banner requiring acknowledgment from the client after password authentication.
- The ability to use callback as an additional security feature.
- Virtual connections.

Configuring PPP Authentication

The following sections describe configuring PPP authentications for two situations:

- Configuring the 2212 to authenticate a remote device.
- Configuring the 2212 to be authenticated by a remote device.

These two situations are independent. You can do one or the other.

Configuring a PPP Interface to Authenticate a Remote Device

To authenticate a remote device or dial-in client:

1. Enable authentication on the PPP interface

- At the Config> prompt, enter the **network** command to select the PPP interface to configure.
- At the PPP Config> prompt, enable the authentication protocol you want to use.

  You can use any of the following protocols:

  – PAP

  – MS-CHAP

  Note: MS-CHAP can use the PPP local database to authenticate, but cannot use an authentication server.

  – CHAP

  – SPAP

  Note: SPAP is only available on interfaces that have IBM DIALs Dial-In circuits configured.

2. Decide whether to authenticate locally or through an authentication server.
   - To authenticate locally, enter the name and password into the PPP user database.

     At the Config> prompt, use the **add ppp_user** command. See “Add” on page 76 for more information.

     A 2212 maintains a single PPP user database. When the remote router or device sends its name and password to the device during the authentication phase, the device checks to see if that name and password are in the PPP user database.

   - To authenticate through an authentication server using TACACS, TACACS+, or RADIUS, you must configure the device to reach the authentication server and the name and password must be in the server’s database. Refer to “Using Local or Remote Authentication” in *Using and Configuring Features*.

Configuring a PPP Interface to be Authenticated by a Remote Device

To configure the device to be authenticated by a remote device or dial-in client, configure the device’s name and password:

1. At the Config> prompt, select the interface you are configuring using the **network** command.
2. At the PPP Config> prompt, type the **set name** command and provide the name and password that the device will use to identify itself to the remote router or device during the authentication phase.

Attention: Do not use the following commands unless you want the device to perform authentication as described in “Using Local or Remote Authentication” in *Using and Configuring Features* .

- **enable pap**
- **enable chap**
- **enable spap**

  Note: SPAP is only available on interfaces that have IBM DIALs Dial-In circuits configured.

- **enable mschap**

Configuring PPP Callback

Callback is a PPP feature associated with single user dial-in solutions. It attempts to accomplish two objectives. These objectives are:

- Callback can be used as a form of security. When used in this way, callback is generally referred to as required callback. When required callback is negotiated the user will be dialed back at a predetermined number. Only then will the PPP link be allowed to come up.
- Callback can also be implemented as a toll-saver feature. When used in this way, callback is generally referred to as roaming callback. Unlike required callback, roaming callback is requested by the client. The primary function of roaming callback is to bill the company maintaining the DIALs Server the toll charges instead of the user.

Callback is supported only on dial-in dial circuits over ISDN networks.

Example 1: Required callback enabled

```
Config>add PPP
Enter user name: [ ]? nocallback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user nocallback [0.0.0.0]?
Enter HostName: [ ]?
Give 'nocallback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'nocallback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback] Requ
Dialback number for this user [ ]? 555-1234
Will 'nocallback' be able to dial-out ? (Yes, No): [No]

PPP User Name: nocallback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Alotted: Box Default
Call-Back Type: Required Callback
Phone Number: 543-3186
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

Example 2: Callback disabled

```
Config>add PPP
Enter user name: [ ]? sallydoe
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user nocallback [0.0.0.0]?
Enter HostName: [ ]?
Give 'no callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'no callback' ? (Yes, No): [No]
Will 'no callback' be able to dial-out ? (Yes, No): [No]


PPP User Name: no callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Alotted: Box Default
Call-Back Type: Not Enabled
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

Example 3: Roaming callback enabled

```
Config>add PPP roaming_callback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]
```

```
IP address for user roaming_callback [0.0.0.0]?
Enter HostName: []?
Give 'roaming_callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'roaming_callback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback]

Will 'roaming_callback' be able to dial-out ? (Yes, No): [No]n

PPP User Name: roaming_callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Alotted: Box Default
Call-Back Type: Roaming Callback
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No]yes
```

Using AAA with PPP

See “Using Local or Remote Authentication” and “Configuring Authentication” in *Using and Configuring Features* for this information.

The PPP Network Control Protocols

PPP has a family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols. The NCPs are responsible for configuring, enabling, and disabling the network layer protocols on both ends of the point-to-point link. NCP packets cannot be exchanged until LCP has opened the connection and the link reaches the OPEN state.

PPP supports the following Network Control Protocols:

- AppleTalk Control Protocol (ATCP)
- Banyan VINES Control Protocol (BVCP)
- Bridging protocols (BCP, NBCP, and NBFCP),
- Callback Control Protocol
- DECnet Control Protocol (DNCP)
- IP Control Protocol (IPCP)
- IPv6 Control Protocol (IPv6CP)
- IPX Control Protocol (IPXCP)
- OSI Control Protocol (OSICP)
- APPN High Performance Routing Control Protocol (APPN HPRCP)
- APPN Intermediate Session Routing Control Protocol (APPN ISRCP)

AppleTalk Control Protocol

ATCP is specified in Request for Comments (RFC) 1378. IBM’s implementation of ATCP supports the AppleTalk-Address option. The implementation supports both full router mode and half router mode. For additional information, refer to “AppleTalk over PPP” in *Protocol Configuration and Monitoring Reference Volume 2*

Banyan VINES Control Protocol

RFC 1763 describes BVCP. IBM’s implementation of BVCP does not support any options.

Bridging Control Protocol

BCP is specified in RFC 1638. IBM's implementation of BCP supports the IEEE 802.5 Line Identification Option and the Tinygram Compression Option.

NetBIOS Control Protocol (NBCP) is a proprietary NCP developed by Shiva Corporation and used by the IBM Dial In Access to LAN Client for OS/2, DOS and Windows for single-user dial-in. NBCP is used to transport NetBIOS and LLC/802.2 bridged traffic from these clients, dialed into a 2212 DIALs Server, onto an attached LAN. IBM's implementation of NBCP supports the MAC-Address and NetBIOS Name Projection options.

NetBIOS Frame Control Protocol (NBFCP) is specified in RFC 2097. NBFCP is used by Microsoft Windows 95 and Windows NT Dial-Up Networking clients for single-user dial-in. NBFCP is used to transport NetBIOS bridged traffic from these clients, dialed into a 2212 DIALs Server, onto an attached LAN. IBM's implementation of NBFCP supports the Name-Projection, Peer-Information and IEEE-MAC-Address-Required options.

Callback Control Protocol

Note: CBCP is only available on interfaces that have IBM DIALs Dial-in circuits configured.

Callback Control Protocol (CBCP) is used by Microsoft Dial-Up Networking clients to negotiate callback. The 2212 supports callback to a single user-specified number (roaming callback) and callback to an administrator-specified number (required callback). The CBCP option of calling a list of numbers is not supported.

PPP users that want to use CBCP callback must have some form of authentication enabled (like PAP, CHAP, SPAP or MS-CHAP). There are no configuration parameters for CBCP. (The client determines when it is used.) See "Configuring PPP Callback" on page 381 for information about configuring PPP users for callback.

DECnet IV Control Protocol

DNCP is specified in RFC 1762. IBM's implementation does not support any DNCP options.

IP Control Protocol

IPCP is specified in RFC 1332. IBM's implementation supports the following options:

- Van Jacobsen IP Header Compression as described in RFC 1144.
- IP Address

  The router can send its IP address, as well as accept an IP address, from a peer, or supply an IP address to a peer, if requested. If the router is configured to "Send Our Address" on a particular interface, and that interface has a valid, numbered IP address, then IPCP sends the address in its initial Configure-Request as option 3 (IP Address). IPCP also sends its address if the peer sends a Configure NAK with 0.0.0.0 for option 3 (IP Address), if a valid numbered address is configured for that PPP interface. IPCP will not send an unnumbered address to its peer.

A peer may specify its address (referred to as “Client Specified”), or request an address from the router by sending 0.0.0.0 for Option 3 in its initial Configure Request. The router may obtain this address from the authenticated user profile or from the interface itself. The user profile address takes precedence over the interface address. If you do not want to offer an address from the user profile, simply leave the address for that user in the profile as 0.0.0.0, and the router will offer the remote address configured for that interface. If there is no remote address configured for the interface or user profile, and the peer continues to request an address, IPCP will fail.

The router automatically adds a static route directed to the PPP interface for the address that is successfully negotiated, allowing data to be routed properly to the dial-in client. When the IPCP connection is ended for any reason, this static route is subsequently removed. By default, the net mask for this route is 255.255.255.255 (hostroute); however, if a net mask is specified in the authenticated user’s profile (see “Configuring PPP Authentication” on page 379) a net mask other than this may be used to allow routing to more than a single host across the PPP link (RIP or other routing protocols could also be used to discover routes if desired).

IPv6 Control Protocol

IPv6 Control Protocol is specified in RFC 2023. In IBM’s implementation of IPv6CP, the router can send its IP address, as well as accept an IP address, from a peer, or supply an IP address to a peer, if requested. If the router is configured to “Send Our Address” on a particular interface, and that interface has a valid, numbered IP address, then IPv6CP sends the address in its initial Configure-Request as option 3 (IP Address). IPv6CP also sends its address if the peer sends a Configure NAK with ::/0 for option 3 (IP Address), if a valid numbered address is configured for that PPP interface. IPv6CP will not send an unnumbered address to its peer.

A peer may specify its address (referred to as “Client Specified”), or request an address from the router by sending ::/0 for Option 3 in its initial Configure Request. The router obtains this address from the interface. If there is no remote address configured for the interface, and the peer continues to request an address, IPv6CP will fail.

The router automatically adds a static route directed to the PPP interface for the address that is successfully negotiated, allowing data to be routed properly to the dial-in client. When the IPv6CP connection is ended for any reason, this static route is subsequently removed. By default, the prefix length for this route is 128 (hostroute).

IPX Control Protocol

IPXCP is specified in RFC 1552. IBM’s implementation does not support any IPXCP options.

OSI Control Protocol

OSICP is specified in RFC 1377. IBM’s implementation of OSICP does not support any options.

APPN HPR Control Protocol

Advanced Peer-to-Peer Networking (APPN) High Performance Routing (HPR) control protocol is specified in RFC 2043. No options are negotiated for this control protocol.

APPN ISR Control Protocol

Advanced Peer-to-Peer Networking (APPN) Intermediate Session Routing (ISR) control protocol is specified in RFC 2043. No options are negotiated for this control protocol.

See “Overview of Encryption” in *Using and Configuring Features* for information about configuring encryption for a PPP interface.

Using and Configuring Virtual Connections

Virtual Connections (VC) are DIALs dial-in circuits that can be suspended when they become inactive for a predetermined period of time. The ability to suspend the connections can help control your networking costs by saving line charges for DIALs dial-in clients that are not active; instead of keeping the connections active, the system saves information about the session and then closes the call. When the same DIALs dial-in client reconnects to the server, the session information is restored and the connection resumes as if there were no interruption. See “Configuring a VC” for more information.

You can configure DIALs servers to end VCs that have been suspended for a specified amount of time. You can also manually end a VC at any time. See the **set** DIALs command and “DIALs Global Monitoring Commands” in *Using and Configuring Features* for related commands.

VC Considerations

Keep the following in mind as you configure VCs:

- You can only use AAA local-list or RADIUS authentication when using VCs.
- A VC will not support IPX. When you configure a user to use VCs, IPX support for that user is disabled.
- The client configuration controls the suspension and resumption of a VC. The DIALs server cannot control that aspect of the connection.
- A VC can be established through an MP bundle.
- VCs cannot run over L2TP.
- Suspended VCs cannot be displayed with current network management tools.
- Do not assign an IP address to remote users by interface. Because another client could use an interface with which a client establishes a VC, when the VC attempts to reconnect with the server the connection will fail because the IP address is in use.
- A dial-in client must use SPAP for authentication.

Configuring a VC

Configure VCs when you add a DIALs client at the `Config>` prompt. When you configure the user, you can either use the DIALs dial-in defaults (see the **set** DIALs

command in the *Using and Configuring Features*) for the maximum suspend time and inactivity timeout, or configure specific values for the particular client. The following example shows the minimum configuration for a VC for DIALs dial-in client "jose."

```
Config>
Config> add ppp
Enter user name:  []? jose
Password:
Enter password again:
Is this a 'DIALs' user? (Yes, No): [Yes§
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Enter hostname for dynamic DNS:  []?
Allow Virtual Connections ? (Yes, No): [No] Yes
   Use Box Default inactivity timeout value and maximum suspended time? (Yes, No): [Yes] No
   User-based Max Suspend Time (hours)
   0-48 0=unlimited: [12] ? 10
   User-based Inactivity Timeout (seconds)
   10-1024: [30] ? 60
Give 'jose' default time allotted ? (Yes, No): [Yes]
Enable callback for 'jose' ? (Yes, No): [No]
Will 'jose' be able to dial-out ? (Yes, No): [No]


      PPP user name: jose
    User IP address: Interface Default
      Netroute Mask: 255.255.255.255
           Hostname:
       Time alotted: Box Default
      Callback type: Not Enabled
           Dial-out: Not Enabled

Is information correct? (Yes, No, Quit): [Yes]

User 'jose' has been added
Config>
```

To display the box-level default values for maximum virtual connections, idle timeout period, and the global default maximum suspend time, use the `DIALs config>`**list vc-parameters** command in the DIALs feature. To display these parameters along with the maximum suspend time and inactivity timeout for all virtual connections, use the **list all** command in the DIALs feature. See "DIALs Global Monitoring Commands" in *Using and Configuring Features*.

Chapter 28. Configuring and Monitoring Point-to-Point Protocol Interfaces

This chapter describes Point-to-Point Protocol interface configuration and operational commands in the device. Sections in this chapter include:

Accessing the Interface Configuration Process

Use the following procedure to access the router's configuration process. This process gives you access to a specific interface's *configuration* process.

1. At the OPCON prompt (*), enter the **status** command to find the PID for CONFIG. (See page 11 for sample output of the **status** command.)
2. At the OPCON prompt, enter the OPCON **talk** command and the PID for CONFIG. (For more detail on this command, refer to "Chapter 3. The OPCON Process" on page 27.) For example:

   ```
   * talk 6
   ```

   After you enter the talk 6 command, the CONFIG prompt (Config>) displays on the console. If the prompt does not appear when you first enter **CONFIG**, press **Return** again.
3. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.
4. Record the interface numbers.
5. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

   ```
   Config> network 1
   ```

   The appropriate configuration prompt (such as TKR Config> for token-ring), now displays on the console.

Note: Not all network interfaces are user-configurable. For interfaces that cannot be configured, you receive the message:

```
That network is not configurable
```

Accessing the PPP Interface Configuration Prompt

To display the PPP config> prompt:

1. Enter **list devices** at the Config> prompt to display a list of interfaces.
2. If you have not already done so, set the data link protocol on one of the serial interfaces to PPP by entering **set data-link ppp** at the Config> prompt. For example:

```
Config> set data-link ppp
Interface Number [0]? 2
```

3. Enter **network** followed by the number of the PPP interface. For example:

```
Config> network 2
PPP config>
```

Point-to-Point Configuration Commands

Table 46 summarizes the PPP configuration commands, and the rest of this section explains these commands. Enter the commands at the `PPP config>` prompt.

Table 46. Point-to-Point Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Disable	Disables data compression (CCP), DTR line handling, CHAP, PAP, ECP. Also disables SPAP authentication in Remote LAN Access Features images.
Enable	Enables data compression (CCP), DTR line handling, CHAP, PAP, ECP. Also enables SPAP authentication in Remote LAN Access Features images.
List	Lists all information related to the point-to-point interfaces protocols, parameters, and options.
Set	Sets physical line (HDLC) parameters, LCP parameters, generic NCP parameters, and various NCP-specific options.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Disable

Disables data compression, authentication protocols, multilink PPP, and the Lower DTR feature.

Syntax:

disable ccp
chap
enp
lower-dtr
mp
mppe
mschap
pap

ccp Disables the use of data compression on the interface. Refer to “Using the Data Compression Subsystem” in the *Using and Configuring Features* for more information.

chap Disables the use of the Challenge-Handshake Authentication Protocol. Refer to “Challenge-Handshake Authentication Protocol (CHAP)” on page 378 for more information.

ecp This allows the router not to force the use of ECP encryption on this interface. The interface will still accept and execute Encryption Control Protocol (ECP) if the peer is using ECP.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See the CONFIG process **load** command in *Access Integration Services Software User's Guide*.

lower-dtr
Determines the way the data terminal ready (DTR) signal is handled for leased serial-line interfaces that are disabled. If this parameter is set to "disabled" (the default) and the interface is disabled, the DTR signal is not dropped.

mp Disables the Multilink Protocol (MP) on this interface. See "Chapter 29. Using the Multilink PPP Protocol" on page 431 for more information.

Example:

```
disable mp
Disabled as a MP link
```

mppe Disables Microsoft Point-to-Point Encryption (MPPE) on this interface.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See "Load" on page 95.

mschap
Disables MS-CHAP authentication on this interface. Disabling MS-CHAP has two effects upon MPPE, depending upon whether MPPE is configured as mandatory or optional. If MPPE is mandatory, disabling MS-CHAP brings down the link. If MPPE is optional, disabling MS-CHAP disables MPPE over the link. See "Microsoft PPP CHAP Authentication (MS-CHAP)" on page 379 for more information.

pap Disables the use of the Password Authentication Protocol. Refer to "Password Authentication Protocol (PAP)" on page 378 for more information.

spap Disables the use of the Shiva Password Authentication Protocol (SPAP).

Note: SPAP is only available on interfaces that have IBM DIALs Dial-In circuits configured.

Enable

Enables data compression, encryption, authentication protocols, lower-DTR, and the multilink PPP protocol on this PPP interface. If multiple authentication protocols are enabled, the device attempts to use them in the following priority order:

1. MS-CHAP
2. CHAP
3. PAP

Syntax:

enable ccp
chap
ecp
lower-dtr

mp

mppe

mschap

pap

ccp Enables the use of data compression on the interface.

chap Enables the use of the Challenge-Handshake Authentication Protocol. You are prompted for a rechallenge interval. Specify 0 if you do not want to rechallenge periodically after the initial authentication phase is complete. Refer to “Challenge-Handshake Authentication Protocol (CHAP)” on page 378 for more information.

Example:

```
enable chap
Rechallenge Interval in seconds (0=NONE)  [0] 10
CHAP enabled
```

ecp Enables the use of data encryption on this interface by negotiating Encryption Control Protocol (ECP). Once this is done, all PPP users with encryption enabled and with a valid encryption key must use ECP to connect to this port unless MS-CHAP is the active authentication protocol for the link. If the authentication protocol is MS-CHAP, ECP cannot be used; encryption must be accomplished using MPPE. PPP users without encryption enabled will still be able to connect to this interface.

When you enable ECP, you are prompted to enter the ECP encryption key for the local router. You must also provide the encryption key for the remote user when you use the talk 6 **add ppp-user** command at the `Config>` prompt to configure the remote user. MPPE does not require you to configure an encryption key on either the local or the remote user.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95.

lower-dtr

Determines the way the data terminal ready (DTR) signal is handled for leased serial-line interfaces that are disabled. If this parameter is set to “disabled” (the default) and the interface is disabled, the DTR signal is not dropped.

If Lower DTR is set to “enabled”, then the DTR signal will be dropped when the interface is disabled. This behavior may be desirable in situations where the interface has been configured as an alternate link for WAN Reroute and the interface is connected to a dial-out modem which maintains its dial connection based on the state of the DTR signal.

When the interface is disabled, the DTR signal is low and the modem keeps the dial connection down. When the interface is enabled, due to a WAN Reroute backup scenario, DTR is raised and the modem dials a stored number to the backup site. When the primary interface is restored, the alternate interface is disabled, DTR is lowered, and the modem hangs up the dial connection.

The following cable types are supported:

RS-232

V.35

V.36

Note: The **enable lower-dtr** command is not supported on PPP dial circuit interfaces.

mp Enables the Multilink Protocol (MP) on this interface. See “Chapter 29. Using the Multilink PPP Protocol” on page 431 for more information.

Example:

```
enable mp
Enabled as a MP link
Is this link a dedicated MP link? [no] yes
MP interface for this MP link? [0] 3
```

mppe *[mandatory/optional] [stateless/stateful]*
Enables Microsoft Point-to-Point Encryption (MPPE). If MS-CHAP is not enabled on the interface, then MPPE cannot be enabled on that interface. See “Microsoft Point-to-Point Encryption (MPPE)” in the chapter “Overview of Encryption” in *Using and Configuring Features* for more information.

mandatory
The client and the server must negotiate MPPE or the link will drop.

optional
The client will attempt to negotiate MPPE, but if the negotiation fails, the PPP link will remain active.

stateless
Session keys will be regenerated after transmitting each packet. This function is currently not supported by Microsoft Dial-Up Networking (DUN) clients.

stateful
Session keys will be regenerated after transmitting every 256 packets.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95.

mschap
Enables MS-CHAP authentication. When you enable MS-CHAP, you are prompted to provide the authenticator rechallenge interval. This value in seconds defines the length of time that will pass before the authenticator sends another challenge to the receiver of the authentication request to reconfirm the authentication. The value 0 indicates that no further challenges will be sent after the initial authentication.

Use the **set name** command to configure the name of the 2212 if the peer router is configured to authenticate the 2212's local name.

Note that MS-CHAP cannot be enabled if an external authentication server, as described in the chapter “Using Local or Remote Authentication” in *Using and Configuring Features*, has been configured. See “Microsoft PPP CHAP Authentication (MS-CHAP)” on page 379 for more information.

pap Enables the use of the Password Authentication Protocol. Refer to “Password Authentication Protocol (PAP)” on page 378 for more information.

List

Use the **list** command to display information related to the PPP interface and its protocol parameters and options.

Syntax:

list all
bcp
ccp
ecp
hdlc
ipcp
ipv6cp
lcp
ncp

all Lists all options and parameters related to the PPP interface.

The **list all** command displays the output of *all* the individual **list...** parameters described below.

bcp Lists the Bridging Network control protocol options.

Example:

```
list bcp
BCP Options
------------
Tinygram Compression:DISABLED
```

Tinygram Compression:
Displays whether Tinygram Compression is enabled/disabled.

ccp Displays the currently selected data compression options if data compression has been enabled. For additional information, see "Using the Data Compression Subsystem" in *Using and Configuring Features* .

If Microsoft Point-to-Point Encryption (MPPE) and data compression are both enabled, the type of data compression is MPPC.

ecp Displays the current Encryption Control Protocol state.

Example:

```
list ecp
 ECP Options
 -----------
 Data Encryption enabled
 Algorithm list: DESE-CBC
 DESE (Data Encryption Standard Encryption Protocol)
```

Note: Encryption support is optional and must be added to your software load using the **load add** command. See "Load" on page 95.

Data Encryption Enabled/Disabled
Indicates whether data encryption is enabled or disabled on interface.

Algorithm List
Displays the supported encryption algorithms. DES, as described by RFC 1969, is the only encryption algorithm currently supported.

hdlc Lists parameters related to the High-Level Data Link Control (HDLC) protocol. On PPP dial circuit interfaces, the "list hdlc" option is not available. For dial circuits, hardware data link parameters are a function of the base net rather than the PPP dial circuit. For additional information, see "Chapter 42. Configuring and Monitoring Dial Circuits" on page 563.

Example:

```
list hdlc
Encoding: NRZ
Idle State: Flag
Clocking:  Internal
Cable type:  V.35 DCE
Speed (bps): 6400

Transmit Delay Counter:  0
Lower DTR:  Disabled
```

Encoding:
HDLC transmission encoding scheme, either NRZ (non-return to zero) or NRZI (non-return to zero inverted).

Idle State:
Bit pattern, either Flag or Mark, transmitted on the point-to-point link when the interface is not transmitting data.

Clocking:
Interface clocking, either external or internal.

Cable type:
Specifies the type of cable in use (RS-232, V.35, or V.36).

Speed (bps):
The physical data rate of the interface. When clocking is internal, this is the data rate generated by the internal clock.

Transmit Delay Counter:
Number of flags sent between frames.

Lower DTR:
Enabled or Disabled. If Lower DTR is enabled, the router drops the DTR signal when a WAN Reroute alternate link is no longer needed. Dropping the DTR signal causes the modem to terminate the leased-line connection for the alternate link.

Notes:

1. The **list hdlc** command is not supported on PPP dial circuit interfaces.
2. This command displays the Lower DTR state only if Lower DTR is supported for the configured cable type.

ipcp Lists the Internet Protocol control protocol options.

Example:

```
list ipcp
IPCP Options
------------
IPCP Compression:                None
Send Our IP Address:              Yes
Remote IP Address to Offer if Requested: 10.0.0.3
```

IPCP compression
Indicates whether the PPP handler accepts compressed IP headers. PPP supports Van Jacobson TCP/IP header compression (RFC 1144). Enable this option when the point-to-point link is running at a low baud rate.

A value of “Van Jacobson” indicates that header compression is supported. A value of “NONE” indicates that compressed headers are not being accepted.

Send Our IP Address
Indicates whether IPCP is configured to send the local IP address for this PPP interface to the remote end of the link in our initial “Configure Request”. Some PPP implementations require this information.

ipv6cp

Lists the Internet Protocol version 6 control protocol options.

Example:

```
list ipv6cp
IPv6CP Options
------------
Send Our IP Address:              Yes
```

Send Our IP Address

Indicates whether IPv6CP is configured to send the local IP address for this PPP interface to the remote end of the link in our initial "Configure Request". Some PPP implementations require this information.

lcp Lists the parameters and options for the Link Control Protocol.

Example:

PPP 7 Config>list lcp

```
LCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:                  10
Terminate Tries:                    10   Retry Timer:                     3000

LCP Options
-----------
Max Receive Unit:                 1522   Magic Number:                      Yes
Peer to Local (RX) ACCM:         A0000
Protocol Field Comp(PFC):           No   Addr/Cntl Field Comp(ACFC):         No

Authentication Options
----------------------
Authenticate remote using:   none
Identify self as:            ibm
```

Link Control Protocol includes the authentication protocols used to authenticate the remote peer. If the authentication protocol is either CHAP or Microsoft PPP CHAP (MS-CHAP), the rechallenge interval is displayed.

Example:

PPP 7 Config>list lcp

```
LCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:                  10
Terminate Tries:                    10   Retry Timer:                     3000

LCP Options
-----------
Max Receive Unit:                 1522   Magic Number:                      Yes
Peer to Local (RX) ACCM:         A0000
Protocol Field Comp(PFC):           No   Addr/Cntl Field Comp(ACFC):         No

Authentication Options
----------------------
Authenticate remote using:   MSCHAP or SPAP or CHAP or PAP  [Listed in priority order]
CHAP Rechallenge Interval:   0
MSCHAP Rechallenge Interval: 0
Identify self as:            ibm
```

Config Request Tries:

Number of times that LCP sends configure-request packets to a peer station while attempting to open a PPP link.

Config Nak Tries:
Number of times that LCP sends configure-nak ("not acknowledged") packets to a peer station while attempting to open a PPP link.

Terminate Tries:
Number of times that LCP sends terminate-request packets to a peer station to close a PPP link.

Retry Timer:
Number of milliseconds that elapse before packet transmission continues according to the number of times set by the "Config tries" parameter.

Max Receive Unit:
Displays the maximum information field (packet) size handled by the link.

Peer to Local (Rx) ACCM
Displays the characters that the peer must "escape" when transmitting packets to the router on asynchronous lines.

Magic Number:
Indicates whether the magic number loopback detection option is enabled.

Protocol Field Comp (PFC):
Indicates whether the PFC option is enabled.

Addr/Cntl Field Comp(ACFC):
Indicates whether ACFC is enabled.

Authenticate remote using:
A list of enabled authentication protocols.

Identify Self As:
The name set with the **set name** command.

ncp Lists the parameters for all Network Control Protocols.

Example:

```
list ncp
NCP Parameters
---------------
Config Request Tries:        20   Config Nak Tries:         10
Terminate Tries:             10   Retry Timer:              3000
```

Config Request Tries:
Number of times NCP sends configure-request packets to a peer station while attempting to open a PPP link.

Terminate Tries:
While awaiting a Terminate-Ack, the number of times NCP sends Terminate-Request before it closes a PPP link.

Config Nak Tries:
Number of times NCP sends configure-nak (not acknowledged) packets to a peer station while attempting to open a PPP link.

Retry Timer:
Number of milliseconds that elapse before timing out of NCP's transmission of configure-request packets (to open the link) and terminate-request packets (to close the link).

LLC

Use the **LLC** command to access the LLC configuration environment (available only if APPN is included in the software load). See “LLC Configuration Commands” on page 217 for an explanation of each of these commands.

Syntax:

llc

Set

Use the **set** command to set HDLC parameters, LCP options and parameters, IPCP options, BCP options, and NCP parameters. “Parameters” are related to internal operations for such things as retry counts. “Options” are things that are negotiated with the other end.

Notes:

1. Values immediately following the command option prompts reflect the current setting of that option. They are not always the default values illustrated in this chapter.
2. The **set hdlc** commands are not supported on PPP dial circuit interfaces.

Syntax:

set
- bcp
- ccp options
- ccp algorithms
- hdlc...
- ipcp
- ipv6cp
- lcp...
- name...
- ncp...

bcp Sets the Bridging Control Protocol (BCP) parameters.

Example:

```
set bcp
TINYGRAM COMPRESSION  [no]:
```

Tinygram Compression
Specifies whether or not Tinygram Compression is used. This option is useful for protocols that are prone to problems when bridged over low-speed (64 Kbps and below) lines. These protocols add zeroes between the data and the frame checksum to pad the Protocol Data Unit (PDU) to the minimum size. Tinygram compression removes the zeroes and preserves the frame checksum at the transmitting end. At the receiving end, it restores the packet to the minimum length.

ccp options
Prompts you for the configurable options of the compression algorithms. Some of the options may be modified later by PPP negotiations with the

peer router on the WAN link. For additional information, see “Using the Data Compression Subsystem” in *Using and Configuring Features* .

Example:

```
set ccp options
STAC: # histories [1]?
STAC: check mode (0=none, 1-LCB, 2=CRC, 3=Seq) [3]?
```

STAC: # histories

This sets the number of compression “contexts” or “histories” that are used by the STAC compression engine.

A nonzero value means that the compression engine maintains the specified number of histories where it keeps information about previous data sent in packets. This historical data is used to improve the effectiveness of the compression.

The receiver maintains a similar history and as long as the transmitter and receiver keep their histories in sync, the receiver can properly decompress the packets it receives. If the histories get out of sync, packets are discarded as unusable data. Normally, you should set the number of histories to 1 unless the link quality is very poor.

A value of zero means that each packet sent is compressed without regard to any past packets sent and may always be reliably decompressed by the receiver. However, because the compressor cannot exploit any information derived from examining prior packets, the effectiveness of the compression usually is not as good.

Some implementations support more than one history, subdividing the data stream into separate streams that are compressed independently. The router does not support the use of more than one history on a PPP link.

STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq)

STAC compressed datagrams normally include a check value used by the two ends of the link to recognize when a compressed packet has been lost or corrupted, and some action is needed to re-synchronize the sender’s and receiver’s histories.

Note: Failure to detect a bad packet can cause all subsequent data to be decompressed incorrectly.

This option sets the exact form of check value used. Choose one of the following:

0 None: No check value is used. Without a check value, there is no way to determine that a packet has been lost, out-of-sequence, or corrupted. Do not use this mode unless the underlying data link provides reliable, sequenced packet delivery.

1 LCB: A “Longitudinal Control Byte” is used. This is a simple, 8-bit exclusive–OR checksum. *Its usage is strongly discouraged* because the receiver cannot detect a lost or an out-of-sequence packet, and the PPP frame checksum is a more reliable test of the packet’s integrity.

2 CRC: A 16-bit cyclic redundancy checksum is used. Although this is a better test of a packet’s integrity than the

LCB, its use is still discouraged because the receiver still cannot use it to detect lost or out of sequence packets, and otherwise it becomes largely redundant with the frame checksum.

3 SEQ: An 8-bit sequence number is used (default). This is the preferred method of operation. If the number of histories is not 0, use of any other mode is strongly discouraged though another mode may be necessary for interoperability with certain non-RFC-compliant routers.

4 EXT: An extended mode that is similar to the sequence number mode, in that each packet includes a sequence number, but the compressed frame format is altered more radically. In extended mode, re-synchronization with a peer is performed differently than with the other modes; the signaling between the two nodes is based upon flags passed in the headers of compressed datagrams rather than distinct CCP control packets.

Extended mode is provided for compatibility with certain non- RFC-compliant implementations. It should be used only with clients that do not support mode 3.

ccp algorithms ***list-of-algorithms***

Specifies an exact list of compression protocols to use. The order of preference depends on the order of entry in the list. When MPPE is activated on the link, the order of the CCP algorithms is ignored and only Microsoft Point-to-Point Compression (MPPC) is used.

When the link negotiates compression with another node, it offers the entire list of protocols to the peer node in preference order. The peer node should select the first protocol it can use from the preference list. Enabling multiple protocols allows the peer to dictate which compression algorithm will be used on the link. If you need to avoid an algorithm, do not specify the algorithm in the list.

Specifying **none** disables the use of any protocol effectively disabling compression. The valid compression algorithms are:

STAC-LZS
The STAC-LZS algorithm as described in RFC 1974

MPPC The Microsoft Point-to-Point Compression algorithm as described in RFC 2118.

Example:

```
set ccp protocols
Enter a prioritized list of enabled compressors
(first is preferred), all on one single line.
Choices (can be abbreviated) are:
Stac-LZS, MPPC
Compressor list [Stac-LZS:]?
```

hdlc cable *cable type*

Set the HDLC cable type (that is connected to the interface) to one of the following types:

RS-232 DTE

RS-232 DCE

V35 DTE

V35 DCE

V36 DTE
X21 DTE
X21 DCE

Example: `set hdlc cable rs-232 dce`

A DTE cable is used when you are attaching the router to some type of DCE device (for example, a modem or a DSU/CSU).

A DCE cable is used when the router is acting as the DCE and providing the clocking for direct attachment.

hdlc clocking *external* **or** *internal*
To connect to a modem or DSU, configure clocking as external. To connect directly to another DTE device, use a DCE cable and set the clocking to "internal" at one end and to "external" at the other.

Configure the clock speed at the end using internal clocking.

Example: `set hdlc clocking internal`

hdlc encoding *NRZ* **or** *NRZI*
Sets the HDLC transmission encoding scheme for an interface. Encoding may be set for NRZ (non-return to zero) or NRZI (non-return to zero inverted). NRZ is the more widely used encoding scheme while NRZI is used in some IBM configurations. The default value is NRZ.

Example: `set hdlc encoding nrz`

hdlc idle *flag* **or** *mark*
Sets the data link idle state to either Flag or Mark.

The flag option provides continuous flags (7E hex) between frames.

The mark option puts the line in a marking state (OFF, 1) between frames.

Example: `set hdlc idle flag`

hdlc speed *value*
For internal clocking, this command specifies the speed of the transmit and receive clock lines. The range is 2400 to 2 048 000 bps.

For external clocking, this command does not affect the hardware but it sets the speed of some protocols, such as IPX, used to determine the routing parameters. In these cases, set the speed to match the actual line speed. If speed is not configured or is set to 0, the protocol assumes a speed of 1 000 000 bps. The maximum speed that can be configured if external clocking is used can be 6 312 000 bps.

- interface 1.
- port 1 of a 4-port WAN concentration adapter.
- ports 1 and 5 of an 8-port WAN concentration adapter.

If you want to use a line speed greater than 2048000, you can only do this on port 1 of the system card's integrated WAN ports and all other integrated WAN ports must be clocked at 64 Kbps or less.

Example: `set hdlc speed 56000`

hdlc transmit-delay *value*

Sets the number of flags sent between frames. The purpose of this command is to slow the serial line so that it is compatible with older, slower serial devices at the other end.

The range is 0 to 15. The default is 0.

Example: `set hdlc transmit-delay 15`

ipcp Sets all Internet Protocol Control Protocol options for that link.

Example:

```
set ipcp
IP COMPRESSION [yes]:
Number of Slots:   [16]?
Send our IP address [yes]:
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0 for none) [0.0.0.0]? 10.0.0.3
```

IPCP compression

Selects whether or not the PPP handler will accept compressed IP data. PPP supports Van Jacobson (VJ) TCP/IP header compression as described in RFC 1144. You should enable this option when the point-to-point link is running at a low baud rate.

Setting this value to **yes** enables the compression option. Setting this value to **no** disables the option. The default setting is **no**.

Slots Sets the number IP headers that are saved for referential purposes when determining the type of compression that is enabled. The range is 1 to 16. The default is 16.

Send Our IP address

Specifies whether or not to send the local IP address to the remote end of the link. You should set this option to **yes** if the other end of the link requires the IP address.

If this value is set to **yes**, IPCP will send the IP address of the PPP interface, if the interface is configured with a numbered IP address, (that is, the address does not begin with 0). If this option is set to **no** and the peer sends us a Configure NAK with 0.0.0.0 for the IP Address option, the 2212 will respond with the address of the PPP interface if it is configured with a numbered address.

ipv6cp

Sets the IPv6 Control Protocol option for the link.

Example:

```
set ipv6cp
Send Our IP address [no]:
```

Send Our IP address

Specifies whether or not to send the local IPv6 address to the remote end of the link. Set this option to **yes** if the other end of the link requires the IPv6 address.

If this parameter is set to **yes**, IPv6CP will send the IPv6 address of the PPP interface, if the interface is configured with a numbered IPv6 address, (that is, the address does not begin with 0). If this option is set to **no** and the peer sends us a Configure NAK with ::/0 for the IPv6 address option, the 2212 will respond with the address of the PPP interface if it is configured with a numbered address.

lcp *options* **or** *parameters*

Sets the Link Control Protocol options and parameters for the PPP link.

Example:

```
set lcp options
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000] ?
Protocol Field Compression (PFC) [no]?
Addr/Cntl Field Compression (ACFC) [no]?
```

Maximum receive unit

Sets the maximum size of the information field that are transferred in a single datagram. The range is 576 to 4089 bytes. The default is 2048.

Magic number

Specifies whether or not the magic number option is enabled. The magic number provides a way of detecting looped back links in serial line configurations. When this option is enabled, the link uses the system clock as a random number generator. The random numbers that are generated are referred to as magic numbers.

When the LCP receives a Configure Request with a magic number present (i.e., the magic number option is enabled), the received magic number is compared with the magic number in the last Configure-Request sent to the peer. If the two magic numbers are different, the link is not considered looped back. If the two numbers are the same, the PPP handler attempts to bring the link down and up again to renegotiate magic numbers.

Setting this value to Yes enables the magic number option. Setting this value to No disables the option. The default setting is Yes.

Async Control Character Map

Indicates which characters that the peer must “escape” when transmitting packets to the router on asynchronous lines. This allows certain sensitive ASCII control characters, such as XON and XOFF, to be transmitted transparently over the link.

Specify a 32-bit bit mask in hexadecimal. If a bit in position ’N’ of the mask is set, the corresponding ASCII character ’N’ must be escaped (the LSB is bit number 0, corresponding to the ASCII NUL character).

The default value for this option is ’0A0000’, indicating that XON and XOFF (control-Q and control-S) need to be escaped. This is for the benefit of modems that use XON/XOFF to perform software handshaking. If this is not an issue, then it is recommended that you change the ACCM to zero (no characters escaped).

LCP is always willing to negotiate the ACCM, even on synchronous lines, and the **list lcp** command in the PPP monitoring process will display the negotiated value. However, synchronous lines employ a “bit-stuffing” mechanism rather than an “escaping” mechanism, so the ACCM is not normally meaningful on synchronous lines. It may be meaningful if the router is connected to a modem that performs sync-to-async conversion, in which case its value should reflect the requirements of the attached modem on the asynchronous side.

Addr/Cntl Field Compression (ACFC)

Specifies whether the peer can employ address and control field compression.

If the ACFC option is successfully negotiated by LCP, it means that the Address and Control field bytes which start off each packet may be omitted in the datagrams sent back and forth on the link. These bytes are always 0xFF 03, so there is no real information provided by them, and enabling ACFC means that the datagrams that are transmitted will be two bytes shorter.

To be precise, if you enable ACFC, you are indicating a receive-side capability. If you enable ACFC and LCP successfully negotiates it, the other end can employ ACFC in the packets it transmits to the local end (most PPP options work like this). The local end will only transmit packets *without* the address and control fields if the other end also indicates its ability to handle such packets.

Enabling ACFC does not obligate the other end to send packets without the address and control fields, even if it accepts the option. Enabling ACFC merely tells the peer that it optionally *may* use ACFC, and the router will be able to handle the incoming packets. If the peer indicates that it can handle ACFC, then the router always performs ACFC on the packets it transmits regardless of whether ACFC is enabled locally.

LCP packets always are sent with address and control fields present. This guarantees that LCP packets will be recognized even if there is a loss of link synchronization.

Protocol Field Compression (PFC)

Specifies whether the peer is to employ protocol field compression.

When you specify “yes”, if the PFC option is negotiated successfully by LCP, the leading zero byte may be omitted from the “Protocol” field for those protocol values in the range ’0x0000’–’0x00FF’, for a one byte savings in the packets being transmitted. This range includes the majority of layer-3 protocol datagrams.

PPP protocol values are all assigned such that the upper byte of the protocol is an even value and the lower byte is an odd value (a limited use of the more generalized mechanism described by the ISO 3309 extension mechanism for address fields). Thus, the receiver can readily detect when the leading byte of a protocol value has been omitted (the first byte of the protocol field is odd rather than even), so there is no ambiguity interpreting frames in the presence of PFC.

PFC, like ACFC, is a receive side capability and the previous description of ACFC applies to PFC.

Example:

```
set lcp parameters
Config tries  [20]?
NAK tries  [10]?
Terminate tries  [10]?
Retry timer (mSec)  [3000]?
```

Note: The value immediately following the command option prompt is the current setting of that option. It is not always the default value illustrated in this chapter.

Retry timer

Sets the amount of time in milliseconds that elapses before LCP’s transmission of configure-request (to open the link) and

terminate-request (to close the link) packets is timed out. Expiration of this timer causes a timeout and the halting of configure-request and terminate-request packet transmission. The range is 200 to 30000 milliseconds. The default setting is 3000 milliseconds.

Config tries
Sets the number of times that LCP sends configure-request packets to a peer station to establish the opening of a PPP link. The default value is 20. The range is 1 to 100.

The retry timer starts after the first configure-request packet is transmitted. This is done to guard against packet loss.

NAK tries
Sets the number of times that LCP sends configure-nak (nak = not acknowledged) packets to a peer station while attempting to open a PPP link. The default value is 10. The range is 1 to 100.

LCP sends configure-nak packets upon receiving configure-request packets with some unacceptable configuration options. These packets are sent to refuse the offered configuration options and to suggest modified, acceptable values.

Terminate tries
Sets the number of times that LCP sends terminate-request packets to a peer station to close a PPP link. The default value is 10. The range is 1 to 100.

The retry timer starts after the first terminate-request packet is transmitted. This is done to guard against packet loss.

name Sets the name that the router uses when responding to authentication requests from another router.

Notes:

1. While the “case” that you use for names and passwords sent to the peer on the link are preserved for this product, interoperability with other vendor products is easier if all names and passwords are entered in *lowercase.*
2. Other implementations may not handle names with the same maximum length as supported in this product. The only indication is a message from the authenticator stating that there is a bad name. If you receive this type of message, try shortening the routerid.
3. This command sets the name of the local router. Use the talk 6 **add ppp-user** command at the `Config>` prompt to add each remote user to the local data base, if you want to use the local data base to track the remote users. The alternative is to configure the external AAA authentication server that is described in the chapter “Using Local or Remote Authentication” in *Using and Configuring Features* .

   Note: The external AAA authentication server cannot be used by MS-CHAP.

Example:

```
set name
PPP 7 Config>set name
Enter Local Name:  [ ]? newyork
Password:
Enter password again:
PPP Local Name = newyork
```

ncp parameters

Sets the basic operational parameters for most NCPs.

Note: Although you access this command through a particular interface, this command will reset the parameters for all PPP interfaces.

Example:

```
set ncp parameters
Config tries  [20]
NAK tries  [10]?
Terminate tries  [10]?
Retry timer (mSec)  [3000]?
```

Config tries

Sets the number of configure-request packets sent by NCP to a peer station to attempt to open a PPP link. The range is 1 to 100. The default is 20.

This action indicates the desire to open an NCP connection with a specified set of configuration options. The retry timer starts after a configure-request packet is transmitted. This is done to guard against packet loss.

NAK tries

Sets the number of configure-nak (nak = not acknowledged) packets that NCP sends to a peer station while attempting to open a PPP link. The range is 1 to 100. The default value is 10.

Upon receiving configure-request packets with some unacceptable configuration options, NCP sends configure-nak packets. These packets are sent to refuse the offered configuration options and to suggest modified, acceptable values.

Terminate tries

Sets the number of terminate-request packets sent by NCP to a peer station to close a PPP link. The range is 1 to 100. The default value is 10.

This action indicates the desire to close an NCP connection. The retry timer is started after a terminate-request packet is transmitted. This is done to guard against packet loss.

Retry timer

Sets the amount of time, in milliseconds, that elapses before NCP's transmission of configure-request (to open the link) and terminate-request (to close the link) packets is timed out. Expiration of this timer causes a timeout and the halting of configure-request and terminate-request packet transmission. The range is 200 to 30000 milliseconds. The default is 3000 milliseconds.

Accessing the Interface Monitoring Process

To access the PPP interface monitoring process, do the following:

1. Enter **interface** at the + prompt to display a list of configured interfaces.
2. Enter **network** followed by the number of the PPP interface.

```
+ network 2
PPP>
```

Point-to-Point Monitoring Commands

This section summarizes and then explains the Point-to-Point monitoring commands. Enter the commands at the PPP> prompt. Table 47 shows the commands.

Note: The options available for these commands depend on what protocols are available in the router software. For example, when the router software (image) does not contain APPN support, the **list isrcp**, **list isr**, **list hprcp**, **list hpr**, and **llc** commands are not available.

Table 47. Point-to-Point Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Clear	Clears all statistics from point-to-point interfaces.
List	Displays information and counters related to the point-to-point interface and PPP parameters and options.
LLC	Displays the LLC monitoring prompt.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Clear

Use the **clear** command to clear all statistics from point-to-point interfaces.

Syntax:

clear

List

Use the **list** command to display information and counters related to the point-to-point interface and PPP parameters and options.

Syntax:

list all
cbcp callback cp
control
errors
interface
lcp - PPP link CP
pap - PAP Authentication CP
chap - CHAP Authentication CP
mschap - MS-CHAP Authentication CP
ecp - Encryption Control Protocol
edp- Encrypted packet statistics
mppe - Microsoft PPP Encryption (MPPE)

spap - SPAP Authentication CP

ccp - PPP Compression CP

cdp - PPP compression

compression - PPP compression

bcp - Bridging (ASRT) CP

brg - Bridging (ASRT)

stp - Spanning Tree Protocol

nbcp - NetBios

nbfcp - NetBios Frame

ipcp - Internet Protocol CP

ip - Internet Protocol

ipv6cp - Internet Protocol version 6 CP

ipv6 - Internet Protocol version 6

ipxcp - Novell IPX CP

ipx - Novell IPX

atcp - AppleTalk (Phase 2) CP

ap2 - AppleTalk (Phase 2)

dncp - DECnet IV CP

dn - DECnet IV

osicp - ISO's OSI CP

osi - ISO's OSI

bvcp - Banyan VINES CP

vines - Banyan VINES

isrcp - APPN ISR CP

isr - APPN ISR

hprcp - APPN HPR CP

hpr - APPN HPR

all Lists all information and counters related to the point-to-point interface and PPP options and parameters. The output displayed for this command is a combination of the displays from all of the individual **list** *item* commands.

Note: If a network control protocol is not available on an interface, a message is displayed indicating that no protocol or statistics information is available for that network control protocol's list commands.

cbcp Lists statistics for the Callback Control protocol.

Example: list cbcp

```
CBCP Statistics          In          Out
---------------          ---         -----
Packets:                  0           0
Octets:                   0           0
Callback attempts:        0
Successful callbacks:     0
```

Packets
Indicates the total number of CBCP packets transmitted (out) and received (in) over the current point-to-point interface.

Octets
For CBCP frames, indicates the total number of bytes in Octets transmitted and received over the current point-to-point interface.

Callback attempts
The number of CBCP callbacks attempted, including those in progress.

Successful callbacks
The number of successful callbacks completed.

control
Lists negotiated options or other state information for a control protocol.

ccp
ecp
lcp
bcp
nbcp
nbfcp
ipcp
ipxcp
atcp
dncp
osicp
bvcp
isrcp
hprcp

Examples of the List Control CCP Command

Example for STAC-LZC compression:

```
list control ccp
CCP State:                Open
Previous State:           Ack Sent
Time Since Change:        264 hours, 56 minutes and 58 seconds

Compressor:   STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ

Max size of compression dictionary:   12494.
Max size of decompression dictionary: 4424.
```

Example for MPPC compression:

```
list control ccp
CCP State        :        Open
Previous State   :        Listen
Time Since Change:        167 minutes

Compressor :   none
Decompressor : none

MPPE : Negotiated 40 bit stateful
```

Definitions of Terms in the List Control CCP Example

CCP state
The current state of the point-to-point link. If “Open”, then

compression was successfully negotiated on this link. If not open, compression is not running on the link. It will also show as “Open” if MPPE has been successfully negotiated.

Previous State
State of the point-to-point link before the state displayed in the current state field.

Compressor
Shows which compressor was negotiated and the options it is using.

Decompressor
Shows which decompressor was negotiated and the options it is using.

Max size of compression dictionary
The size of the data space allocated for the compression “context” or “history”.

Max size of decompression dictionary
The size of the data space allocated for the decompression “context” or “history”.

MPPE MPPE options negotiated. See the talk 6 **enable mppe** command for descriptions of these parameters and “Microsoft Point-to-Point Encryption (MPPE)” in the chapter “Overview of Encryption” in *Using and Configuring Features* for more information.

Example of the List Control ECP Command

Example:

```
PPP x>list control ecp

ECP State:                Open
Previous State:           Ack Sent
Time Since Change:        16 minutes and 40 seconds

Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

Definitions of Terms in the List Control ECP Example

ECP State:
The current state of the point-to-point link. If “Open” then encryption was successfully negotiated on this link. If not “Open”, encryption is not running on the link.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95 .

Previous State:
The state of the point-to-point link before the state displayed in the current state field.

Time Since Change:
The elapsed time between the above two state changes.

Local (transmit) encrypter:
This encryption algorithm is used for encrypting the data being sent on this PPP interface.

Remote (receive) encrypter:
The encryption algorithm is used for decrypting the received data on this interface.

Example of the List Control LCP Command

Example:

```
list control lcp

Version:                    1
            Link phase:                 Establishing connection (LCP)
            LCP State:                  Listen
            Previous State:             Req Sent
            Time Since Change:          1 minute and 57 seconds
            Remote Username:            - No Authentication -
            Last Identification Rx'd
            Time Connected:             - No Connection -

            LCP Option                  Local                       Remote
            ----------                  -----                       ------
            Max Receive Unit:           2048                        1500
            Async Char Mask:            FFFFFFFF                    FFFFFFFF
            Authentication:             None                        None
            Magic Number:               7A8CBFD7                    None
            Protocol Field Comp:        No                          No
            Addr/Cntl Field Comp:       No                          No
            32-Bit Checksum:            No                          No
```

Definitions of Terms in the List Control LCP Example

Version
Displays the current version of the Point-to-Point Protocol.

Link phase
Displays the current activity on the link. This can have one of the following values:

Dead There is no activity on the link; the interface is down.

LCP The link is in LCP negotiation. This state occurs when first bringing up an interface. The interface may be in self-test at this time.

Authenticate
The link is performing initial authentication.

ECP The link is negotiating an ECP encryption algorithm.

Note: Encryption support is optional and must be added to your software load using the **load add** command. See the CONFIG process **load** command in *Access Integration Services Software User's Guide*.

Ready Link is operating normally. NCPs can negotiate and data traffic associated with can flow after successful NCP negotiation.

Terminate
The link is being shut down.

LCP State
Displays the current state of the point-to-point link. These states include the following:

OPEN - Indicates that a connection has been made and data can be sent. The retry timer does not run in this state.

CLOSED - Indicates that the link is down and no attempt is being made to open it. In this state, all connection requests from peers are rejected.

LISTEN - Indicates that the link is down and no attempt is being made to open it. In contrast to the CLOSED state, however, all connection requests from peers are accepted.

REQUEST-SENT - Indicates that an active attempt is being made to open the link. A Configure-request packet has been sent but a Configure-Ack has not yet been received nor has one been sent. The retry timer is running at this time.

ACK-RECEIVED - Indicates that a Configure-request packet has been sent and a Configure-Ack packet has been received. The retry timer is still running since a Configure-Ack packet has not been transmitted.

ACK-SENT - Indicates that a Configure-Ack packet and a Configure-request packet have been sent but a Configure-Ack packet has not been received. The retry timer always runs in this state.

CLOSING - Indicates that an attempt is being made to close the connection. A Terminate-request packet has been sent but a Terminate-Ack packet has not been received. The retry timer is running in this state.

Previous State
Displays the state of the point-to-point link prior to the state displayed in the Current state field. These states are the same as those described in the Current state field.

Time since change
Displays the amount of time that has elapsed since the last link state change.

Remote Username
When authentication is required on the link, this field shows the name that the peer supplied.

Last Identification Rx'd
An optional packet type that is defined for LCP is an "Identification" packet. The contents of this packet are undefined but are normally expected to be a human-readable string provided by the peer to give some identifying information such as a name, manufacturer, model number, or other information the manufacturer wishes to provide. If the router receives such a packet, the contents of the last such packet received are displayed here.

Time Connected
Indicates how long the peer has been connected on this link.

LCP Option
These fields indicate the values of options that have been negotiated with the peer when LCP is in the Open state. When LCP is not open, these values represent initial defaults or configured values that will be used in subsequent LCP negotiations.

Max Receive Unit
Indicates the maximum length for the packet size that the local and remote ends can transmit. This is the maximum length of the payload portion of a PPP packet and it does not include PPP header and trailer bytes.

When LCP is in an Open state, the values indicate the lengths that have been negotiated with the peer. The router does not support differing MRU lengths for the peer and local end, so these values will be the same.

Async Character Mask
This indicates the asynchronous control character mask that has been negotiated. The router accepts ACCM negotiation even on synchronous lines, although this does not affect the actual packet data sent. See the **set lcp options** command on page 400 for more information about the ACCM.

Authentication
Indicates which authentication protocol, if any, each end of the link requires. Multiple protocols may be available at each end; this value indicates which protocol the units agreed to use.

Magic number
Displays the current magic number being used for both the local and remote ends of the link for loopback detection.

Protocol compression
Indicates whether PFC has been negotiated.

Address/Control compression
Indicates whether ACFC has been negotiated.

32-bit checksum
Not currently supported. PPP will reject this option if it is received.

Example of the List Control BCP Command

Example:

```
list control bcp
BCP State:            Closed
Previous State:        Closed
Time Since Change:     5 hours, 25 minutes and 3 seconds

BCP Option             Local                    Remote
Tinygram Compression   DISABLED                 DISABLED
Source-route Info:
Remote side does not support source-route bridging
```

Definitions of Terms in the List Control BCP Example

The BCP State fields are the same as those described under the **list control lcp** command.

Tinygram Compression
Displays whether or not Tinygram Compression is enabled or disabled on the local and remote ends of the link.

Source-route Info
Displays whether or not source route bridging is enabled for the local and remote ports that correspond to this interface.

Example of the List Control NBCP CommandDefinitions of Terms in the List Control NBCP ExampleExample of the List Control NBFCP Command

Example:

```
list control nbfcp
NBFCP State:              Closed
Previous State:           Closed
Time Since Change:        4 hours, 5 minutes and 58 seconds

NetBIOS Frame Control Protocol Info:
Local  MAC Address = 0x000000000000
Remote MAC Address = 0x444553540000
Remote NetBIOS Names: (0)

Remote Peer Class:        0
Remote Peer Version Major: 0
Remote Peer Version Minor: 0
```

Definitions of Terms in the List Control NBFCP Example

The NBFCP State fields are the same as those described under the **list control lcp** command.

Local MAC Address

The Local MAC Address is the MAC Address that is used by the Win 95/NT Dial-Up Networking client. It is a pseudo-random number, or a Locally Administered Address (LAA), if you configured an LAA in the client.

Remote MAC Address

The Remote MAC Address is the MAC Address that the 2212 DIALs Server has assigned to this client for use on the LAN.

Remote NetBIOS Name

The list of NetBIOS names of LAN resources to which the client has requested access.

Remote Peer

The Remote Peer Class, Version Major, and Version Minor is the information passed back to the 2212 by the NBFCP Peer Information option.

Example of the List Control IPCP Command

Example:

```
list control ipcp
IPCP State:               Listen
Previous State:           Closed
Time Since Change:        1 hour, 57 minutes and 52 seconds

IPCP Option               Local               Remote
-----------               -----               ------
IP Address                0.0.0.0             10.0.0.152
Compression Slots         None                None

DHCP State:               BOUND
Lease Server:             10.0.0.111
Leased IP Address:        10.0.0.152
Lease Time:               4 minutes and 0 seconds
Renewal Time:             2 minutes and 0 seconds
Rebind Time:              3 minutes and 30 seconds
Lease Time Elapsed:       1 second
Lease Time Remaining:     3 minutes and 59 seconds

DHCP Client ID:           0100120B0000
```

Definitions of Terms in the List Control IPCP Example

The IPCP state fields are the same as those described under the **list control lcp** command.

IP Address:
Indicates if this interface's IP address (Local) and the negotiated address of the remote (Remote), if any.

Compression Slots
Indicates the number of IP headers saved for referential purposes when determining the type of compression that is enabled.

DHCP State
This is the Proxy DHCP as described in RFC 1541.

Lease Server
The server from which the lease was acquired.

Leased IP address
The address leased to the client. This address should be equivalent to the "Remote IP Address" listed above.

Lease Time
Length of lease from the DHCP server for this address. When "Lease Time Elapsed" equals this time, the lease will be expire and the IPCP connection closed.

Renewal Time
Time after which Proxy DHCP attempts to extend this lease from the server. When "Lease Elapsed Time" equals this time, Proxy DHCP attempts to renew the lease, resetting the "Lease Time," "Lease Elapsed Time," and "Lease Time Remaining," if successful.

Rebind Time
Time before Proxy DHCP attempts to obtain a new lease from any configured DHCP server. When "Lease Elapsed Time" equals this time, Proxy DHCP attempts to obtain a new lease, resetting the "Lease Time," "Lease Elapsed Time," and "Lease Time Remaining," if successful.

Leased Time Elapsed
Time elapsed for this lease. This is not necessarily the time for this particular dial-in session, as the lease may have been renewed. When the lease is renewed, this timer is set back to 0.

Leased Time Remaining
Time remaining for this lease. This parameter is equal to "Lease Time" minus "Lease Time Elapsed."

DHCP client ID
A unique ID for this client (dial-in user). All DHCP messages are identified to and from the DHCP server by this client ID.

Example of the List Control IPXCP Command

Example:

```
list control ipxcp
IPXCP State:           Closed
Previous State:        Closed
Time Since Change:     2 hours, 9 minutes and 9 seconds
```

The IPXCP state fields are the same as those described under the **list control lcp** command.**Example of the List Control ATCP Command**

Example:

```
list control atcp
ATCP State:            Closed
Previous State:        Closed
Time Since Change:     6 hours, 27 minutes and 7 seconds

AppleTalk Address Info:
Common network number = 12
Local node ID = 49
Remote node ID = 76
```

Definitions of Terms in the List Control ATCP Example

The ATCP State fields are the same as those described under the **list control lcp** command.

Common Network Number
Network number of the two ends of the point-to-point link. (You must statically configure both ends of the link to have the same network number.)

Local Node ID
Unique node number of the local end of the link.

Remote Node ID
Unique node number of the remote end of the link.

Example:

```
list control dncp
DNCP State:               Closed
Previous State:           Closed
Time Since Change:        2 hours, 2 minutes and 58 seconds
```

The DNCP state fields are the same as those described under the **list control lcp** command.

Example:

```
list control osicp
OSICP State:          Closed
Previous State:       Closed
Time Since Change:    6 hours, 28 minutes and 32 seconds
```

The OSICP State fields are the same as those described under the **list control lcp** command.**Example of the List Control BVPC Command**

Example:

```
list control bvcp
BVCP State:               Open
Previous State:           Ack Sent
Time Since Change:        403 hours, 49 minutes and 2 seconds
```

The BVCP State fields are the same as those described under the **list control lcp** command.

Note: The command word **bvcp** and the acronym BVCP stand for the Banyan VINES Control Protocol (BVCP).

Example of the List Control ISRCP Command

Example:

```
list control isrcp
APPN ISRCP State:         Open
Previous State:           Ack Rcvd
Time Since Change:        1 hour, 48 minutes and 5 seconds
```

The APPN ISR control protocol (ISRCP) state fields are the same as those described under the list control lcp command.**Example of the List Control HPRCP Command**

Example:

```
list control hprcp
APPN HPRCP State:          Open
Previous State:            Ack Rcvd
Time Since Change:         1 hour, 48 minutes and 10 seconds
```

The APPN HPR control protocol (HPRCP) state fields are the same as those described under the list control lcp command

error Lists information related to all error conditions tracked by the PPP software.

Example:

```
list error
Error Type                Count          Last One
----------                -----          --------
Bad Address:                 0                0
Bad Control:                 0                0
Unknown Protocol:            0                0
Invalid Protocol:            0                0
Config Timeouts:             0                0
Terminate Timeouts:          0                0
```

Bad address
Indicates the total number of bad addresses encountered over the point-to-point link. “Bad addresses” refers to the HDLC framing byte at the start of the packet.

Bad control
Indicates the total number of bad control packets encountered over the point-to-point link. “Bad control” refers to the 0x03 prefix on HDLC encapsulated PPP packets (“UI” value that follows the 0xFF).

Unknown protocol
Indicates the total number of unknown protocol packets encountered by the current link.

Invalid protocol
Indicates the total number of invalid protocol packets encountered by the current link.

Config timeouts
Indicates the total number of configuration timeouts experienced by the link.

Terminate timeouts
Indicates the total number of link termination timeouts experienced by the link.

interface
Lists PPP interface statistics.

Example:

```
list interface
Interface Statistic          In              Out
-------------------          --              ---
Packets:                      0               0
Octets:                       0               0
```

Packets
Indicates the number of packets received and transmitted on this interface.

Octets
Indicates the number of octets received and transmitted on this interface.

lcp Lists statistics for the Link Control Protocol.

Example:

```
list lcp
LCP STATISTIC        IN       OUT
-------------        --       ---
PACKETS:             42       42
OCTETS:              1260     1260
CFG REQ:             0        0
CFG ACK:             0        0
CFG NAK:             0        0
CFG REJ:             0        0
TERM REQ             0        0
TERM ACK             0        0
ECHO REQ:            21       21
ECHO RESP:           21       21
DISC REQ:            0        0
CODE REJ:            0        0
```

Packets
Indicates the total number of LCP packets transmitted (out) and received (in) over the current point-to-point interface.

Octets
For LCP frames, indicates the total number of bytes in octets transmitted and received over the current point-to-point interface.

CFG REQ
Indicates the total number of configure-request LCP packets transmitted and received over the current point-to-point interface.

CFG ACK
Indicates the total number of configure-ack (acknowledged) LCP packets transmitted and received over the current point-to-point interface.

CFG NAK
Indicates the total number of configure-nak (not acknowledged) LCP packets transmitted and received over the current point-to-point interface.

CFG REJ
Indicates the total number of configure-reject LCP packets transmitted and received over the current point-to-point interface.

TERM REQ
Total number of terminal request LCP packets transmitted and received over the current point-to-point interface.

TERM ACK
Total number of terminal ack LCP packets transmitted and received over the current point-to-point interface.

ECHO REQ
Indicates the total number of echo-request LCP packets transmitted and received over the current point-to-point interface.

ECHO RESP
Indicates the total number of echo-response LCP packets transmitted and received over the current point-to-point interface.

DISC REQ
Indicates the total number of discard-request LCP packets transmitted and received over the current point-to-point interface.

CODE REJ
Indicates the total number of code-reject LCP packets transmitted and received over the current point-to-point interface.

pap Lists statistics for the Password Authentication Protocol.

Example:

```
list pap
PAP Statistics            In                    Out
--------------            --                    ---
Packets:                  0                     0
Octets:                   0                     0
Requests:                 0                     0
Acks:                     0                     0
Naks:                     0                     0
```

Packets
The total number of PAP packets sent or received.

Octets
The number of bytes of data that were sent or received in those packets.

Requests
The number of PAP "Request" packets sent or received. These are the packets which contain the PAP name/password pairs.

Acks The number of Acks (success replies) sent or received for the PAP requests (for example, if the peer sends a valid Request packet, the router replies with an Ack).

Naks The number of Naks sent or received for the PAP requests (for example, if the peer sends an invalid Request packet, the router replies with a Nak).

chap Lists statistics for the Challenge-Handshake Authentication Protocol.

Example:

```
list chap
CHAP Statistics           In                    Out
---------------           --                    ---
Packets:                  0                     0
Octets:                   0                     0
Challenges:               0                     0
Responses:                0                     0
Successes:                0                     0
Failures:                 0                     0
```

Packets
The total number of CHAP packets sent or received.

Octets
The number of bytes of data that were sent or received in the packets.

Challenges
The number of CHAP "Challenge" packets sent or received. A CHAP Challenge packet includes a randomly generated encryption key and is a demand on the peer to generate a suitable response based on that key and on stored password information.

Responses
The number of CHAP "Response" packets sent or received. A Response packet contains a peer's answer to a "Challenge" request.

Successes/Failures
The number of Success or Failure packets sent or received. A unit sends out a Challenge packet and waits for the peer's Response reply. It then examines the Response packet and sends a Success or Failure packet to indicate whether the Response was valid.

These counters reflect the number of Success or Failure packets sent. A peer gets several tries to respond successfully before authentication is considered to have failed.

mschap
Lists MS-CHAP statistics for each direction.

Packets
Total number of MS-CHAP packets.

Octets
Total number of bytes contained in MS-CHAP packets.

Challenges
Number of MS-CHAP challenge packets.

Responses
Number of MS-CHAP response packets.

Successes
Number of MS-CHAP success packets.

Failures
Number of MS-CHAP failure packets.

Failure: Restricted Hours
Number of failure packets sent due to the PPP user's attempt to access the 2212 outside of that user's permitted hours. This counter is not supported and will always be 0.

Failure: Account Disabled
Number of failure packets sent because the PPP user's ID has been disabled at the 2212.

Failure: Password Expired
Number of failure packets sent because the PPP user's password has expired.

Failure: No Dialin Permission
Number of failure packets sent because the PPP user is not authorized to dial in to this 2212.

Failure: Authentication
Number of failure packets sent because the PPP user's credentials (ID or password) are not known to the 2212.

Failure: Change Password
Number of failure packets sent as a result of error encountered while processing the Change Password packet.

Change Password
Number of change password packets. The router will never send a change password packet; therefore, the outbound counter will always be 0.

ecp Lists statistics for ECP (encryption control protocol) packets sent or received on the interface.

Example:

```
PPP x>list ecp

ECP Statistic              In                      Out
-------------              --                      ---
Packets:                   2                       2
Octets:                    26                      26
Reset Reqs:                0                       0
Reset Acks:                0                       0
Prot Rejects:              0                       -
Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

Note: Encryption support is optional and must be added to your software load using the **load add** command. See "Load" on page 95.

Packets
Indicates the total number of ECP packets transmitted (out) and received (in) over the current point-to-point interface.

Octets
Indicates the total number of bytes transmitted and received in the ECP packets.

Reset Reqs
Indicates the number of Reset requests transmitted and received on this interface. A Reset Request will be sent whenever ECP discard an EDP packet.

Note: Because DES, the only supported encryption algorithm, does not send reset requests this number will be zero.

Reset Acks
Indicates the reset acknowledgments transmitted and received on this interface. A Reset Ack packet will be sent for every Reset Request packet received.

Note: Because DES, the only supported encryption algorithm, does not send any Reset Requests this number will be zero.

Prot Rejects
Indicates the total number of protocol reject packets transmitted and received over the current point-to-point interface.

Local (transmit) encrypter
This encryption algorithm will be used to encrypt the data being sent on this point-to-point interface.

Remote (receive) encrypter
This encryption algorithm will be used to decrypt the received data on this point-to-point interface.

edp Lists statistics associated with the ECP-encrypted packets being sent or received on the interface.

Example:

```
PPP x>list edp

Encryption Statistic       In                      Out
--------------------       --                      ---
Packets:                   20                      30
Octets:                    29164                   44790
Encrypted Octets:          29280                   44880
Discarded Packets:         0                       0
Prot Rejects:              0                       -
```

Note: Encryption support is optional and must be added to your software load using the **load add** command. See “Load” on page 95.

Packets
Indicates the total number of IP packets transmitted (out) and received (in) over the current point-to-point interface.

Octets
Indicates the total number of octets of data bytes transmitted and received over the current IP connection.

Encrypted Octets
Indicates the number of encrypted octets transmitted or received on this interface.

Discarded Packets
Indicates the number of packets that were discarded because they could not be successfully decrypted.

Prot Rejects
Indicates the total number of protocol reject packets transmitted and received over the current point-to-point interface.

mppe Displays encryption data statistics for Microsoft PPP Encryption (MPPE) configuration.

Example:

```
list mppe
MPPE Statistic          In                  Out
--------------          --                  ---
Encrypted Octets :      0                   0
Encrypted Packets :     0                   0
Discarded Packets :     0                   0
```

spap Lists statistics for the Shiva Password Authentication Protocol.

Example:

```
list spap
SPAP Statistic            In                      Out
--------------            --                      ---
Packets:                  0                       0
Octets:                   0                       0
Requests:                 0                       0
Acks:                     0                       0
Naks:                     0                       0
Dialbacks:                0                       0
PleaseAuthenticates:      0                       0
Change Passwords:         0                       0
Alerts:                   0                       0
MCCP Call Reqs            0                       0
MCCP Callbacks            0                       0
MCCP ACKs                 0                       0
MCCP NAKs                 0                       0
```

Packets
The total number of SPAP packets sent or received.

Octets
The number of bytes of data that were sent or received in those packets.

Requests
The number of SPAP “Request” packets sent or received. These are the packets which contain the SPAP name/password pairs.

Acks The number of Acks (success replies) sent or received for the SPAP requests (for example, if the peer sends a valid Request packet, the router replies with an Ack).

Naks The number of Naks sent or received for the SPAP requests (for example, if the peer sends an invalid Request packet, the router replies with a Nak).

Dialbacks
The number of times a user:

- Requested a callback (roaming callback) and it was granted.
- Dialed-in and they were configured for required callback and dialed back at the predetermined number stored in the user profile.

PleaseAuthenticates
The number of SPAP please authenticate packets that have been sent or received on this interface. An SPAP please authenticate packet is sent as the result of a timeout when waiting for the other end to send an SPAP authenticate request.

Change Passwords
The number of change password requests that sent or received on this interface.

Alerts The number of SPAP banners that have been sent or received.

MCCP Call Reqs
Indicates that the sender requested another phone number to dial a second MP link.

MCCP Callbacks
Indicates that the sender supplied a phone number on which to be called back to establish a second MP link.

MCCP ACKs
The number of acknowledgments sent or received by MCCP.

MCCP NAKs
The number of negative acknowledgments sent or received by MCCP.

ccp Lists statistics for compression control protocol.

Example:

```
list ccp
CCP   Statistic           In                    Out
---------------           --                    ---
Packets:                  24                    25
Octets:                   174                   177
Reset Reqs                0                     0
Reset Acks:               0                     0
Prot Rejects:             0                     0
```

Packets
Indicates the number of packets received and transmitted on this interface.

Octets
Indicates the number of octets received and transmitted on this interface.

Reset Reqs
The number of CCP dictionary “Reset Requests” that were transmitted or received.

Reset Acks

The number of CCP dictionary “Reset Acknowledgments” that were transmitted or received.

Reset Request and Reset Acknowledgment packets are control packets passed between the CCP entities at each end, used to maintain synchronization of the data dictionaries at each end of the link.

Prot Rejects

Indicates the number of protocol rejects of CCP packets sent by the peer (reception of a protocol reject would signify that the peer does not support CCP).

cdp Displays statistics associated with compressed data packets sent or received on this interface.

Example:

```
list cdp
Compression Statistic      In                      Out
---------------------      --                      ---
Packets:                   31035                   46550
Octets:                    1614885                 2421137
Compressed Octets:         931416                  1521039
Incompressible Packets:    0                       0
Discarded Packets:         0                       0
Copied Packets:            1                       0
Prot Rejects:              0                       -

Compressor (transmit) statistics:
    Recent compression ratio: 1.7:1
Decompressor (receive) statistics:
    Recent compression ratio: 1.7:1
```

Packets

These counters indicate the number of compressed datagrams sent and received. On the output side, the count includes only those packets that were actually sent as PPP compressed datagrams; it does not include packets that were found to be incompressible and sent in their original uncompressed form.

These counters count the packets sent or received that had the PPP protocol type of X'00FD' (CDP). When STAC extended mode or MPPC has been negotiated, incompressible packets may be encapsulated in CDP datagrams. This encapsulation would include the incompressible packets in these counts.

Octets

These counters indicate the number of bytes effectively transmitted or received in compressed form. These counts reflect the lengths of the original datagrams before compression or after decompression.

Compressed octets

These counters indicate the number of bytes for all of the compressed datagrams sent and received. These counts are the lengths of the actual CDP packets after compression or before decompression.

Incompressible packets

These counters indicate the number of packets that were incompressible and therefore sent in original uncompressed form.

Discarded packets

These counters indicate how many packets were discarded because they could not be successfully decompressed. Typically these packets will be packets that the peer was transmitting just

after the router has sent a Reset-Request, but before the peer has received and processed the Reset-Request. Packets are also dropped if the router detects that data in the packets is incorrect. An example of incorrect data is a packet that contains a bad sequence number.

If the number of discarded packets increases too rapidly, then packets are being lost or corrupted on the line, probably due to noise on the line, and the link performance may be degraded.

Protocol rejects

This counter indicates the number of Protocol-Rejects of CDP packets that have been received from a peer. This count should be zero, because the link will not send CDP packets if the use of compression has not already been negotiated.

Compression ratios

The ratios give an approximate indication of the effectiveness of the compressor and decompressor. These ratios are based on the number of plain-text bytes divided by the number of corresponding compressed bytes, so values greater than 1 are preferable for both input and output. The higher the number, the more effective the compression.

The output ratio is computed as the ratio of the number of original plain-text bytes divided by the number of bytes sent as a result of attempting compression - whether the packet actually was compressed or sent as a CDP packet. If a data stream does not compress well and most of the packets are sent in their original form or in enlarged CDP packets, the compression output ratio will drop. If the ratio drops below 1.0, the compressor is actually reducing the effective bandwidth of the line rather than increasing it, and should be disabled on that interface if the state persists for a long time.

The input ratio is computed based on the number of bytes received in CDP frames divided into the number of decompressed bytes. Unlike the output ratio, this count does not include any packets that were incompressible and sent in plain-text form. This is because the router cannot determine if a received non-CDP packet was an incompressible packet that the peer sent in plain-text form, or just a packet that the peer did not attempt to compress.

Because of the method of calculation, the output ratio on one end of the link does not necessarily match the input ratio at the other end.

compression

This command displays the same information as list cdp.

bcp Lists statistics for the Bridging control protocol. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list bcp
BCP Statistic           In                  Out
--------------          --                  ---
Packets:                0                   0
Octets:                 0                   0
Prot Rejects:           0                   -
```

brg Lists statistics on the bridge packets received and transmitted over the PPP interface. These fields are the same as those described under the **list ip** command. (See “ip”.)

Example:

```
list brg
BRG Statistic           In                  Out
--------------          --                  ---
Packets:                0                   0
Octets:                 0                   0
Prot Rejects:           0                   -
```

stp Lists statistics for the spanning tree protocol. These fields are the same as those described under the **list ip** command. (See “ip”.)

Example:

```
list stp
Spanning Tree Statistic       In            Out
-----------------------       --            ---
Packets:                      0             0
Octets:                       0             0
```

nbcp Lists NetBIOS Control Protocol statistics for the point-to-point interface. These fields are the same as those described under the **list ip** command. (See “ip”.)

Example:

```
list nbcp
NBCP Statistic            In                    Out
---------------           --                    ---
Packets:                  0                     0
Octets:                   0                     0
Prot Rejects:             0                     -
```

nbfcp Lists NetBIOS Frame Control Protocol statistics for the point-to-point interface. These fields are the same as those described under the **list ip** command. (See “ip”.)

Example:

```
list nbfcp
NBFCP Statistic           In                    Out
---------------           --                    ---
Packets:                  0                     0
Octets:                   0                     0
Prot Rejects:             0                     -
```

ipcp Lists Internet Protocol Control Protocol statistics for the point-to-point interface. These fields are the same as those described under the **list ip** command. (See “ip”.)

Example:

```
list ipcp
IPCP STATISTIC       IN         OUT
--------------       --         ---
PACKETS:             0           0
OCTETS:              0           0
PROT REJECTS:        0
```

ip Lists all information related to IP packets over the point-to-point link.

Example:

```
list ip
IP Statistic         In         Out
------------         --         ---
Packets:             349        351
Octets:              128488     129412
Prot Rejects:        0          -
```

Packets
Indicates the total number of IP packets transmitted (out) and received (in) over the current point-to-point interface.

Octets
Indicates the total number of octets transmitted and received over the current IP connection.

Prot Rejects
Indicates the total number of protocol reject packets transmitted and received over the current point-to-point interface.

ipv6cp
Lists Internet Protocol version 6 Control Protocol statistics for the point-to-point interface. These fields are the same as those described under the **list ip** command. (See "ip" on page 424.)

Example:

```
list ipv6cp
IPv6CP STATISTIC       IN         OUT
--------------         --         ---
PACKETS:               0           0
OCTETS:                0           0
PROT REJECTS:          0
```

ipv6 Lists all information related to IPv6 packets over the point-to-point link. These fields are the same as those described under the **list ip** command. (See "ip" on page 424.)

Example:

```
list ipv6
IPv6 Statistic       In         Out
--------------       --         ---
Packets:             0           0
Octets:              0           0
Prot Rejects:        0
```

ipxcp Lists statistics for the IPX control protocol. These fields are the same as those described under the **list ip** command. (See "ip" on page 424.)

Example:

```
list ipxcp
IPXCP Statistic          In               Out
--------------          --               ---
Packets:                0                0
Octets:                 0                0
Prot Rejects:           0                -
```

ipx Lists IPX statistics for the point-to-point interface. These fields are the same as those described under the **list ip** command. (See "ip" on page 424.)

Example:

```
list ipx
IPX Statistic          In        Out
------------           --         ---
Packets:               0          0
Octets:                0          0
Prot Rejects:          0          -
```

atcp Lists statistics for the AppleTalk control protocol. These fields are the same as those described under the **list ip** command. (See "ip" on page 424.)

Example:

```
list atcp
ATCP Statistic          In                   Out
---------------         --                   ---
Packets:                0                    0
Octets:                 0                    0
Prot Rejects:           0                    -
```

ap2 Lists AppleTalk Phase 2 statistics for the point-to-point interface. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list ap2
AP2 Statistic        In         Out
-------------        --         ---
Packets:             349        351
Octets:              128488     129412
Prot Rejects:        0
```

dncp Lists statistics on the DECnet control protocol packets. These fields are the same as those described under the **list ip** command. (See “ip” on page 424 .)

Example:

```
list dncp
DNCP Statistic           In                 Out
--------------           --                 ---
Packets:                 0                  0
Octets:                  0                  0
Prot Rejects:            0                  -
```

dn Lists statistics on the DECnet packets received and transmitted over the PPP interface. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list dn
DN Statistic           In         Out
------------           --         ---
Packets:               0          0
Octets:                0          0
Prot Rejects:          0          -
```

osicp Lists statistics for the OSI control protocol. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list osicp
OSICP Statistic          In                   Out
---------------          --                   ---
Packets:                 0                    0
Octets:                  0                    0
Prot Rejects:            0                    -
```

osi Lists statistics on the OSI packets received and transmitted over the PPP interface. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list osi
OSI Statistic          In             Out
-------------          --             ---
Packets:               0              0
Octets:                0              0
Prot Rejects:          0              -
```

bvcp Lists statistics on the Banyan VINES control protocol. These fields are the same as those described under the **list ip** command. (See “ip” on page 424 .)

Example:

```
list bvcp
BVCP Statistic           In                 Out
--------------           --                 ---
Packets:                 0                  0
Octets:                  0                  0
Prot Rejects:            0                  -
```

vines Lists statistics for the Banyan VINES packets received and transmitted over

the PPP interface. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list vines
Vines Statistic           In                      Out
---------------           --                      ---
Packets:                  10                      13
Octets:                   320                     340
Prot Rejects:             0                       -
```

isrcp Lists statistics for APPN ISR Control Protocol packets. These fields are the same as those described under the **list ip** command. (See “ip” on page 424 .)

Example:

```
list isrcp
APPN ISRCP Statistic      In                      Out
---------------           --                      ---
Packets:                  3                       3
Octets:                   12                      12
Prot Rejects:             0                       -
```

isr Lists statistics on the APPN ISR packets received and transmitted over the PPP interface. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list isr
APPN ISR Statistic        In                      Out
-------------             --                      ---
Packets:                  220                     219
Octets:                   1266                    1157
Prot Rejects:             0                       -
```

hprcp Lists statistics for APPN HPR Control Protocol packets. These fields are the same as those described under the **list ip** command. (See“ip” on page 424 .)

Example:

```
list hprcp
APPN HPRCP Statistic      In                      Out
---------------           --                      ---
Packets:                  3                       3
Octets:                   12                      12
Prot Rejects:             0                       -
```

hpr Lists statistics on the APPN HPR packets received and transmitted over the PPP interface. These fields are the same as those described under the **list ip** command. (See “ip” on page 424.)

Example:

```
list hpr
APPN HPR Statistic         In                      Out
-------------             --                      ---
Packets:                  780                     715
Octets:                   131907                  69685
Prot Rejects:             0                       -
```

LLC

Use the **LLC** command to access the LLC monitoring prompt. LLC commands are entered at this new prompt. See “LLC Monitoring Commands” on page 221 for an explanation of each of these commands.

Note: This command is available only when APPN is included in the software load.

Syntax:

Point-to-Point Protocol Interfaces and the GWCON Interface Command

The PPP interface traffic is carried by an underlying data-link level device driver. Additional statistics that can be useful when monitoring PPP links may be obtained from the device driver statistics which are displayed using the **interface** command from the GWCON environment. (For more information on the **interface** command, refer to “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 111.)

The statistics in this section are displayed when you run the **interface** command from the GWCON environment (talk 5) for the following interfaces used in point-to-point configurations:

Example:

```
+int 0
                                                Self-Test  Self-Test Maintenance
Net   Net'   Interface                             Passed     Failed      Failed
0     0      PPP/0                                      2          0
  0

  Point to Point MAC/data-link on SCC Serial Line interface

  Adapter cable:               V.35 DCE  RISC Microcode Revision:
   0

   V.24 circuit: 105 106 107 108 109
   Nicknames:    RTS CTS DSR DTR DCD
   PUB 41450:    CA  CB  CC  CD  CF
   State:        ON  ON  ON  ON  ON

  Line speed:              2.048 Mbps
  Last port reset:         5 hours, 27 minutes, 4 seconds ago

  Input frame errors:
   CRC error                          0   alignment (byte length)
   0
   missed frame                       0   too long (>  2055 bytes)
   0
   aborted frame                      0   DMA/FIFO overrun
   0

  Output frame counters:
   DMA/FIFO underrun errors           0   Output aborts sent
   0
```

Net Interface number as assigned by software during initial configuration.

Net’ Base interface number as assigned by software during initial configuration.

Note: For dial circuit interfaces, Net’ is different from Net. For dial circuit interfaces, Net’ indicates the base interface (ISDN or V.25bis) that the dial circuit uses.

Interface No
Type of interface and its instance number. The Point-to-Point interface type is PPP.

Slot The slot number of the interface over which PPP is running.

Port The port number of the interface that is running PPP.

Self-Test: Passed
Total number of times the point-to-point interface passed its self-test.

Self-Test: Failed
Total number of times the point-to-point interface failed its self-test.

Maintenance: Failed
Total number of maintenance failures.

Adapter cable
Type of adapter cable that has been configured; for example, V.35 DTE.

V.24 circuit
Circuits being used on the V.24. Note: The symbol - - - in monitoring output indicates that the value or state is unknown.

Nicknames
Control signals Note: The symbol - - - in monitoring output indicates that the value or state is unknown.

PUB 41450
Pin assignments Note: The symbol - - - in monitoring output indicates that the value or state is unknown.

State State of the V.24 circuits (on or off). Note: The symbol - - - in monitoring output indicates that the value or state is unknown.

Line speed
Configured line speed or default value assumed (if line speed is configured as 0).

Last port reset
Length of time since the port was reset.

CRC error
The number of packets received that contained checksum errors and as a result were discarded.

Alignment (byte length)
The number of packets received that were not an even multiple of 8 bits in length and as a result were discarded.

Too long (> 2048 bytes)
The number of packets that were greater than the configured frame size, and as a result were discarded.

Aborted frame
The number of packets received that were aborted by the sender or a line error.

DMA/FIFO overrun
The number of times the serial interface could not send data fast enough to the system packet buffer memory to receive them from the network.

Missed frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the `L & F bits not set` counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the `L & F bits not set` counter will be affected by traffic.

Output Frame Counters:

DMA/FIFO underrun errors
The number of times the serial interface could not retrieve data fast enough from the system packet buffer memory to transmit them onto the network.

Output aborts sent
The number of transmissions that were aborted as requested by upper-level software.

Chapter 29. Using the Multilink PPP Protocol

This chapter describes how to use the Multilink PPP Protocol (MP). It includes the following sections:

The Multilink PPP Protocol allows you to increase the bandwidth of:

- PPP leased lines, including channelized and I43x ISDN circuits
- PPP ISDN dial circuits
- PPP V.25bis dial circuits
- PPP V.34 dial circuits
- PPP Layer 2 Tunneling circuits

Increased bandwidth is accomplished by defining a ***virtual link***made up of multiple links. The bandwidth of the resulting MP bundle is almost equal to the sum of the bandwidths of the individual links. The advantage is that large data packets transmitted across a single link can now be fragmented, transmitted across multiple links, and rebuilt at the receiving end station. MP uses both the Bandwidth Allocation Protocol and the Bandwidth Allocation Control Protocol to dynamically add and drop PPP dialcircuits to a virtual link. MP also uses Bandwidth-On-Demand (BOD) to add "dedicated" MP dial links to an existing bundle.

There are two types of MP links: those that are dedicated and those that are simply enabled. A dedicated MP link is an MP-enabled interface configured as a link to a particular MP interface. If the link attempts to join another MP bundle, or if MP is not negotiated at all, the software terminates the link. All PPP links except for layer-2-tunneling interfaces can be configured as dedicated MP links. PPP leased links must be configured as dedicated MP links.

PPP dial-circuits and Layer 2-Tunneling can be configured as MP enabled. An MP-enabled link that is not dedicated can become a link in any MP bundle. If MP is not negotiated, the link operates as an independent interface using the link's configured protocols.

You can configure a Multilink PPP interface that consists of multiple PPP dial circuits as part of the MP bundle.

There are also two types of MP interfaces: those that have a dedicated link and those that do not. An MP interface needs a dedicated link in any one of the following situations:

- The link is only for the MP interface
- The MP interface is configured for outbound calls. The dedicated link must then be configured with the destination phone number and caller identification.
- The MP interface is configured to receive a particular inbound call. In this case, the dedicated link is configured with the inbound destination phone number and caller identification.
- The MP interface needs to perform outbound authentication. In this case, all links use the same authentication name.

Using MP

MP interfaces that do not have a dedicated link must be inbound-only interfaces. These interfaces are similar to the any inbound dial circuit.

The Bandwidth Allocation Protocol (BAP) and its control protocol (BACP) allow an MP interface to increase and decrease its bandwidth by adding and dropping dial circuits. When the bandwidth utilization algorithm determines that a link should be added to the bundle, if there is an available PPP dial-circuit, and the peer agrees, an additional call is placed.

BAP first searches for any idle dedicated PPP dial circuits for the MP interface, and then for any MP-enabled PPP dial circuit. It will not, however, use a dedicated PPP dial circuit of another MP circuit. The configured maximum number of links on the MP interface will never be exceeded.

BOD uses configured dial-circuit phone numbers to place calls when needed to add dedicated MP dial links to an existing bundle. Links are added to the bundle one at a time, if needed, during a polling period. BOD adds any PPP serial links to the bundle first and will retain the serial links throughout the life of the bundle. BOD only drops dial links.

MP supports the following features:

- BRS
- WRR
- WRS
- Dial-on-Demand
- DIALs

However, WRS, Dial-on-Demand, and DIALs are only supported on MP bundles that contain only dial circuits.

MP Considerations

When configuring an MP bundle, keep the following in mind:

- Mixing dial circuits with “leased” lines causes the software to disable BAP on the bundle and use BOD instead. Only mix dial circuits with “leased” circuits when you desire to use BOD to manage the bundle.
- You cannot use Dial-on-Demand or WRS for MP bundles that contain either PPP “leased” lines or Layer 2 Tunneling circuits.
- You cannot use DIALs on bundles that contain PPP “leased” lines.
- All devices joining an MP bundle must have link speed configured.

  Important:

  1. Do not configure a bundle with media with extremely dissimilar properties. The largest link should have no more than 4 times the capacity of the smallest link. If the speeds of the links in an MP bundle differ greatly, you may need to add receive buffers to the faster link.
  2. When bundling ISDN B-channels with slower media types, you may need to increase the number of ISDN buffers. Bundling ISDN B-channels with slower links is not recommended for ISDN primary.

Multi-Chassis MP

An MP bundle with a Layer 2 Tunnel that contains a phone hunt group that spans multiple physical Network Access Servers is known as a *multi-chassis MP.* Multi-chassis MP uses rhelm or user-based tunneling (see "Using Local or Remote Authentication" in *Using and Configuring Features*) to establish the MP endpoint destination. See "Using Layer 2 Tunneling Protocol (L2TP)" in *Using and Configuring Features* for more information about L2TP.

Configuring a Multilink PPP Interface

Configuring an MP interface depends on the type of interface used in the MP bundle. The following sections contain examples of the various configurations.

After configuring the MP interface, you may configure bandwidth-on-demand (BOD). The following example configures BOD on existing MP interface 17:

```
Config> net 17
MP config:  17> enable bod
Enable BAP? [N]

MP config:  17> set bandwidth-on-demand parameters
Add bandwidth % [90]:
Drop bandwidth % [70]:
Bandwidth test interval (sec) [15]

MP config:  17>
```

Configuring MP on PPP Dial Circuits

This section shows how to configure a Multilink PPP interface by using an example that configures Multilink PPP with two ISDN dial circuits.

1. Add the two dial circuits and the multilink PPP interface.

```
*t 6

Config>add dev dial-circuit
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
Config>add dev dial-circuit
Adding device as interface 8
Defaulting Data-link protocol to PPP
Use "net 8" command to configure circuit parameters
Config>add dev multilink-ppp
Enter the number of multilink PPP interfaces [1]?
Adding device as interface 9
Defaulting Data-link protocol to PPP
Use "net intf" command to configure circuit parameters
Config>
```

2. Configure each PPP dial circuit. (See "Chapter 42. Configuring and Monitoring Dial Circuits" on page 563.) In this example, the destination, call direction, and LIDs are set for one of the dial circuits.

```
Config>net 7
Circuit configuration
Circuit config:   7>set dest out
Circuit config:   7>set calls outbound
Circuit config:   7>set net 6
Circuit config:   7>
```

3. Enable MP on each dial circuit to be used for MP as follows:

```
Circuit config:   7>encapsulator
Point-to-Point user configuration
PPP 7 Config>enable mp
```

```
Enabled as a Multilink PPP Link,
Use as a dedicated Multilink PPP link? [No]: yes
Multilink PPP net for this Multilink PPP link [1]? 9
NOTE: PPP configuration will be obtained from the Multilink PPP
      net.  It is NOT necessary to configure PPP for this net!
```

Note: You cannot configure PPP parameters for dedicated links from this prompt. Dedicated links use the existing MP interface's PPP configuration.

By answering "Yes" to the question "Use as a dedicated Multilink PPP link?" the link becomes dedicated to the specified Multilink PPP interface (9 in this example). In this case, the link ***must*** be used for an MP bundle and ***must*** join the specified MP interface. The link cannot be used as a regular PPP dial circuit.

Answering "No" to "Use as a dedicated Multilink PPP link?" will allow this PPP dial-circuit to join any MP interface. At least one PPP dial-circuit ***must*** be a dedicated link to an outbound MP interface.

A dedicated PPP dial circuit obtains all PPP parameters (LCP options, authentication, and others) from its MP interface. MP enabled PPP dial circuits joining the same MP bundle ***must*** negotiate the same LCP parameters and authentication name.

4. Configure the MP interface. Protocols, BAP, BRS, WAN restoral, WAN reroute, and dial-on-demand are all run on the MP interface and not the PPP dial circuits.

Configuring MP on PPP Serial Links

To configure MP on a PPP serial link, you enable MP on the interface using the **net** command. The link obtains its PPP configuration from the MP net.

Example:

```
Config> net 1
PPP 1 Config> enable MP

Multilink PPP net for this Multilink PPP link [1]? 8
NOTE: PPP configuration will be obtained from the Multilink PPP
      net.  It is NOT necessary to configure PPP for this net!
PPP 1 Config>
```

Configuring MP on Layer-2-Tunneling Nets

To configure MP on an L2TP net, you enable MP through the L2TP encapsulator. You then must configure the same PPP negotiation parameters (see "Configuring L2TP" in *Using and Configuring Features*) for information about all nets joining in a single bundle.

Example:

```
Config> feature layer-2-tunneling
Layer-2-Tunneling Config> encapsulator
PPP-L2TP Config> enable mp

NOTE: It IS necessary to configure PPP for this net!  PPP
      negotiation parameters must be configured the same for
      all nets wishing to join the same Multilink PPP bundle.
PPP-L2TP Config>
```

Configuring Multi-Chassis MP

To configure MP for Multi-Chassis MP, configure the DIALs feature for multi-chassis MP. The software prompts you for the endpoint discriminator to use.

Example:

```
Config> feature DIALs
DIALs Config> set multi-chassis-mp
   Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
DIALs Config>
```

The following example shows multichassis MP when ports RTR-2 and RTR-3 are in a hunt group.

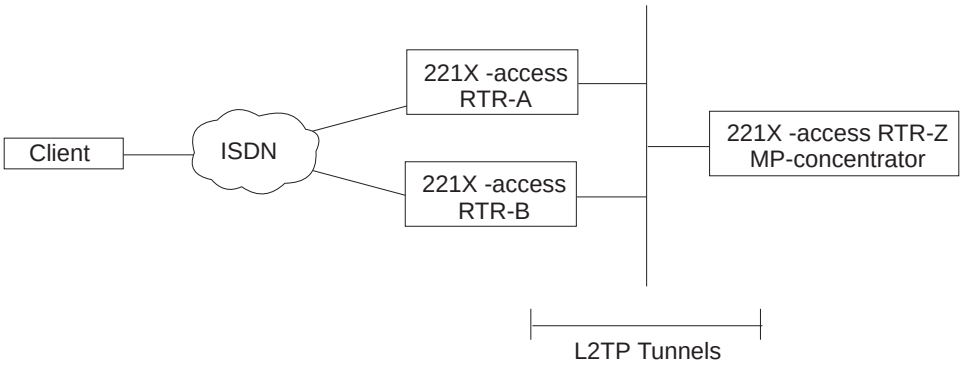

Figure 26. Multichassis MP

Because there is a many-to-many relationship between access routers and MP-concentrators, all access routers (RTR-A, RTR-B) should be kept on a separate administrative domain from “MP concentrator” routers (RTR-Z). This applies if you want to use remote authentication (that is,RADIUS), you will need two RADIUS servers, one for access routers and one for MP concentrators. If you are using local-list, you are already using separate administrative domains.

In this scenario, you can choose to tunnel based on PPP username or ″rhelm″ name. It is less rigorous to use rhelm-based tunneling. The idea is to configure a tunnel-profile for RTR-Z on both RTR-A and RTR-B. No additional PPP users are required on these routers. RTR-Z would require 2 tunnel-profiles: one for RTR-A and one for RTR-B and a PPP username (in the form <*username*>@RTRZ) for each anticipated user. All dial-in circuits are configured on the “access” routers. The “MP concentrators” would have layer-2-tunneling devices and multilink-PPP devices.

At this point, we have “statically configured” multi-chassis MP. This means that a particular PPP username will always terminate MP on a preconfigured router as opposed to supporting an additional protocol which dynamically finds MP bundle heads and tunnels when needed. This network implementation will also help avoid client PPP negotiation idiosyncrasies when using different media types for each link in a bundle (for example, tunnel one link and not the other). For example, DIALs clients cannot renegotiate LCP at any point. Also, Microsoft DUN clients do not fully support LCP renegotiation.

Chapter 30. Configuring and Monitoring Multilink PPP Protocol (MP)

This chapter describes how to configure specific Multilink PPP interfaces in a device. The chapter includes:

Accessing the MP Configuration Prompt

To access the `MP config>` prompt:

1. Enter **talk 6** at the * prompt.
2. Enter **net *n***, where n is the number of the dial circuit or MP interface that you enabled to use MP.

   Note: You are now configuring the Multilink PPP interface and not the PPP dial circuit that is part of the MP bundle.

MP Configuration Commands for Multilink PPP Interfaces

Table 48 lists the commands available at the `MP config>` prompt.

Table 48. MP Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Disable	Disables the negotiation of bandwidth on demand.
Enable	Enables the negotiation of bandwidth on demand.
Encapsulator	Places you in the `PPP config>` prompt so you can change the data-link protocol configuration.
List	Displays the MP interface configuration parameters.
Set	Configures MP interface for inbound or outbound traffic. Also allows you to set the idle timeout and other MP and BAP parameters.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Disable

Use the **disable** command to disable the negotiation of bandwidth-on-demand (BOD). Disabling BOD prevents the link from allocating additional bandwidth when necessary.

Syntax:

disable bod

Enable

Use the **enable** command to enable the negotiation of BOD. Enabling BOD allows the link to allocate additional bandwidth when necessary.

Syntax:

enable bod

Encapsulator

Use the **encapsulator** command to access the PPP link-layer configuration for the Multilink PPP interface.

Syntax:

encapsulator

Example:

```
encapsulator
Point-to-Point user configuration
PPP config>
```

List

Use the **list** command to display the current MP configuration.

Syntax:

list

Example:

```
list
Idle timer = 0 (fixed circuit)
Outbound calls = allowed
Dialout MP Link net = 7
Max fragment size = 750
Min fragment size = 375
Maximum number of active links = 2
Links associated with this MP bundle:
net number 7
net number 8
BAP enabled
Add bandwidth percentage = 90
Drop bandwidth percentage = 70
Bandwidth test interval (sec) = 15
```

Idle timer
The setting of the idle timer for this circuit in seconds.

A setting of 0 indicates a fixed circuit. A nonzero setting configures a dial-on-demand MP circuit that will be brought down when the circuit is idle for the specified number of seconds The circuit is reactivated when network traffic resumes.

Outbound calls
Specifies whether the interface is configured to initiate outbound calls. If the interface cannot initiate outbound calls, this line is not displayed.

Inbound calls
Specifies whether the interface is configured to initiate inbound calls. If the interface cannot accept inbound calls, this line is not displayed.

Max fragment size
Specifies the largest number of bytes of data a packet can contain before the packet is fragmented to be sent over MP links.

Min fragment size
This is the minimum size of the fragments (in bytes) the software creates when a packet exceeds ***Max fragment size***.

Maximum number of active links
Specifies the configured maximum number of links in the MP virtual link (also known as ***bundle***).

Links associated with this MP bundle
Displays the links dedicated to this MP interface.

BAP enabled
Specifies whether BAP is enabled on this interface.

Add bandwidth percentage
The amount of bandwidth utilization at which the software will try to add a new link if BAP is enabled.

Drop bandwidth percentage
The amount of bandwidth utilization at which the software will remove a link from the MP bundle if BAP is enabled.

Bandwidth test interval
The time, in seconds, after which the software will check the bandwidth utilization to determine whether to add or drop a link from the bundle.

Set

Use the **set** command to configure:

- The MP interface for inbound or outbound calls
- The idle timeout
- The MP parameters
- The BAP parameters

Syntax:

set bod parameters
calls
idle
mp parameters

bod parameters
Prompts you to specify the BOD add and drop bandwidth percentages and the BOD test interval.

Example:

```
set bod parameters
Add bandwidth % [90]? 80
Drop bandwidth % [70]? 50
Bandwidth test interval (sec) [15]? 25
```

Add bandwidth %
The amount of bandwidth utilization at which the software will try to add a new link.

Valid Values: 1 to 99

Default Value: 90

Drop bandwidth %
The amount of bandwidth utilization at which the software will remove a link from the MP bundle.

Valid values: 1 to 99

Default value: 70

Bandwidth test interval (sec)
The time, in seconds, after which the software will check the bandwidth utilization to determine whether to add or drop a link from the bundle.

Valid Values: 10 to 200 seconds

Default Value: 15

calls Specifies whether this MP interface will initiate outbound calls, only accept outbound calls, or participate in both types of calls.

Valid values: inbound, outbound, or both

Default value: inbound

Note: If you specify outbound or both, the software will request the net number of the dedicated MP link that will place the first call.

Example:

```
set calls outbound
Dialout MP link net for this MP net []? 4
```

idle Specifies the time period in seconds that an interface can have no protocol traffic at which the MP interface will end calls on all the links.

Valid Values: 0 to 65535

Default Value: 0

mp parameters
Prompts you to enter the maximum and minimum fragment sizes and the maximum number of active links.

Example:

```
set mp parameters
Max frag size [750]? 675
Min frag size [375]? 300
Max number of active links [2]? 4
```

Max frag size
Specifies the largest of number of bytes of data a packet can contain before the packet is fragmented to be sent over MP links.

Valid Values: 100 to 3 000

Default Value: 750

Min frag size
This is the minimum size of the fragments (in bytes) the software creates when a packet exceeds ***Max fragment size***.

Valid Values: 100 to 3 000

Default Value: 375

Max number of active links
Specifies the configured maximum number of links in the MP virtual link (also known as ***bundle***).

Valid Values: 1 to 64

Default Value: 2

Monitoring MP Interface Status

To determine the status of all the MP interfaces in your device, use the **configuration** command in **talk 5** (see “Configuration” on page 114).

Accessing the MP Monitoring Commands

To access the MP monitoring commands:

1. Enter **talk 5** at the * prompt.
2. Enter **net *n***, where ***n*** is the number of the MP interface that was created in talk 6 using **add device multilink-ppp** command.

Multilink PPP Protocol Monitoring Commands

Table 49 shows the monitoring commands available for an MP interface.

Table 49. MP Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
List	Displays BAP, BACP, BOD, and MP statistics, errors, and other information.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

List

Use the **list** command to display information about the MP interface including bandwidth allocation statistics.

Syntax:

list
bacp
bap
control bacp
control bod
control mp
mp

Note: The examples that follow assume that the MP interface on this device is net number 6.

bacp The **list bacp** command lists the statistics for bandwidth allocation control packets which have been sent or received on this MP circuit.

Example:

```
PPP 6> list bacp

BACP Statistic            In          Out
--------------            --          ---
Packets:                  6           8
Octets:                   60          80
Rejects:                  0           -
```

bap The **list bap** command lists the statistics for bandwidth allocation protocol packets which have been sent or received on this MP circuit.

Example:

```
PPP 6> list bap

BAP Statistic               In          Out
-------------               --          ---
Packets:                    3           3
Octets:                     22          37
Call Requests:              1           0
Call Response(ACK):         0           1
Call Resp(NK & FLLNK):      0           0
Call Response(Rej):         0           0
Callback Requests:          0           0
Callback Response(ACK):     0           0
Cllbck Resp(NK & FLLNK):    0           0
Callback Response(Rej):     0           0
Drop Requests:              0           1
Drop Response(ACK):         1           0
Drop Resp(NK & FLLNK):      0           0
Drop Response(Rej):         0           0
Call Status(Success):       1           0
Call Status(Fail):          0           0
```

There are four different responses to a peer's request: ACK, NAK, FULL-NAK, and REJECT.

ACK Indicates the peer's request has been granted.

NAK (NK)
Indicates that the peer's request is supported but not desired at this time. Try again later.

FULL-NAK (FLLNK)
Indicates that the peer s request is supported but because of a resource condition, cannot be granted at this time. The request should not be sent again until the total bandwidth across the MP bundle changes.

REJECT (REJ)
Indicates that the request is not supported.

control bacp
The **list control bacp** command lists the current state of the BACP state-machine within PPP. The state information is identical to that produced for all of the PPP control protocols. Information about favored peer is also listed. Favored peer is used to alleviate BAP packet collisions (when both sides simultaneously initiate requests). During BACP negotiations, each side sends a magic-number and the one with the smallest magic number is the favored peer and should take precedence in the event of a collision. Typically, the call initiator will choose a ***magic number*** of X'1' and the call receiver will choose a magic number of X'FFFFFFFF' establishing the call initiator as the favored peer.

```
PPP 6> list control bacp

BACP State:               Open
```

```
BACP Option              Local                  Remote
----------               -----                  ------
Magic Number:            FFFFFFFF               1
Favorite Peer:           NO                     YES
```

control bod

The **list control bod** command lists the current state of bandwidth-on-demand (BOD). This information includes BAP state, configured bandwidth-on-demand parameters for adding and subtracting bandwidth, current bandwidth, and information from the last bandwidth poll.

Valid BAP states are:

Closed
BACP is not opened – BAP is either not enabled or not supported by the peer.

Ready BACP is opened and there is no outstanding request being processed.

Call Req Sent
There is an outstanding call-request that was sent from the local machine.

Callback Req Sent
There is an outstanding callback-request that was sent locally.

Call Placed
As a result of a BAP request to add bandwidth, a call has been placed.

Retry Status Sent
The outgoing call failed to join the MP bundle, a retry status was sent.

No Retry Status Sent
The outgoing call either succeeded or exhausted all retries, a no retry status was sent.

Drop Req Sent
There is an outstanding drop request that was sent locally.

Configured bandwidth-on-demand parameters include add percentage, drop percentage, maximum number of active links in the MP bundle, and the bandwidth polling interval.

A BAP request to add a link to the bundle will be initiated if both the following conditions are met:

- The current number of active links is less than the configured maximum number of links.
- The bandwidth utilization across all links in the MP bundle is greater than the add percentage of the total available bandwidth for the MP bundle.

A BAP request to drop a link from the MP will be initiated if both the following conditions are met:

- The number of active links is greater than one.
- The bandwidth utilization across all links in the MP bundle is less than the drop percentage of the total available bandwidth for the MP bundle for the number of links minus one.

Bandwidth can be polled only when BAP is in the ready state. The information listed from the previous poll will give you an idea of the bandwidth utilization across the MP bundle.

These two sets of information are displayed when a drop can be initiated:

- Bandwidth utilization across the entire bundle
- Bandwidth utilization across number of links minus one

To prevent thrashing, the second set of information is used when determining whether to drop a link.

Example:

```
PPP 11>list control bod

BOD :                                          Disabled
BAP :                                          Disabled
Bandwidth test interval (sec):                 15
Add bandwidth percentage:                      90
Drop percentage (links-1):                     70
Max # active links in MP bundle:               2
Time since last Bandwidth check (sec):         19
Currently:
    # active links in MP bundle:              0
    Total MP bandwidth (Bytes/sec):            0
Last Bandwidth Check:
    # active links in MP bundle:              0
    Avg Inbound bandwidth util (%):            0
    Avg Outbound bandwidth util (%):           0
```

control mp

The **list control mp** command lists the current state of this MP circuit including the number of active links and bandwidth, the configured maximum number of links, and statistics for number of dropped packets. Dropped MP packets are classified into four categories:

M
The packet is dropped because a sequence number has not been received and it is less than the minimum sequence number across all links' last received sequence number.

Timeout
The packet is dropped because a sequence number has not been received during a timeout period.

Q depth
The packet is dropped because the maximum queue depth was exceeded.

Seq order
The packet is dropped because the sequence number received was not expected. This occurs when MP receives delayed packet that it has already declared lost.

If a packet is dropped at the network layer, it can be either an M, Timeout, or Q depth packet. These counters are incremented appropriately when a packet is dropped.

```
PPP 11> list control mp
 Current # active links in MP bundle:          0
 Max # active links in MP bundle:              2
 Total MP bandwidth (Bytes/sec):               0
 Dropped Frags (lost packets):                 0
 Dropped Frags (timeout or receive overflow):  0
 Dropped Frags (sequence not expected):        0

 PPP 11>
```

mp The **list mp** command lists the statistics for packets which have been sent or received on this MP circuit. The number of bytes displayed is for pre-decompressed packets if compression was negotiated for the multilink PPP bundle.

```
PPP 6> list mp

MP Statistic               In          Out
------------               --          ---
Bytes (Compressed):        61230       60259
```

Chapter 31. Configuring SDLC Relay

This chapter describes the Synchronous Data Link Control (SDLC) Relay configuration and operational commands.

For further information on when to use DLSw SDLC versus SDLC Relay, refer to "Relationship to the SDLC Relay Function" in the "Using and Configuring DLSw" chapter of *Protocol Configuration and Monitoring Reference Volume 1*.

The chapter includes the following sections:

Basic Configuration Procedure

This section outlines the minimum configuration steps required to get the SDLC Relay protocol up and running. For further configuration information and explanation, refer to the configuration commands described in this chapter.

Note: You must restart the router for new configuration changes to take effect.

- *Add a number.* You must add a number to a group of primary or secondary ports using the **add group** command. The default number for this command is 1.
- *Add a local port.* This identifies the interface that you are using for the local port. This also assures that no IP address is configured for the interface that you select. Use the **add local-port** command.
- *Add a remote port.* This identifies the port directly connected to the remote side of the serial line. Use the **add remote-port** command.

Accessing the SDLC Relay Configuration Environment

To access the SDLC relay (SRLY) configuration environment:

1. At the `Config>` prompt, enter **set data-link srly**.
2. Enter the interface number.
3. To configure the SRLY interface, enter the **network** *interface#* command. The `SRLY` *`interface#`* `Config>` prompt is displayed when **network** ***interface#*** is entered:

```
Config>network 2
SDLC relay interface user configuration
SRLY 1 Config>
```

4. To configure the SRLY protocol parameters, enter the **protocol sdlc** command. The `SDLC Relay config>` prompt is displayed when **protocol sdlc** is entered:

```
Config>protocol sdlc
SDLC Relay protocol user configuration
SDLC Relay config>
```

SDLC Relay Configuration Commands

This section summarizes the SDLC Relay configuration commands. Both the **network** and **protocol** parameters for SDLC relay are documented in this chapter.

The SDLC Relay configuration commands allow you to specify router parameters for interfaces transmitting SDLC Relay frames. Restart the router to activate the configuration commands. Table 50 shows the commands for both the **network sdlc** and **protocol sdlc**.

Table 50. SDLC Relay Configuration Commands Summary

Command	Network SRLY	Protocol SDLC	Function
? (Help)	yes	yes	Lists all of the SDLC Relay configuration commands or lists the options associated with specific commands.
Add		yes	Adds groups, local ports, and remote ports.
Delete		yes	Deletes groups, local ports, and remote ports.
Disable		yes	Disables groups and ports.
Enable		yes	Enables groups and ports.
List	yes	yes	Displays entire SDLC Relay and group specific configurations.
Set	yes		Sets the link parameters and remote station parameters.
Exit	yes	yes	Exits the SDLC Relay configuration environment and returns to the CONFIG environment.

Add

Use the **add** command to add group numbers, local ports, and remote ports.

Syntax:

add group *group#*
local-port
remote-port

group Assigns a number to a group of primary or secondary ports added to the router.

Example: `add group`

```
Group number: [1]? 1
```

Group number
The group number that you are designating for the port.

local–port
Identifies the interface that you are using for the local port.

Example: `add local–port`

```
Group number: [1]? 1
Interface number: [0]? 2
(P)rimary or (S)econdary:[S]? p
```

Group number
The group number for the port. This number must match one of the **add group** parameters configured previously.

Interface number
The interface number of the router that designates the local port.

Primary or Secondary
Designates the port type, primary (P) or secondary (S).

remote–port
Identifies the IP address of the port directly connected to the serial line on the remote router.

Example: `add remote–port`

```
Group number: [1]? 1
IP address of remote router:[0.0.0.0]? 128.185.121.97
(P)rimary or (S)econdary:[S]? s
```

Group number
The group number for the port. This number must match one of the add group parameters configured previously.

IP address of remote router
Identifies the IP address of the interface on the remote router.

Primary or Secondary
Designates the port type, primary (P) or secondary (S).

Delete

Use the **delete** command to remove group numbers, local ports, and remote ports.

Syntax:

delete group . . .
local-port . . .
remote–port

group *group#*
Removes a group (group#) of SDLC Relay configured ports.

Example: `delete group 1`

local–port *interface#*
Removes the local port for the specified interface (interface#).

Example: `delete local–port 2`

remote–port
Removes the remote port for the specified group.

Example: `delete remote–port`

```
Group number: [1]? 1
(P)rimary or (S)econdary:[S]? S
```

Group number
The group number for the remote port.

Primary or Secondary
Designates the port type, primary (P) or secondary (S).

Disable

Use the **disable** command to suppress relaying for an entire relay group or a specific relay port.

Syntax:

disable group . . .

port

group *group#*

Suppresses transfer of SDLC Relay frames to or from a specific group (group#).

Example: `disable group 1`

port Suppresses transfer of SDLC Relay frames to or from a specific local port.

Example: `disable port`

```
Group number: [1]? 2
(P)rimary or (S)econdary:[S]? s
```

Group number

The group number of the port that you want to disable.

Primary or Secondary

Designates the port type, primary (P) or secondary (S).

Enable

Use the **enable** command to turn on data transfer for an entire group or a specific local interface port.

Syntax:

enable

group . . .

port

group *group#* Allows transfer of SDLC Relay frames to or from the specified group (group#).

Example: `enable group 1`

port Allows transfer of SDLC Relay frames to or from the specified local port.

Example: `enable port`

```
Group number: [1]? 2
(P)rimary or (S)econdary:[S]? s
```

Group number

The group number of the port that you want to enable.

Primary or Secondary

Designates the port type, primary (P) or secondary (S).

List (for network SRLY)

Use the **list** command to display the configuration of a specific group or of all groups.

Syntax:

list

Example:

```
list
Maximum frame size in bytes = 2048
Encoding:  NRZ
Idle State:  Flag
Clocking:  External
Cable Type:  RS-232 DTE
Speed (bps):  0
Transmit Delay Counter:  0
```

Maximum frame size in bytes
Maximum frame size that can be sent over the link. The maximum frame size must be large enough to accommodate the largest frame and the 15 byte SRLY header.

Encoding
The transmission encoding scheme for the serial interface. Scheme is NRZ (non-return to zero) or NRZI (non-return to zero inverted).

Idle State
The data link idle state: flag or mark.

Clocking
The type of clocking: internal, external.

Cable Type
The serial interface cable type.

Speed (bps)
Lists the speed of the transmit and receive clocks.

Transmit Delay Counter
Number of flags sent between consecutive frames.

List (for protocol SDLC)

Use the **list** command to display the configuration of a specific group or of all groups.

Syntax:

list all

group . . .

all Displays the configurations of all local ports.

Example: `list all`

```
              SDLC Relay Configuration

Group Number     Port Status      Net   SDLC Station    IP Address
                                 Number address (hex)
-------------- ---------------- ------ -------------  ------------
    1 (E)      Local   PRMRY (D)   2
    1 (E)      Remote SCNDRY (E)                     128.185.452.11
    2 (D)      Local   PRMRY (D)   1
    2 (D)      Remote SCNDRY (D)                     128.185.450.31
```

Group Number
Indicates the group number and the status of the group, enabled (E) or disabled (D).

Port Status
Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).

Net Number
Indicates the device number of the local port. This number matches the number displayed using the Config list devices command.

IP Address
Indicates the IP address of the remote port.

group *group#*
Displays the configuration of a specified group.

Example: `list group 1`

```
              SDLC Relay Configuration

 Group Number     Port Status      Net   SDLC Station    IP Address
                                  Number address (hex)
-------------- -----------------  ------ -------------  ------------
    1 (E)      Local   PRMRY (D)   2
    1 (E)      Remote SCNDRY (E)                     128.185.452.11
```

Group Number
Indicates the group number and the status of the group, enabled (E) or disabled (D).

Port Status
Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).

Net Number
Indicates the device number of the local port. This number matches the number displayed using the Config list devices command.

IP Address
Indicates the IP address of the remote port.

Set

Use the **set** command to configure the SRLY parameters.

Syntax:

set cable
clocking
encoding
frame-size
idle
speed
transmit-delay

cable Sets the cable used on the serial interface. The options are:

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- X21 DTE
- X21 DCE

A DTE cable is used when you are attaching the router to some type of DCE device (for example, a modem or a DSU/CSU).

A DCE cable is used when the router is acting as the DCE and providing the clocking for direct attachment.

clocking *internal* **or** *external*
Configures the SRLY link's clocking. To connect to a modem or DSU, configure clocking as external. To connect directly to another DTE device, use a DCE cable, set the clocking to internal, and configure the clock speed. For internal clocking, you must enter a valid line speed in the range 2400 - 2048000 bits per second.

Example:

```
set clocking internal
```

encoding *nrz* **or** *nrzi*
Configures the SRLY interface's encoding scheme as NRZ (Non-Return to Zero) or NRZI (Non-Return to Zero Inverted). NRZ is the default.

Example:

```
set encoding nrz
```

frame-size
Configures the maximum size of the frames that can be transmitted and received on the data link. If this value is set to a larger value than that specified with the add remote-secondary command, then this value is changed to reflect that maximum. The IBM 2212 generates an ELS message warning the user that this value is changing. The user will continue receiving this ELS message until it is changed in the SRAM configuration. Valid entries are shown in Table 51.

Note: The frame size must be large enough to accommodate the largest frame received plus a 15–byte SRLY header.

Table 51. Valid Values for Frame Size in Set Frame-Size Command

Minimum	Maximum	Default
128	8187	2048

idle flag
Configures the transmit idle state for framing on the SRLY interface. The default is the flag option which provides continuous flags (7E hex) between frames.

The link will receive a flag idle transparently.

idle mark
Configures the transmit idle state for framing on the SRLY interface. The mark option puts the line in a marking state (OFF, 1) between frames.

The link will receive a mark idle transparently.

speed For internal clocking, this command specifies the speed of the transmit and receive clock lines. The range of speeds supported is 2400 - 2048000 bits per second.

- interface 1.
- port 1 of a 4-port WAN concentration adapter.
- ports 1 and 5 of an 8-port WAN concentration adapter.

If you want to use a line speed greater than 2048000, you can only do this on port 1 of the system card's integrated WAN ports and all other integrated WAN ports must be clocked at 64 Kbps or less.

transmit-delay *value*
Allows the insertion of a delay between transmitted packets. This command ensures a minimum delay between frames so that it is compatible with older, slower serial devices at the other end. This value is specified as the number of flag bytes that should be sent between consecutive frames. The range is 0 - 15. The default is 0.

Accessing the SDLC Relay Monitoring Environment

To monitor information related to the SDLC Relay interface, access the interface monitoring process by doing the following:

1. Enter the **status** command to find the PID for GWCON. (See page 11 for sample output of the **status** command.)
2. At the OPCON prompt, enter the **talk** command and the PID for GWCON. For example:

   ```
   * talk 5
   +
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.
3. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

   ```
   + configuration
   ```

   See page 114 for more sample output from the **configuration** command.
4. Enter the **protocol sdlc** command. For example:

   ```
   + prot sdlc
   SDLC Relay>
   ```

   The SDLC Relay prompt is displayed on the console. You can then view information about the SDLC Relay ports by entering the SDLC Relay monitoring commands.

SDLC Relay Monitoring Commands

This section summarizes and then explains the SDLC Relay monitoring commands. The SDLC Relay monitoring commands allow you to view parameters for interfaces transmitting SDLC Relay frames. The `SDLC Relay>` prompt is displayed for all SDLC Relay monitoring commands. Table 52 shows the commands.

Table 52. SDLC Relay Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Clear-Port-Statistics	Clears SDLC Relay statistics for the specified port.
Disable	Temporarily suppresses groups and ports.
Enable	Temporarily turns on groups and ports.
List	Displays entire SDLC Relay and group specific configurations.

Table 52. SDLC Relay Monitoring Commands Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Clear-Port-Statistics

Use the **clear-port-statistics** command to discard the SDLC Relay statistics for all ports. The statistics include counters for packets forwarded and packets discarded.

Syntax:

clear-port-statistics

clear-port-statistics
Clears port statistics gathered since the last time you restarted the router or cleared statistics.

Example:

```
clear-port-statistics
Clear all port statistics? (Yes or No): Y
```

Disable

Use the **disable** command to suppress data transfer for an entire group or a specific relay port. SRAM (static read access memory) does not permanently store the effects of the **disable** monitoring command. Therefore when you restart the router, the effects of this command are erased.

Syntax:

disable group . . .

port

group *group#*
Suppresses transfer of SDLC Relay frames to or from a specific group (group#).

port *interface# primary-or-secondary*
Suppresses transfer of SDLC Relay frames to or from a specific local port.

Example:

```
disable port
Interface number: [0]? 2
(P)rimary or (S)econdary: [s]? P
```

Interface number
Indicates the interface number of the local port that you want to disable.

Primary or Secondary
Indicates whether the port is a primary or secondary.

Enable

Use the **enable** command to turn on data transfer for an entire group or a specific local interface port. SRAM does not permanently store the effects of the **enable** monitoring command. Therefore when you restart the router, the effects of this command are erased.

Configuring and Monitoring SDLC Relay

Syntax:

enable group . . .

port

group *group#*

Allows transfer of SDLC Relay frames to or from the specified group (group#).

port Allows transfer of SDLC Relay frames to or from the specified local port.

Example:

```
enable port
Interface number: [0]? 2
(P)rimary or (S)econdary: [s]? P
```

Interface number

Indicates the interface number of the local port that you want to enable.

Primary or Secondary

Indicates whether the port is a primary or secondary.

List

Use the **list** command to display the configuration of a specific group or of all groups.

Syntax:

list all

group . . .

all Displays the configurations of all local ports.

Example:

```
list all
                SDLC Relay Configuration

Group  Port Status       Net    Packets    IP Address
Num                      Num   fwrd  disc

1 (E)  Local PRMRY (E)    2    2880   57
1 (E)  Remote SCNDRY (E)       4860   13   128.185.452.11
2 (D)  Local PRMRY (D)    1    0      0
2 (D)  Remote PRMRY (D)        0      0    128.185.450.31
```

Group Number

Indicates the group number and the status of the group, enabled (E) or disabled (D).

Port Status

Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).

Net Number

Indicates the device number of the local port. This number matches the number displayed using the `Config>` **list devices** command.

Packets (fwrd and disc)

Indicates how many packets were forwarded (fwrd) and discarded (disc) for that port.

IP Address

Indicates the IP address of the remote port.

group *group#*

Displays the configurations of a specified group.

Example:

```
list group 1
             SDLC Relay Configuration

Group  Port Status        Net  Packets    IP Address
Num                      Num  fwrd disc

1 (E)  Local PRMRY (D)    2    2880   57
1 (E)  Remote SCNDRY (E)       4860   13  128.185.452.11
```

SDLC Relay Interfaces and the GWCON Interface Command

While SDLC Relay interfaces have their own monitoring processes for monitoring purposes, the router also displays complete statistics for installed network interfaces when you use the **interface** command from the GWCON environment. (For more information on the **interface** command, refer to Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands.)

Chapter 32. Using SDLC Interfaces

This chapter how to use the SDLC interface and includes the following sections:

- "Basic Configuration Procedure"
- "Configuring Switched SDLC Call-In Interfaces"
- "SDLC Configuration Requirements" on page 460

You enter SDLC configuration commands at the `SDLC # Config>` prompt, where # identifies the interface you specify with the network command. Changes made to the routers configuration do not take effect immediately, but become part of the router's static configuration memory when it is restarted.

Basic Configuration Procedure

This section outlines the minimum configuration required for SDLC to be usable by DLSw or by APPN.

Before beginning any configuration procedure, use the **list device** command from the config process to list the interface numbers of different devices. At the config prompt, select the interface you want to configure by entering either: **network** *interface number* or **n** *interface number*. If you need any further configuration command explanations, refer to the configuration commands described in this chapter.

Configuring Switched SDLC Call-In Interfaces

A switched SDLC call-in interface allows a PU type 2.0 device to dial into a 2212 using a switched SDLC line, providing an additional connectivity option to your network. The interface is restricted to PU type 2.0 devices and can run DLSw only.

Note: You cannot configure APPN over a switched SDLC call-in interface.

To configure a switched SDLC call-in interface:

1. Configure a V.25bis base network:

```
Config> set data-link v25bis 2
Config> net 2
V25bis Config>
 (configure the V25bis net)
```

   See "Chapter 36. Using the V.25bis Network Interface" on page 499 for more information about configuring V25bis.

   Note: Any physical layer parameters such as the **encoding type** and **full** vs. **half duplex** are configured on the V.25bis interface and not on the Switched SDLC dial circuit interface.

2. Add a dial circuit device:

```
Config> add device dial
```

3. Set the data link for the dial circuit interface to SDLC. In this example, the dial circuit is interface 3.

```
Config> set data-link sdlc 3
```

4. Configure the dial circuit:

```
Config> net 3
Dial circuit config> set net 2 1
Dial circuit config> encapsulator
sdlc config>
   (configure SDLC)
sdlc config> exit
Dial circuit config> exit
Config>
```

5. Configure DLSw:

```
Config> prot dls
DLSw protocol user configuration
DLSw config> add sdlc
Interface # [0]? 3
SDLC Address or 'sw' (switched dial-in) [sw]? sw 2
Source MAC address [4000112402C1]? 4000003174d2
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000004 3
Destination SAP in hex [0]? 4 4

XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
For a switched dial-in link station .....
  - PU type is forced to be 2
  - Configured XID block/id num is used to override
     fields in the XID0 from the SDLC station
      - if block/id set to zeroes, XID0 is not modified
      - otherwise configured fields are put into XID0
  - Poll type is not configured (not used)
DLSw config>li sdlc all
Net Addr   Status    Source SAP/MAC   Dest SAP/MAC      PU  Blk/IdNum  PollFrame
 3  FF(sw) Enabled   04 4000003174D2  04 400000000004   2   017/00001  TEST

DSLw config> exit
Config>
```

1 You will not be able to set any other dial circuit parameters as the software will take defaults for all other parameter values. For information about the defaults, see “Encapsulator” on page 564.

2 Specifying “sw” indicates that this is a switched SDLC call-in interface.

3 The destination MAC address cannot be all 0s. If you specify or default to a value of 0, the software will prompt you for a valid address.

4 The destination SAP cannot be 0. If you specify or default to a value of 0, the software will prompt you for a valid address.

See the “Using and Configuring DLSw” and the “Monitoring DLSw” chapters of *Protocol Configuration and Monitoring Reference Volume 1* for additional information about configuring DLSw.

SDLC Configuration Requirements

In addition to the SDLC-specific configuration procedures and commands described in this chapter, you need to configure SDLC in the DLSw or APPN protocol. Only one protocol at a time, DLSw or APPN, may run over a given SDLC interface. In other words, link stations on a given SDLC interface cannot be divided between APPN and DLSw. If a DLSw configuration and an APPN configuration exist for the same SDLC interface, the first protocol to come active will own the SDLC interface.

Chapter 33. Configuring and Monitoring SDLC Interfaces

This chapter describes the SDLC configuration and operational commands.

This chapter includes the following sections:

Changes made at the configuration command console (`SDLC CONFIG>`) become part of the SRAM configuration when you restart the router.

Conversely, SDLC monitoring commands entered within the SDLC monitoring process take effect immediately. However, changes made with monitoring commands do not become part of the router's static configuration. When the router is restarted, the effects of the monitoring commands are overwritten by the router's static configuration. Monitoring consists of these actions:

- Monitoring the protocols and network interfaces that are currently in use by the router
- Making real-time changes to the SDLC configuration without permanently affecting the SRAM configuration
- Displaying ELS (Event Logging System) messages relating to router activities and performance

Accessing the SDLC Configuration Environment

Use the CONFIG process to change the configuration of the router. The new configuration takes effect when the router is restarted.

To enter the configuration process:

1. Enter **talk 6** (or **t 6**), at the OPCON (*) prompt. This brings you to the `CONFIG>` prompt as shown in the following example:

   ```
   MOS Operator Control

   * talk 6

   CONFIG>
   ```

   If the `CONFIG>` prompt does not appear immediately, press the **Enter** key again. All SDLC configuration commands are entered at the `SDLC config>` prompt.

2. At the `Config>` prompt, enter the **set data-link sdlc** command. When prompted, enter the name of the interface to associate with the SDLC device.

   ```
   Config>set data-link sdlc
   Interface number [0]? 2
   Config>
   ```

3. Next, enter the **network** command, plus the number of an SDLC interface that you entered earlier.

   ```
   Config>network 2
   SDLC 2 Config>
   ```

Refer to “Chapter 1. Getting Started” on page 3 for information related to the configuration environment.

SDLC Configuration Commands

The SDLC configuration commands allow you to create or modify the SDLC interface configuration. This section summarizes and describes the commands you can issue from the `SDLC Config>` prompt within the network configuration console. Defaults for any command and its parameters are displayed on the console, they are enclosed in brackets immediately following the prompt.

Note: In addition to configuring SDLC using the commands described in this chapter, you also need to configure SDLC in the DLSw or APPN protocol.

2212 supports SDLC connections over RS-232, X.21, and V.35 serial interfaces. Table 53 lists SDLC configuration commands and their function.

Table 53. SDLC Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Add	Adds an SDLC end station.
Delete	Removes an SDLC end station.
Disable	Prevents connections to one of the SDLC link stations.
Enable	Allows connections to one of the SDLC link stations.
List	Displays configured information for one of the SDLC link stations.
Set	Configures specific interface and link-station information.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Add

Use the **add** command to add an end station. The router is, by default the primary end station. If you do not use this command and if you configured an SDLC station in DLSw or in APPN, the end station is added for you. The software assigns the following defaults to the station:

- Maximum BTU is maximum allowable by the interface
- Tx and Rx Windows are 7 for MOD 8, 127 for MOD 128

If the defaults are satisfactory, you do not need to add SDLC station.

Syntax:

add station

Example:

```
add station
Enter station address (in hex) [C3]?
Enter station name [SDLC_C3]?
Include station in group poll list ([Yes] or No):
Enter max packet size [2009]?
Enter receive window [7]?
Enter transmit window [7]?
```

Enter station address

The station’s SDLC address in the range 01 - FE.

Enter station name
The name designation of the SDLC station (maximum characters is 8).

Include station in group poll list
Select whether or not to include this station in the group poll list for this link. The SDLC software supports the IBM 3174 group poll function for SDLC secondary station. You must add a group poll address using the **set link group-poll** command for this parameter to have an affect.

Enter max packet size
The maximum packet size that can be sent to or received from the remote link station. This value cannot be greater than that specified for the link. This value is configured with the **set link frame-size** command.

Enter receive window
The maximum number of packets that the router can receive without sending a response.

Enter transmit window
The maximum number of packets that the router can transmit without receiving a response.

Delete

Use the **delete** command to remove the specified end station (station name or address) from the SDLC configuration. The router is considered the primary end station (default).

Syntax:

delete station *name* or *address*

Disable

Use the **disable** command to prevent connections from being created with a SDLC link station.

Syntax:

disable link
station . . .

link Prevents the transmitting and receiving of data to all configured SDLC link stations on the interface.

station *name* **or** *address*
Prevents the transmitting and receiving of data to the specified end station (station name or address).

Enable

Use the **enable** command to enable connections to remote SDLC link stations.

Syntax:

enable link
station

link Allows subsystems in the router (for example, DLSw) to use SDLC's facilities.

station *name* **or** *address*
Allows connections to the specified secondary remote end station (link station name).

List

Use the **list** command to display configuration information on one or all SDLC link stations.

Syntax:

list link
station *name* or all

link Displays the SDLC interface's configuration.

Example:

```
list link
Link configuration for: LINK_2   (ENABLED)

Role:          SECONDARY        Type:        POINT-TO-POINT
Duplex:        FULL             Modulo:      8
Idle state:    FLAG             Encoding:    NRZ
Clocking:      EXTERNAL         Frame Size:  2048
Speed:         0                Group Poll:  F3
Cable          V.36 DTE

Timers:     XID/TEST response:  2.0 sec
            SNRM response:      2.0 sec
            Poll response:      0.5 sec
            Inter-poll delay:   0.2 sec
            Inter-frame delay:  DISABLED
            Leading flags:  DISABLED
            Inactivity timeout  30.0 sec

 Counters:  XID/TEST retry:  8
             SNRM retry:      6
             Poll retry:      10
```

Link configuration
The name and status of SDLC link station that are in the router's configuration.

Role The primary, secondary, or negotiable role for link stations that you configure using the **set link role** command.

Type The type of link, MULTIPOINT or POINT-TO-POINT.

Duplex
Duplex configuration, HALF or FULL.

Modulo
The sequence number range to use on the link: MOD 8 (0-7) or MOD 128 (0 - 127).

Idle state
The bit pattern (FLAG or MARK) transmitted on the line when the interface is not transmitting data.

Speed The physical data rate of the interface. When the clocking is internal, this is the data rate generated by the internal clock.

Group Poll
Address used for the group poll feature for multipoint link configurations. Secondary stations having group inclusion coded as yes will respond to unnumbered polls received from this address. This address must be non-null for the group poll feature to be in effect for any secondary stations under this link. Each secondary station will still have a unique station address in addition to the group address.

Cable Specifies the type of cable in use (RS-232, V.35, V.36, or X.21).

Encoding
Configures the SDLC transmission encoding scheme as NRZ (Non-Return to Zero) or NRZI (Non-Return to Zero Inverted).

Clocking
Interface clocking, EXTERNAL or INTERNAL.

Frame Size
The maximum frame size that can be sent over the interface.

Timers:
All the timers listed below have a 100ms resolution.

XID/TEST resp.
The time to wait for an XID or TEST response message before retransmitting the XID or TEST frame. A value of 0 indicates that the router will continue to retry indefinitely.

SNRM response
The maximum time to wait for an UA response message before the station retransmits SNRM(E).

Poll response
The maximum time to wait for a response from any polled station before retrying.

Inter-poll delay
The amount of time the router (configured with a primary role) waits after receiving a response, before polling the next station.

Interframe delay
The number of flags sent between frames.

Leading Flags
The number of flags sent if the interframe delay is not sufficient for a response to the device on the other end of this link.

Inactivity timeout
For idle NRM/E secondary stations, sets the time after which the interface changes the station to its recovery state. A 0 (zero) causes the station to remain idle indefinitely.

Counters:

XID/TEST retry
The maximum number of times the router sends an XID or TEST frame without receiving a response before timing out. A value of 0 indicates that the router will retry indefinitely.

SNRM The maximum number of times the router will send an SNRM(E) frame without receiving a response before timing out. A value of 0 indicates that the router will retry indefinitely.

Poll retry
The maximum number of times the router polls the station without receiving a response before timing out. A value of 0 indicates that the router will continue to retry indefinitely.

Note: Physical layer parameters such as **duplex type**, **speed**, **cable type**, **encoding**, **clocking**, **leading flags**, and **inter-frame delay** do not apply for SDLC dial circuit interfaces and are not displayed by the **list link** command.

station *all* **or** *address* **or** *link station name*
Displays information for the specified SDLC link station or for all link stations.

Example:

```
list station c1
 Address   Name     Status   Max BTU   Rx Window   Tx Window
 -------  ------    ------   -------   ---------   ---------
 C1(00)  SDLC_C1    Enabled     2005         7           7
```

Example:

```
list station all
 Address   Name      Status     Max BTU  Rx Window  Tx Window
 -------  --------  ----------  -------  ---------  ---------
 C1(00)   SDLC_C1     ENABLED      2005        7          7
 C3(F3)   SDLC_C3     DISABLED     2009        7          7
```

Address
The address of the SDLC link station. The address in parentheses is the group address of the station. A (00) indicates that a group address is not defined.

Name The character string name designation of SDLC link station.

Status
The status of the SDLC link station, ENABLED or DISABLED.

Max BTU
The frame size limit of the station. This frame size must not be larger than the maximum Basic Transmission Unit (BTU) packet size configured with the **set link frame-size** command.

Rx Window
The size of the receive window.

Tx Window
The size of the transmit window.

Set

Use the **set** command to configure specific information for one or all SDLC link stations.

Syntax:

set
- link cable*
- link clocking*
- link duplex* . . .
- link encoding* . . .
- link frame-size
- link group poll* ...

link idle* . . .

link inactivity ...

link inter-frame delay*

link leading flags*

link modulo . . .

link name

link poll . . .

link role* . . .

link snrm

link speed*

link type* . . .

link xid/test

station *address* . . .

***Note:** These commands are not available for SDLC dial circuit interfaces.

link cable *type*

Sets the cable connected to this interface. The options are V.36 and the following DCE and DTE types: RS-232, V.35, and X.21.

A DTE cable is used when you are attaching the router to some type of DCE device (for example, a modem or a DSU/CSU).

A DCE cable is used when the router is acting as the DCE and providing the clocking for direct attachment.

link clocking *internal* **or** *external*

Configures the SDLC link's clocking. To connect to a modem or DSU, set clocking external. To connect directly to another DTE device, use a DCE cable, set the clocking to internal, and configure the clock speed.

link duplex *full* **or** *half*

Configures the SDLC line for *full-duplex* or *half-duplex* signalling. *Half-duplex* means that the 2212 raises RTS and expects to see CTS before it will transmit data. *Full-duplex* means that the 2212 does not wait for CTS to be raised before is transmits data.

Note: The duplex type does not control how SDLC operates at the SDLC protocol level. The 2212 only supports two-way alternating mode which is sometimes also referred to as SDLC half-duplex.

link encoding *nrz* **or** *nrzi*

Configures the SDLC transmission encoding scheme as NRZ (Non-Return to Zero) or NRZI (Non-Return to Zero Inverted). NRZ is the default.

link frame-size

Configures the maximum size of the frames that can be transmitted and received on the data link. Valid entries are shown in Table 54.

Table 54. Valid Values for Frame Size in Link Frame-Size Command

Minimum	Maximum	Default
262	8187	2048

Set the link frame size greater than the maximum packet size that you configured with the **set station xxx max packet** command. Otherwise, the router automatically resets the maximum packet size to the link frame size and issues the following ELS message:

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

Example: set link frame-size

```
Frame size in bytes (262 - 8187)[2048]?
```

link group-poll

Sets a group poll address for secondary stations on the link. The SDLC software supports the IBM 3174 group poll function. Use the **add station** or the **set station group inclusion** command to include a station in the group poll list.

Example:

```
set link group-poll
Enter group poll address (in hex) [00:]?f3
Group poll support enabled
```

link idle flag

Configures the transmit idle state for SDLC framing. The default is the flag option which provides continuous flags (7E) between frames.

Example: `set link idle flag`

The link will receive a flag idle transparently.

link idle mark

Configures the transmit idle state for SDLC framing. The mark option puts the line in a marking state (OFF, 1) between frames.

link inactivity *#-of-seconds*

For idle NRM/E secondary stations, sets the time after which the interface changes the station to its recovery state. The range is 0 to 7200 seconds. The default is 30. A 0 (zero) causes the station to remain idle indefinitely.

Example:

```
set link inactivity
Enter secondary link station inactivity timeout :[30.0]?
```

link inter-frame delay *seconds*

Allows the insertion of a delay between transmitted packets. This command ensures a minimum delay between frames for compatibility with older, slower serial devices at the other end. This parameter is the amount of time between frames in seconds.

Valid values: 0 to 120

Default value: 0

Example:

```
set link inter-frame delay
Transmit Delay Counter [0]?
```

link modulo 8 or 128

Specifies the sequence number range to use on the link: MOD 8 (0-7) or MOD 128 (0 - 127). Default is 8.

Note: When you change this value, the window sizes become invalid. Use the **set station** command to change the receive window and transmit window sizes. Valid window sizes for mod 8 are 0 through 7; for mod 128 they are 8 through 127.

Also, at connection start-up, an SNRME rather than a SNRM is used and supervisory frame headers are expanded by an additional byte.

link name

Establishes a character string for the link that you are configuring. This parameter is for informational purposes only.

Example:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay

Configures the time delay between each poll that is sent over the interface.

Example:

```
set link poll delay
Enter delay between polls [0.2]?
```

link poll retry

Configures the number of times the interface retries to poll the secondary SDLC link station before it closes the connection.

Example:

```
set link poll retry
Enter poll retry count (0 = forever) [10]?
```

link poll timeout

Configures the amount of time the interface waits for a poll response before timing out.

Example:

```
set link poll timeout
Enter poll timeout [2.0]?
```

link role *primary* **or** *secondary* **or** *negotiable*

Configures the interface as an SDLC primary, secondary, or negotiable link station (default is primary).

Notes:

1. For DLSw, ***negotiable*** uses X'FF' (broadcast address) for the initial poll.

   When using broadcast address to negotiate the role, the link uses a default SDLC configuration.

   When ***primary*** is the link role, the link performs an initial poll to a specific address.
2. For APPN point-to-point or negotiable, the broadcast address is used for the initial poll. For primary multipoint, the specific address is used.
3. For switched SDLC, the device must be primary, so **link role type** is not configurable for SDLC dial circuit interfaces.

link snrm *timeout* **or** *retry*

Configures the following SNRM(E) information for primary stations:

timeout
: The time to wait for an Unnumbered Acknowledgements (UA) response before retransmitting an SNRM(E).

retry
: The number of times to retransmit an SNRM(E) without receiving a response before giving up.

Example:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

Example:

```
set link snrm retry
Enter SNRM retry count (0=forever) [6]?
```

link speed

For internal clocking, this command specifies the speed of the transmit and receive clock lines.The supported range is 2400 to 2048000 bps.

- interface 1.
- port 1 of a 4-port WAN concentration adapter.
- ports 1 and 5 of an 8-port WAN concentration adapter.

If you want to use a line speed greater than 2048000, you can only do this on port 1 of the system card's integrated WAN ports and all other integrated WAN ports must be clocked at 64 Kbps or less.

Example:

```
set link speed
Line Speed [64000]?
```

link type *multipoint* **or** *point-to-point*

Configures the SDLC link to either a multipoint link or a point-to-point link.

Note: For switched SDLC, the link is always point-to-point, so **link type** is not configurable for SDLC dial circuit interfaces.

link xid/test *timeout* **or** *retry*

Configures the following XID/test information for primary stations:

timeout
The maximum amount of time to wait for an XID or TEST frame response before retransmitting the XID or TEST frame.

retry The maximum number of times an XID or TEST frame is resent before giving up. A 0 (zero) causes the router to retry indefinitely.

remote-secondary *address* **or** *link_station_name address* **<***argument***>**

Changes the remote station's SDLC address in the range 02 - FE.

Example: `set remote-secondary SDLC_C1 address ce`

station *address* **or** *name* **address**

Changes the station's SDLC address in the range 01 to FE.

Example:

```
set station c1 address
Enter station address (in hex) [C1]?
```

station *address* **or** *link station name* **group-inclusion** *no* **or** *yes*

For SDLC secondary stations, set whether to include this station in the group poll list for this link. For this to be effective, add a group poll address using the **set link group-poll** command.

Example: `set station c1 group-inclusion yes`

station *address* **or** *name* **max-packet**

The maximum size of the packet that the station can receive (default: 2048). Do not set the maximum packet size larger than the link frame size that is configured with the **set link frame-size** command; if you do, the router automatically resets the maximum packet size to the link frame size and issues the following ELS message:

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

Example:

```
set station c1 max-packet
Enter max packet size [2048]?
```

station *address* **or** *name* **name**
The name of the SDLC station.

Example:

```
set station c1 name
Enter station name [SDLC_C1]?
```

station *address* **or** *name* **receive window**
The maximum number of frames the router can receive before sending a response. The range is 1 to 7. The default is 7.

Example:

```
set station c1 receive-window
Enter receive window [7]?
```

station *address* **or** *name* **transmit-window**
The maximum number of frames the router can transmit before receiving a response frame. The range is 1 to 7. The default is 7.

Example:

```
set station c1 transmit-window
Enter transmit window [7]?
```

Accessing the SDLC Monitoring Environment

The monitoring environment is the GWCON process. To enter the GWCON process:

1. Enter **talk 5** (or **t 5**) at the OPCON (*) prompt. This brings you to the GWCON (+) prompt as shown in the following example:

   ```
   MOS Operator Control

   * talk 5
   +
   ```

2. Next, enter the **network** # command using the number that identifies the interface that you previously configured for the SDLC device.

   ```
   + network 2
   SDLC Console
   SDLC-2>
   ```

You enter all GWCON (Monitoring) commands at the + prompt.

Refer to “Chapter 1. Getting Started” on page 3 for information related to the monitoring environment.

SDLC Monitoring Commands

This section summarizes and then explains the SDLC console and related commands. Use these commands to gather information from the database. Table 55 lists SDLC monitoring commands and their function.

Table 55. SDLC Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.

Table 55. SDLC Monitoring Commands Summary (continued)

Command	Function
Add	Adds an SDLC link station
Clear	Clears the counters on the SDLC interface.
Delete	Dynamically removes an SDLC link station.
Disable	Disables connections to one SDLC link station.
Enable	Enables connections to one SDLC link station.
List	Displays SDLC link stations configurations and link station information.
Set	Configures specific interface and link station information.
Test	Tests the link between the router and the SDLC link station.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Add

Use the **add** command to add an end station. The router is, by default the primary end station. If you do not use this command and if you configured an SDLC station in DLSw or APPN, the end station is added for you.

Syntax:

add station

For an example and for additional information on the **add** command, see “Add” on page 462 .

Clear

Use the **clear** command to clear counters for the interface, for a station, or for all stations. Use the **list all stations** command to list stations.

Syntax: clear link

station ...

link *name* **or** *address*
Clears the counters for an SDLC interface.

station *name* **or** *address* **or all**
Clears counters for a specific station or for all stations.

Delete

Use the **delete** command to terminate an existing SDLC connection without affecting the SDLC configuration in SRAM. This command terminates any SDLC session that may be in progress on the link station. The router is considered the primary end station by default.

Syntax:

delete station *name* or *address*

Disable

Use the **disable** command to disable connection establishment on one or all SDLC link stations without affecting the SDLC configuration in SRAM. The **disable** command also terminates any existing connection to the station.

Syntax: disable
link

station . . .

link Prevents connection on all configured SDLC link stations on the interface by terminating all connections.

station *name* **or** *address*
Prevents connection to the specified end station (link station name) by terminating any existing connection.

Enable

Use the **enable** command to enable connection establishment with remote SDLC link stations without affecting the SDLC configuration SRAM.

Syntax:

enable link

station . . .

link Allows subsystems (for example, DLSw) to use SDLC's facilities.

station *name* **or** *address*
Allows connections to the specified end station.

List

Use the **list** command to display statistics specific to the data link layer and the interface.

Syntax:

list link configuration

link counters

station . . .

link configuration
Displays information for all configured SDLC link stations on the interface.

For an example and for additional information on the **list** command, see "List" on page 464.

link counters Displays information for the SDLC counters since the last router restart or the last clear counters.

I-Frames
Total number of Information frames received and transmitted.

I-Bytes
Total number of Information bytes received and transmitted.

Re-Xmit
Total number of frames that were retransmitted.

UI-Frames
Total number of Unnumbered Information frames received and transmitted.

UI-Bytes
Total number of Unnumbered Information bytes received and transmitted.

RR Total number Receive-Ready (RRs) received and transmitted.

RNR Total number Receive-Not-Ready (RNRs) received and transmitted.

REJ Total number of Rejects received and transmitted.

UP Unnumbered Polls (group poll) received and transmitted.

station *all* **or** *address* **or** *link station name*

Displays the status of the specified SDLC link station or all stations. The software displays an * next to the stations that were not explicitly configured using the **add station** command but were added to the configuration because they were defined and activated in the protocol layer (DLSw or APPN).

Displays information for the specified SDLC link station (link station name) on the interface.

Address
The address of the SDLC link station. The address in parentheses is the group address of the station. A (00) indicates that a group address is not defined.

Name The character string name designation of SDLC link station.

Status
The status of the SDLC link station:

Enabled
Enabled, but not allocated

Idle Allocated, but not in use

Connected
Connected

Disconnected
Disconnected

Connecting
Connection establishment in progress.

Discnectng
Disconnection in progress

Recovering
Attempting to recover from a temporary data link error.

Max BTU
The frame size limit of the remote station. This frame size must not be larger than the maximum Basic Transmission

Unit (BTU) packet size configured with the **set link frame-size** command. The default is 2048 bytes.

Rx Window
The size of the receive window.

Tx Window
The size of the transmit window.

station *name* **or** *address* **counters**
Displays frame transmit and receive counts for the specified link station.

I-Frames
Number of information frames received and transmitted

I-Bytes
Number of information bytes received and transmitted

Re-Xmit
Number of frames retransmitted

UI-Frames
Number of Unnumbered Information frames received and transmitted

UI-Bytes
Number of Unnumbered Information bytes received and transmitted

XID-Frames
Number of Exchange Identification frames received and transmitted

RR Number of Receive Ready frames received and transmitted

RNR Number of Receive Not Ready frames received and transmitted

REJ Number of Rejects received and transmitted

TEST Number of Test frames received and transmitted

SNRM Number of Set Normal Response Mode frames received and transmitted

DISC Number of Disconnect frames received and transmitted

UA Number of Unnumbered Acknowledgment frames received and transmitted

DM Number of Disconnected Mode frames received and transmitted

FRMR Number of Frame Reject frames received and transmitted

UP Unnumbered Polls (group poll) received and transmitted.

Example:

```
list link counters
     I-Frames     I-Bytes     Re-Xmit     UI-Frames     UI-Bytes
     --------     -------     -------     ---------     --------
Send       0           0           0             0            0
Recv       0           0                         0            0

          RR        RNR        REJ           UP
```

```
     -------      ------       ----       ---------
Send       0           0          0                0
Recv       0           0          0                0
```

Example:

```
list station all

Address    Name      Status    Max BTU   Rx Window     Tx Window
--------   -----     ------    -------   ---------     ---------
 C1(00)    SDLC_C1   IDLE        2048       7            7
 C2(F3)    SDLC_C2   ENABLED     2048       7            7
```

Example:

```
list station c1
Address   Name      Status     Max BTU     Rx Window   Tx Window
-------  ------    --------    -------     ---------   ---------
* C1(00) SDLC_C1    ENABLED       2048         7           7
```

Example:

```
list station c1 counters
         I-Frames    I-Bytes     Re-Xmit   UI-Frames    UI-Bytes   XID-Frames
        ----------  ----------  ---------  ----------  ----------  ----------
 Send            9         384          0           0           0           6
 Recv           29       42792                      0           0           3

            RR          RNR        REJ        TEST        SNRM        DISC
        ----------  ----------  ---------  ----------  ----------  ----------
 Send          598           0          0           0           1           0
 Recv          587           0          0           0           0           0

            UA          DM         FRMR       UP
        ----------  ----------  ---------  ---------
 Send            0           0          0          0
 Recv            1           0          0          0
```

Set

Use the **set** command to dynamically configure specific information for one or all SDLC link stations without affecting the SRAM configuration. In the SDLC monitoring environment, the **set** command can be executed only on disabled links or stations. All time values are entered in seconds, with a 0.1 second resolution.

Syntax:

set

- link modulo . . .
- link name
- link poll . . .
- link role* . . .
- link type* . . .
- link xid/test
- station . . .

***Note:** These commands are not supported on SDLC dial circuit interfaces.

link modulo

Dynamically changes the range of sequence numbers to be used on the data link without affecting the SRAM configuration. Modulo 8 specifies a sequence number range 0 - 7, and modulo 128 specifies 0 - 127. Default is 8.

Note: When you change this value, the transmit and receive window sizes become invalid. Use the **set station** command to change the receive-window and transmit-window sizes.

link name

Dynamically changes the name of the link without affecting the SRAM configuration. A maximum of 8 characters can be entered. This parameter is for informational purposes only.

Example:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay or timeout or retry

Dynamically changes the following poll information without affecting the SRAM configuration.

delay Configures the delay between each poll that is sent over the interface.

timeout
Configures the amount of time the router waits for a poll response before timing out.

retry Configures the number of times the interface retries to poll the remote SDLC link station before it closes the connection.

Example:

```
set link poll delay
Enter delay between polls [0.2]?
```

link role *primary*, *secondary*, **or** *negotiable*

Configures the interface as an SDLC primary, secondary, or negotiable link station. The default is primary. Use of this command does not affect the SRAM configuration.

Notes:

1. For DLSw, ***negotiable*** uses X'FF' (broadcast address) for the initial poll.

   When using broadcast address to negotiate the role, the link uses a default SDLC configuration.

   When ***primary*** is the link role, the link performs an initial poll to a specific address.
2. For APPN point-to-point or negotiable, the broadcast address is used for the initial poll. For primary multipoint, the specific address is used.
3. For switched SDLC, the device must be primary, so **link role type** is not configurable for SDLC dial circuit interfaces.

link snrm *timeout* **or** *retry*

For primary stations, dynamically changes the following SNRM(E) information without affecting the SRAM configuration.

timeout
The time to wait for an Unnumbered Acknowledgment (UA) response before retransmitting an SNRM(E).

retry The number of times to retransmit an SNRM(E) without receiving a response before giving up.

Example:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

link type multipoint or point-to-point
Dynamically changes the SDLC link to either a multipoint link or a point-to-point link without affecting the SRAM configuration.

Note: For switched SDLC, the link is always point-to-point, so **link type** is not configurable for SDLC dial circuit interfaces.

link xid/test *timeout* **or** *retry*
For primary stations, dynamically changes the following XID/test information without affecting the SRAM configuration.

timeout
The maximum amount of time to wait for an XID or TEST frame response before retransmitting the test frame.

retry The maximum number of times an XID or TEST frame is resent before giving up. A 0 (zero) causes the router to retry indefinitely.

Note: Examples for, and explanations of, the following parameters can be found in the SDLC configuration chapter at “Set” on page 466.

station *address* **or** *name* **address**
Changes the station’s SDLC address.

station *address* **or** *name* **max-packet**
Maximum size of packet that this station can receive.

station *address* **or** *name* **name**
Name of the SDLC station.

station *address* **or** *name* **receive-window**
Maximum number of frames router sends before responding.

station *address* **or** *name* **transmit-window**
Maximum number of frames router transmits before receiving a response frame.

Test

Transmits a specified number of TEST frames to the specified station and waits for a response. Use this command to test the integrity of the connection. Press any key to cancel the test.

Note: Disable the specified link station before using this command

Syntax:

test station *name* or *address #frames-to-send frame-size*

Example:

```
test station c1
Number of frames to send [1]? 5
Frame length [265]?
Starting echo test -- press any key to abort
5 frames sent, 5 frames received, 0 compare errors, 0 timeouts
```

Number of test frames to send
Total number of frames to send.

Frame length
Length of frames to be sent. Frame length cannot be larger than the maximum frame length of the specified station.

The test may be aborted by pressing any key.

SDLC Interfaces and the GWCON Interface Command

While the SDLC interface has a console process for operational purposes, the 2212 also displays complete statistics for installed interfaces when you use the **interface** command from the GWCON environment. (For more information on the interface command, refer to “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 111.)

Statistics Displayed for SDLC Interfaces

Using the **interface** command, you can display statistics for SDLC devices without entering the SDLC monitoring process. To do this, enter the **interface** command and an interface number at the + prompt.

Nt Indicates the interface number as assigned by software during initial configuration.

Nt′ Indicates the interface number as assigned by software during initial configuration.

Note: For SDLC interfaces, the Nt' interface number is always the same as the Nt interface number.

Slot Indicates the slot number of the interface that is running SDLC.

Port Indicates the port number of the interface that is running SDLC.

Self-test passed
Indicates the total number of times the SDLC interface passed its self-test.

Self-test failed
Indicates the total number of times the SDLC interface was unable pass its self-test.

Maintenance failed
Indicates the number of maintenance failures.

The following parameters are displayed only if a cable is connected. The information displayed depends on the cable that is connected. Different parameters are displayed with other cables.

Adapter cable
Indicates the type of adapter cable that the level converter is using.

V.24 circuit
Indicates the circuits being used on the V.24.

Nicknames
Indicates the signals being used on the V.24 circuit.

RS-232
The EIA 232 (RS 232) circuit names.

State Indicates the state of V.24 circuits, signals, and pin assignments (ON or OFF).

Line speed (configured)
Indicates the currently configured line speed for the SDLC interface.

Last port reset
Indicates how long ago the port was last reset.

Input frame errors
Indicates the input frame error type (CRC error, too short, aborted, alignment, too long, DMA/FIFO overrun) and the total number of errors that have occurred.

Output frame counters
Indicates the total number of DMA/FIFO overruns and output aborts sent for output frames.

Missed frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the Last and First bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the `L & F bits not set` counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the `L & F bits not set` counter will be affected by traffic.

Chapter 34. Using Binary Synchronous Relay (BRLY)

This chapter describes how to use the Binary Synchronous Relay (BRLY) protocol. It includes the following sections:

- "BRLY Overview"
- "BRLY Considerations" on page 484

Binary Synchronous Relay (BRLY) is a protocol that encapsulates binary synchronous communications (BSC) traffic and transmits the traffic across IP connections. This function permits BSC traffic to flow between BSC peers as if a BSC connection exists between the peers. The following sections describe BRLY, some common configurations, and how to configure a BRLY scenario.

BRLY Overview

BSC connections are similar to SDLC connections in that they consist of a primary end-point (polling) and a secondary end-point (polled). The connections can be either point-to-point, where the primary communicates with a single secondary, or multipoint, where the primary communicates with multiple secondaries. BRLY supports both physical and virtual multipoint connections.

In this implementation, the primary and secondary BSC devices are connected to routers which then connect to each other through IP. Figure 27 is a diagram of a point-to-point and a physical multipoint BRLY configuration. A physical multipoint connection is one where all of the secondary devices are on the same physical connection.

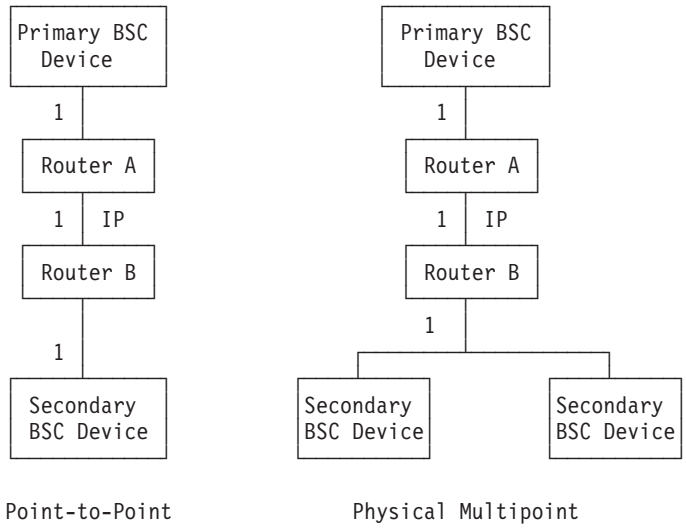

Figure 27. Physical BSC Relay Configurations. The numbers in the figure represent the group numbers for BSC Relay.

A virtual multipoint connection connects a single BSC primary and multiple BSC secondaries by using different BRLY groups (different physical connections). Figure 28 on page 482 is a diagram of a virtual multipoint configuration.

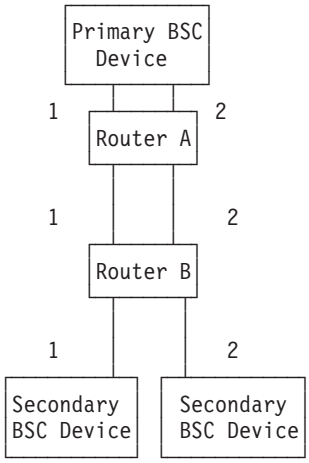

Figure 28. Virtual BSC Relay Multipoint Configuration. The numbers in the figure represent the group numbers for BSC Relay.

BSC Relay also supports a combination of virtual and physical multipoint connections. Figure 29 is a diagram of a combination of virtual and physical multipoint connections.

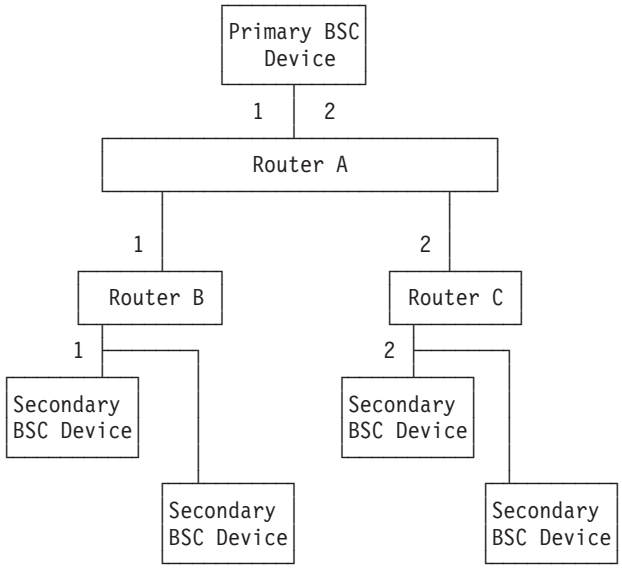

Figure 29. Combination Virtual and Physical BRLY Multipoint Configuration. The numbers in the figure represent the group numbers for BSC Relay.

Sample BRLY Configuration

The following examples illustrate configuring a BRLY network similar to the network in Figure 29. These examples use the following assumptions:

- Interface 1 on Routers A, B, and C have already been configured as BSC interfaces.
- The IP address for the Primary BSC Device's local port is 6.6.6.4.
- The IP address for the Router B's Secondary BSC devices local port is 6.6.6.1.
- The IP address for the Router C's Secondary BSC devices local port is 6.6.6.2.

```
Config>protocol brly
BSC Relay protocol user configuration
BRLY config>add group 1
Local group number: [1]?
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]?
Interface number: [0]? 1
(P)rimary or (S)econdary: [S]? p
Does this interface communicate with multiple remote groups [N]? y
BRLY config>add remote
Local group number: [1]?
IP address of remote router: [0.0.0.0]? 6.6.6.1
Remote router group number: [1]?
(P)rimary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c1
BRLY config>li all
                    BSC Relay Configuration


 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  -----------------  ------  ------  -------   ---------------
  1 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             1      C1      6.6.6.1

 E = enabled, D = disabled

BRLY config>add group 2
Local group number: [1]? 2
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]? 2
Interface number: [0]? 1
(P)rimary or (S)econdary: [S]? p
Does this interface communicate with multiple remote groups [N]? y
BRLY config>add remote
Local group number: [1]? 2
IP address of remote router: [0.0.0.0]? 6.6.6.2
Remote router group number: [1]? 2
(P)rimary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c5
BRLY config>li all
                     BSC Relay Configuration


 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  -----------------  ------  ------  -------   ---------------
  1 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             1      C1      6.6.6.1

  2 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             2      C5      6.6.6.2

 E = enabled, D = disabled
```

Figure 30. BRLY Configuration for Router A (Commands entered at Router A)

Notes:

1. The configuration for group 1 starts at 1.
2. The configuration for group 2 starts at 2.

```
BRLY config>add group
Local group number: [1]?
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]?
Interface number: [0]? 1
(P)rimary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c1
BRLY config>add remote
Local group number: [1]?
IP address of remote router: [0.0.0.0]? 6.6.6.4
Remote router group number: [1]?
(P)rimary or (S)econdary: [S]? p
BRLY config>li all

                    BSC Relay Configuration


 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  ----------------  ------  ------  -------   ---------------
  1 (E)  MULTI  Local  SCNDRY (E)     1             C1
                Remote  PRMRY (E)            1             6.6.6.4

 E = enabled, D = disabled
```

Figure 31. BRLY Configuration for Router B (Commands entered at Router B)

```
BRLY config>add group
Local group number: [1]? 2
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]? 2
Interface number: [0]? 1
(P)rimary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c5
BRLY config>add remote
Local group number: [1]? 2
IP address of remote router: [0.0.0.0]? 6.6.6.4
Remote router group number: [1]? 2
(P)rimary or (S)econdary: [S]? p
BRLY config>li all

                    BSC Relay Configuration


 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  ----------------  ------  ------  -------   ---------------
  2 (E)  MULTI  Local  SCNDRY (E)     1             C5
                Remote  PRMRY (E)            2             6.6.6.4

 E = enabled, D = disabled
```

Figure 32. BRLY Configuration for Router C (Commands entered at Router C)

BRLY Considerations

When configuring BRLY, keep the following in mind:

- Enabling BRLY will result in an increase of polling in the network which will reduce the total network throughput.
- BSC devices automatically disconnect if their inactivity timer expires. By default, this occurs after three seconds. An extremely busy network could result in BSC devices that disconnect frequently.

Chapter 35. Configuring and Monitoring BSC Relay

This chapter describes the binary synchronous communications (BSC) Relay configuration and operational commands. It also includes a procedure for configuring a BSC interface.

The chapter includes the following sections:

Basic Configuration Procedure

This section outlines a procedure to configure a BSC interface and the BSC Relay protocol. Refer to the configuration commands that are described in this chapter for further configuration information and explanation.

To configure a BSC relay interface and run BRLY over that interface:

1. Configure an interface as a BSC interface.
   a. Enter **set data-link bsc** at the `Config>` prompt.
   b. Enter the interface number when prompted.
   c. Access the BSC interface configuration prompt:

      ```
      Config>network 2
      BSC interface user configuration
      BSC 2 Config>
      ```

   d. Display the current interface settings using the **list** command and change, if necessary, using the **set** command.
   e. Repeat until you have configured all of the BSC interfaces you need.
2. Configure the BRLY protocol.
   a. Access the BRLY protocol.

      ```
      Config>protocol brly
      BSC Relay protocol user configuration
      BSC Relay config>
      ```

   b. Add a group using the **add group** command.
   c. Add a local port using the **add local-port** command.
   d. Add a remote port using the **add remote-port** command. This identifies the port that is directly connected to the remote side of the serial line and specifies the IP address for the connection.
   e. Repeat steps 2.b through 2.d until you have configured all of the groups, local ports, and remote ports needed.

BSC Relay Configuration Commands

This section describes the BSC Relay configuration commands. This chapter describes both network and protocol parameters for BSC relay.

The BSC Relay configuration commands allow you to specify router parameters for interfaces that transmit BSC Relay frames. Restart the router to activate the

configuration commands. Table 56 shows the commands for both the network BSC and protocol BRLY.

Table 56. BSC Relay Configuration Commands Summary

Command	Network BSC	Protocol BRLY	Function
? (Help)	yes	yes	Lists all of the configuration commands or lists the options associated with specific commands.
Add		yes	Adds groups, local ports, and remote ports.
Delete		yes	Deletes groups, local ports, and remote ports.
Disable		yes	Disables groups and ports.
Enable		yes	Enables groups and ports.
List	yes	yes	Displays entire BSC Relay, group-specific, and interface configurations.
Set	yes		Sets the link parameters and remote station parameters.
Exit	yes	yes	Exits the BSC Relay configuration environment and returns to the CONFIG environment.

Add

Use the **add** command to add groups, local ports, and remote ports.

Syntax:

add group *group#*

local-port

remote-port

group *group#*

Defines a primary to secondary connection. Each different connection requires a different group number.

Example: `add group`

```
Group number: [1]? 1
Group type: [multipoint]
```

Group number

The group number that you are designating for the group.

Valid values: 1 to 16

Default value: 1

Group type

Specifies the type of BSC connection this group supports.

Valid values: point-to-point or multipoint

Default value: multipoint

local-port

Identifies the interface that you are using as the local port for a specific group. The local port is a connection to a BSC device that is connected directly to the 2212 you are configuring. The following example adds a primary local port.

Example: `add local–port`

```
Group number: [1]? 1
Interface number: [0]? 2
(P)rimary or (S)econdary:[S]? p
```

Group number
The group number for the port. This number must be configured previously using the **add group** command.

Interface number
The interface number of the router that designates the local port.

Primary or Secondary
Designates the port type, primary (P) or secondary (S).

Default value: S

Station Address Character
Specifies the character that the system displays for a secondary port. You will be prompted for this only if you configure the local port as a secondary.

Valid values: X'01' to X'FF'

Default value: None

Note: This value is used for display purposes only and identifies a group of secondaries.

remote–port
Identifies the IP address of the port that is directly connected to the serial line on the remote (peer) router. The following example shows the configuration of a remote port as a secondary.

Example: `add remote–port`

```
Group number: [1]? 1
IP address of remote router:[0.0.0.0]? 128.185.121.97
(P)rimary or (S)econdary:[S]? s
Remote group number: [1]? 2
Station address character? cd
```

Group number
The group number for the port. This number must be configured previously using the **add group** command.

IP address of remote router
Identifies the IP address of the interface that communicates with the remote router.

Primary or Secondary
Designates the port type, primary (P) or secondary (S).

Remote group number
Specifies the group number for the remote port as it is defined at the remote router.

Station Address Character
Specifies the character that the system displays for a secondary port. You will be prompted for this only if you configure the local port as a secondary.

Valid values: X'01' to X'FF'

Default value: None

Note: This value is used for display purposes only and identifies a group of secondaries.

Delete

Use the **delete** command to remove groups, local ports, and remote ports.

Syntax:

delete group *group#*
local-port
remote–port

group *group#*
Removes a group (group#).

Example: `delete group 1`

local–port *group#*
Removes the local port for the specified group.

Example: `delete local–port`

```
Group number: [1]? 2
```

Group number
The group number for the local port.

remote–port
Removes the remote port for the specified group.

Example: `delete remote–port`

```
Group number: [1]? 1
```

Group number
The group number for the remote port.

Disable

Use the **disable** command to suppress relaying for an entire relay group or a specific relay port.

Syntax:

disable group *group#*
port

group *group#*
Suppresses transfer of BSC Relay frames to or from a specific local group.

Example: `disable group 1`

port Suppresses transfer of BSC Relay frames to or from a specific local or remote relay port.

Example: `disable port`

```
Group number: [1]? 2
Local or Remote:[local]? remote
```

Group number
The group number of the port that you want to disable.

Local or Remote
Specifies whether to disable the local or remote port.

Default value: local

Enable

Use the **enable** command to turn on data transfer for an entire relay group or a specific relay port.

Syntax:

enable group *group#*

port

group *group#*

Allows transfer of BSC Relay frames to or from the specified group.

Example: `enable group 1`

port Allows transfer of BSC Relay frames to or from the specified local port.

Example: `enable port`

```
Group number: [1]? 2
Local or Remote: [local]? remote
```

Group number

The group number of the port that you want to enable.

Local or Remote

Specifies whether to enable the local or remote port.

Default value: local

List (for network BSC)

Use the **list** command to display the configuration of a specific BSC interface.

Syntax:

list

Example:

```
list
Maximum frame size in bytes:  2048
Encoding:                     NRZI
Idle State:                   Sync
Clocking:                     Internal
Cable type:                   V.35 DCE
Speed (bps):                  2048000
Code:                         ASCII
Link EOT:                     No
Number of pairs of SYNs:      1
```

Maximum frame size in bytes

Maximum frame size that can be sent over the link. The maximum frame size must be large enough to accommodate the largest frame and the 15 byte BRLY header.

Encoding

The transmission encoding scheme for the serial interface. Scheme is NRZ (non-return to zero) or NRZI (non-return to zero inverted).

Idle State

The data link idle state: sync or mark.

Clocking

The type of clocking: internal, external.

Cable Type
The serial interface cable type.

Speed (bps)
Lists the speed of the transmit and receive clocks.

Code The code type used by this device.

Link EOT
Specifies whether EOT transmissions are combined with poll and select transmissions when the transmissions occur back-to-back.

Number of pairs of SYNs
The number of pairs of synchronization characters the system sends before any data.

List (for protocol BRLY)

Use the **list** command to display the configuration of a specific group or of all groups.

Syntax:

list all

group *group#*

all Displays the configurations of all groups.

Example: `list all`

```
              BSC Relay Configuration

 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  -----------------  ------  ------  -------   ---------------
  1 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             1      C1      6.6.6.1

  2 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             2      C5      6.6.6.2

 E = enabled, D = disabled
```

Note: The system does not display the remote port's net number at the local port as it is not part of the local group's configuration.

Group Number
Indicates the group number and the status of the group, enabled (E) or disabled (D).

Port Status
Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).

Net Number
Indicates the interface number of the local port.

Remote Group
The number of the group at the remote router.

Address Character
The address character assigned to one secondary station.

IP Address
Indicates the IP address of the remote port.

group *group#*
Displays the configuration of a specified group.

Set

Use the **set** command to configure the BSC interface parameters.

Syntax:

set cable
clocking [internal or external]
code [ebcdic or ascii]
encoding [nrz or nrzi]
eotlink [yes or no]
frame-size
idle [sync or mark]
speed *bps*
syns *number*

cable Sets the cable used on the serial interface. The options are:

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- X21 DTE
- X21 DCE

Use a DTE cable when you are attaching the router to some type of DCE device (for example, a modem or a DSU/CSU).

A DCE cable is used when the router is acting as the DCE and providing the clocking for direct attachment.

clocking [internal or **external]**
Configures the BSC link's clocking. To connect to a modem or DSU, configure clocking as external. To connect directly to another DTE device, use a DCE cable, set the clocking to internal, and configure the clock speed.

Example:

```
set clocking internal
```

code [ebcdic or **ascii]**
Specifies the code type that is used by this BSC device.

Default value: ebcdic

encoding [*nrz* **or** *nrzi***]**
Configures the BSC interface's encoding scheme as NRZ (Non-Return to Zero) or NRZI (Non-Return to Zero Inverted). NRZ is the default.

Example:

```
set encoding nrz
```

eotlink [yes or **no]**
Specifies whether to combine EOT transmissions with poll and select transmissions when the transmissions occur back-to-back.

Default value: yes

frame-size
Configures the maximum size of the frames that the system can transmit and receive on the data link. If this value is set to a value larger than the value specified with the **add remote-secondary** command, the system changes this value to reflect that maximum. The IBM 2212 generates an ELS message that warns the user. The user will continue receiving this ELS message until it is changed in the SRAM configuration. Valid entries are shown in Table 57.

Note: The frame size must be large enough to accommodate the largest frame that is received plus a 15-byte BRLY header.

Table 57. Valid Values for Frame Size in Set Frame-Size Command

Minimum	Maximum	Default
128	8190	2048

idle [sync or **mark]**
Specifies which character the system sends in between BSC data transmissions.

sync Specifies that the BSC synchronizing character is sent. (See the **syns** parameter.)

mark Specifies that the all ones bits character (X'FF') is sent.

Default value: mark

speed *bps*
For internal clocking, this command specifies the speed of the transmit and receive clock lines.The range of speed supported are 2400 to 2048000.

- interface 1.
- port 1 of a 4-port WAN concentration adapter.
- ports 1 and 5 of an 8-port WAN concentration adapter.

If you want to use a line speed greater than 2048000, you can only do this on port 1 of the system card's integrated WAN ports and all other integrated WAN ports must be clocked at 64 Kbps or less.

syns Specifies the number of pairs of SYN characters the system sends before any data. SYNs are the BSC synchronizing characters. (See the **idle** parameter.)

Accessing the BSC Relay Monitoring Environment

To monitor information that is related to the BSC Relay protocol, access the interface monitoring process by:

1. At the OPCON prompt, enter the **talk** command and the PID for GWCON. For example:

```
* talk 5
+
```

The system displays the GWCON prompt (+) on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.

2. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

```
+ configuration
```

See page 114 for more sample output from the **configuration** command.

3. Enter the **protocol BRLY** command. For example:

```
+ prot brly
BSC Relay>
```

The system displays the BSC Relay prompt on the console. You can then view information about the BSC Relay ports by entering the BSC Relay monitoring commands.

BSC Relay Monitoring Commands

This section summarizes, and then explains the BSC Relay monitoring commands. The BSC Relay monitoring commands allow you to view parameters for interfaces that transmit BSC Relay frames. The system displays the `BSC Relay>` prompt for all BSC Relay monitoring commands. Table 58 shows the commands.

Table 58. BSC Relay Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Clear	Clears BSC Relay statistics.
Disable	Suppresses groups and ports.
Enable	Turns on groups and ports.
List	Displays entire BSC Relay and group specific configurations.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Clear

Use the **clear** command to discard the BSC Relay statistics for all ports. The statistics include counters for packets forwarded, and packets discarded. The command clears local and remote port statistics that is gathered since the last time you restarted the router or cleared statistics.

Syntax:

clear

Example:

```
clear
Clear all port statistics? (Yes or No): Y
```

Disable

Use the **disable** command to suppress data transfer for an entire group or a specific relay port. SRAM (static read access memory) does not permanently store

the effects of the **disable** monitoring command. Therefore when you restart the router, the effects of this command are erased.

Syntax:

disable group *group#*

port

group *group#*
Suppresses transfer of BSC Relay frames to or from a specific group.

port Suppresses transfer of BSC Relay frames to or from a specific local or remote port.

Example:

```
disable port
Group number: [1]? 2
Local or Remote: [local]? remote
```

Group number
Indicates the group number of the port that you want to disable.

Local or Remote
Specifies whether to disable the local or remote port.

Default value: local

Enable

Use the **enable** command to turn on data transfer for an entire group or a specific local interface port. SRAM does not permanently store the effects of the **enable** monitoring command. Therefore when you restart the router, the effects of this command are erased.

Syntax:

enable group *group#*

port

group *group#*
Allows transfer of BSC Relay frames to or from the specified group.

port Allows transfer of BSC Relay frames to or from the specified local port.

Example:

```
enable port
Group number: [0]? 2
Local or Remote: [local]? remote
```

group number
Indicates the group number of the port that you want to enable.

Local or Remote
Specifies whether to disable the local or remote port.

Default value: local

List

Use the **list** command to display the configuration of a specific group or of all groups.

Syntax:

list all

group *group#*

all Displays the statistics of all local groups. See the **list group** command for a sample output.

group *group#*
Displays the statistics of a specified group.

Example:

```
list group 1
                        BSC Relay Configuration

  Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  -----------------  ------  ------  -------   ---------------
  1 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             1      C1     6.6.6.1

 Local port statistics:
   Packets forwarded =       0
   Packets discarded =       0

 Remote port statistics:
   Packets forwarded =       0
   Packets discarded =       0
```

Local Group
Indicates the group number and the status of the group, enabled (E) or disabled (D).

Group Type
Specifies the type of BSC connection this group supports: point-to-point or multipoint.

Port Status
Indicates the type of port (local/remote primary/secondary) and its status, enabled (E) or disabled (D).

Net Number
Indicates the device number of the local port.

Station Address
The character that the system displays for a secondary port.

IP Address
Indicates the IP address of the remote port.

Remote Group
The number of the group at the remote router.

Packets Forwarded
Indicates how many packets the system forwarded for the port.

Packets Discarded
Indicates how many packets the system discarded for the port.

The following example displays the configuration built for Router A in the figure for “Sample BRLY Configuration” on page 482.

Configuring and Monitoring BSC Relay

```
Ctrl-P
* talk 5
+p brly
BSC Console
BSC>li all

                        BSC Relay Configuration


 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  -----------------  ------  ------  -------   ---------------
  1 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             1      C1      6.6.6.1

 Local port statistics:
   Packets forwarded =       0
   Packets discarded =       0

 Remote port statistics:
   Packets forwarded =       0
   Packets discarded =       0


 Local   Group        Port          Net    Remote  Station         IP
 Group   Type        Status        Number  Group   Address       Address
 ------  -----  -----------------  ------  ------  -------   ---------------
  2 (E)  MULTI  Local   PRMRY (E)     1
                Remote SCNDRY (E)             2      C5      6.6.6.2

 Local port statistics:
   Packets forwarded =       0
   Packets discarded =       0

 Remote port statistics:
   Packets forwarded =       0
   Packets discarded =       0



 E = enabled, D = disabled

BSC>exit
```

BSC Relay Interfaces and the GWCON Interface Command

While BSC Relay interfaces have their own monitoring processes, the router also displays complete statistics for installed network interfaces when you use the **interface** command from the GWCON environment. (For more information on the **interface** command, refer to Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands.)

Chapter 36. Using the V.25bis Network Interface

The V.25bis interface allows routers to establish serial connections over switched telephone lines using V.25bis modems. This chapter describes how to use the V.25bis interface. It includes the following sections:

- "Before You Begin"
- "Configuration Procedures"

Notes:

1. You can assign a destination name to a **connection list** and assign a destination number to each line in the list. When that destination name is called, the numbers in the list are tried one by one until a connection is made or the list is exhausted.
2. V.25bis is supported only on the 8-port EIA 232 adapter.

Before You Begin

Before you configure V.25bis on the router, make sure you have the following:

- V.25bis modems that support synchronous V.25bis commands and the 1988 ITU/CCITT V.25bis specification.
- If your modem does not automatically detect answer originate, you must:
  - Configure the modem at one end of the link to originate calls.
  - Configure the modem at the other end of the link to answer calls.
  - Set up the modem on the answering end to auto-answer.

Configuration Procedures

This section describes how to configure your router for V.25bis. The tasks you need to perform are:

1. Adding V.25bis addresses
2. Configuring V.25bis parameters
3. Adding dial circuits
4. Configuring dial circuits

Note: You must restart the router for changes to the V.25bis configuration to take effect.

Adding V.25bis Addresses

You need to add a V.25bis address for each local V.25bis interface as well as for each destination. The V.25bis address includes:

- *Address Name.* The address name is a description of the address. You can use any string of up to 23 printable ASCII characters.
- *Network Dial Address.* Telephone number of the local or destination port. You can enter up to 30 characters that are in the valid format of the connected V.25bis modem. For additional information consult your modem manual.

  Note: The valid character set for telephone numbers as defined by the CCITT and supported by the IBM 2212 includes:

- The decimal digits 0 through 9
- Colon (:) — ″Wait Tone″
- Left-angled bracket (<) —″Pause″, used for inserting a fixed delay (dependent on modem) between digit sequences. For example, when going through a PBX or PTN.
- Equal (=) — ″Separator 3″, which is ″for national use.″ (Consult your modem manual.)
- The letter P — ″Dialing to be continued in Pulse mode.″ (Not supported by some modems.)
- The letter T — ″Dialing to be continued in DTMF mode.″ (Not supported by some modems.)

To add a V.25bis address, enter the **add v25-bis-address** command at the Config> prompt. For example:

```
Config>add v25-bis-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-30 digits][]? 19095551234
```

Configuring the V.25bis Interface

This section explains how to configure the V.25bis interface. To configure, do the following:

1. To set up a serial line interface for V.25bis, set the data-link protocol for the serial line interface. From the Config> prompt, use the **set data-link v25bis** command. For example:

   ```
   Config>set data-link v25bis
   Interface Number [0]? 2
   ```

2. Display the V.25bis Config> prompt by entering the **network** command followed by the number of the interface. For example:

   ```
   Config>network 2
   V.25bis Data Link Configuration
   V25bis Config>
   ```

   You can use the **list devices** command at the Config> prompt to display a list of interface numbers configured on the router.

3. Use the **set local-address** command to specify the network address name of the local port. You must enter one of the address names you defined using the **add v25bis-address** command. For example:

   ```
   V25bis Config>set local-address
   Local network address name  []? remote-site-baltimore
   ```

Note: You must restart the router for configuration changes to take effect.

Optional V.25bis Parameters

The following are optional V.25bis parameters you can set. For a complete description of these commands, see “V.25bis Configuration Commands” on page 503 .

- You can limit the number of successive calls to an address that is inaccessible or that refuses those calls. To do so, use the **set retries-no-answer**and the **set timeout-no-answer** commands.
- The **set disconnect-timeout** command controls the amount of time the router waits to initiate a call after dropping a signal from the previous call.

- The **set command-delay-timeout** command specifies the amount of time the router waits to initiate or answer a call after it turns on DTR.
- The **set connect-timeout** command specifies the number of seconds allowed for a call to be established.
- The **set duplex** command specifies the duplexing mode for the call.
- The **set encoding** command sets the encoding for the call.
- When you have finished configuring the interface, you can use the **list** command to display your configuration.

Adding Dial Circuits

Dial circuits are mapped to V.25bis serial line interfaces. You can map multiple dial circuits to one serial line interface.

To add a dial circuit, use the **add device dial-circuit** command from the `Config>` prompt. The software assigns an interface number to each circuit. You will use this number to configure the dial circuit.

Example:

```
Config>add device dial-circuit
Adding device as interface 6
```

Note: Dial circuits default to the Point-to-Point protocol (PPP). You can also set the dial circuit to use Frame Relay (FR) or SDLC.

Configuring Dial Circuits

This section describes how to configure a dial circuit. For a complete description of the dial circuit commands, see “Chapter 42. Configuring and Monitoring Dial Circuits” on page 563.

Note: If the encapsulator type is SDLC, the only dial circuit parameter that you can set is the base net number.

To configure the dial circuit, do the following:

1. Display the `Circuit Config>` prompt by entering the **network** command followed by the interface number of the dial circuit. You can use the **list devices** command at the `Config>` prompt to display a list of the dial circuits that you added. For example:

   ```
   Config>network 6
   Circuit configuration
   Circuit Config>
   ```

2. Map the dial circuit to a V.25bis interface. The Base net is the V.25bis interface number. For example:

   ```
   Circuit Config>set net
   Base net for this circuit [0]?  0
   ```

3. Specify the address name of the remote router to which the dial circuit will connect. You must use one of the names you defined using the **add v25-bis-address** command. For example:

   ```
   Circuit Config>set destination
   Assign destination address name []? newyork
   ```

4. Configure the dial circuit to initiate outbound calls only, accept inbound calls only, or both initiate and accept calls.

   Use the **set calls** command. To avoid a conflict if both ends of the link attempt to establish a call at the same time, configure the dial circuit at one end of the

link to accept inbound calls only, and configure the dial circuit at the other end of the link to initiate outbound calls only. For example:

```
Circuit Config>set calls outbound
Circuit Config>set calls inbound
```

Note: For WAN Restoral operations or another dial-on-demand application, you should set up the circuit for either inbound or outbound calls.

5. Specify the timeout period for the circuit.

   Use the **set idle** command. If there is no traffic over the circuit for this specified time period, the dial circuit hangs up. To configure the circuit as a dedicated circuit, set the idle timer to zero. To configure the circuit to dial on demand, set the idle timer to a value other than zero. The range is 0 to 65535 and the default is 60 seconds. For example:

   ```
   Circuit Config>set idle
   Idle timer (seconds, 0 means always active) [60]? 0
   ```

   Note: For WAN Restoral or WAN Reroute operations you must set the idle time to 0.

6. Optionally, you can delay the time between when a call is established and the initial packet is sent.

   Use the **set selftest-delay** command. Setting a selftest delay can prevent initial packets from being dropped. If your modems take extra time to synchronize, adjust this delay. For example:

   ```
   Circuit Config>set selftest-delay
   Selftest delay(milli-seconds,0 means no delay)[150]?200
   ```

7. Set the inbound address name.

   Use the **set inbound** command. You need to use this command only if you set up the circuit for both inbound and outbound calls and if the router's destination address is different from the destination address that the remote router dials. For example, the numbers would be different if one of the routers must go through a PBX, international, or inter-LATA exchange. For example:

   ```
   Circuit Config>set inbound
   Assign destination inbound address name []? newyork
   ```

   The inbound address name must match one of the names that you defined using the **add v25-bis-address** command.

8. Set the duplexing mode for the circuit using the **set duplex** command.
9. Set the encoding mode for the circuit using the **set encoding** command.
10. Optionally, you can enter the configuration process for the data-link layer protocol that is running on the dial circuit (PPP or Frame Relay). Use the **encapsulator** command. For example:

    ```
    Circuit Config>encapsulator
    ```

Chapter 37. Configuring and Monitoring the V.25bis Network Interface

This chapter describes the V.25bis configuration and operational commands and GWCON commands. It includes the following sections:

Accessing the Interface Configuration Process

Use the following procedure to access the V.25bis configuration process.

1. At the OPCON prompt, enter the **talk** command and the PID for CONFIG. (For more detail on this command, refer to Chapter 3. The OPCON Process.) For example:

   ```
   * talk 6
   Config>
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter **CONFIG**, press **Return** again.
2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.
3. Record the interface numbers.
4. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

   ```
   Config> network 1
   V.25bis Config>
   ```

   The V.25bis configuration prompt now displays on the console.

V.25bis Configuration Commands

Table 59 summarizes and the rest of the section explains the V.25bis configuration commands. These commands allow you to display, create, or modify a V.25bis configuration. Enter the V.25bis configuration commands at the `V.25bis Config>` prompt.

Table 59. V.25bis Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
List	Displays the V.25bis configuration.
Set	Sets the local address, connect, disconnect, and no answer timeouts, number of retries after no answer, the duplexing mode, command delay timeout, and encoding.

Table 59. V.25bis Configuration Commands Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

List

Use the **list** command to display the current V.25bis configuration.

Syntax:

list

Example:

```
list
          V.25bis Configuration

Duplex                        =  Full
Encoding                      =  NRZ
Local Network Address Name    = v403
Local Network Address         = 15088982403

Non-Responding addresses:
Retries             = 1
Timeout             = 0 seconds

Call timeouts:
Command Delay       = 0 ms
Connect             = 60 seconds
Disconnect          = 2 seconds

Cable type          = V.35 DTE
Speed               = 9600
```

Duplex
Displays the duplex mode for the interface once the dial connection has been established.

Encoding
Displays the transmission encoding scheme for the interface once the dial connection has been established. Encoding is either NRZ (non-return to zero) or NRZI (non-return to zero inverted).

Local Network Address Name:
Displays the network address name of the local port.

Local Network Address:
Displays the network dial address of the local port.

Non-responding addresses:

Retries
Maximum number of calls the router attempts to make to a non-responding address during the timeout period.

Timeout
If the router reaches the maximum number of retries to a non-responding address, it does not attempt to establish the call until this time has expired. This timeout period begins when the router attempts the first call.

Call timeouts:
Number of call timeouts.

Command Delay
Amount of time, in milliseconds, that the router waits to initiate or answer a call after it turns on DTR (Data Terminal Ready). If you set this parameter to 0, the router waits for the modem to respond to DTR with the CTS (Clear to Send) signal before it issues commands.

Connect
Number of seconds allowed for a call to be established. If this parameter is set to 0, the modem controls the connection establishment timeout.

Disconnect
After the routers drops DTR it waits this amount of time before it initiates further calls. If you set this parameter to 0, the router waits for the modem to respond to the DTR drop by dropping CTS and DSR before it initiates the next call.

Set

Use the **set** command to configure local addresses, timeouts and delays for calls, retries and timeouts for non-responding addresses, and the HDLC cable type.

Syntax:

set command-delay timeout . . .
connect-timeout . . .
disconnect-timeout . . .
duplex
hdlc cable . . .
hdlc encoding . . .
hdlc speed . . .
local-address . . .
retries-no-answer . . .
timeout-no-answer . . .

command-delay-timeout *# of milliseconds*
After the router turns on DTR (Data Terminal Ready), it waits this amount of time before it initiates or answers a call. If you set this parameter to 0, the router waits for the modem to respond to DTR with the CTS (Clear to Send) signal before it issues commands. The range is 0 to 65535 milliseconds, and the default is 0.

connect-timeout *# of seconds*
Sets the number of seconds allowed for a call to be established. The range is 0 to 65535 seconds, and the default is 60. If you set this parameter to 0, the modem controls the connection timeout. You should initially set this parameter to 0 and then use ELS event V25B.027 to find out how long it takes to establish connections to various destinations. You can then set this parameter to a number slightly higher than the longest connect time.

Note: Normally government regulation limits modem manufacturers to a maximum length for call setup. This value is merely an optimization, although inter-operation with some DSUs may require that you change this parameter.

disconnect-timeout *# of seconds*

Specifies the amount of time, in seconds, that the router waits after dropping DTR before it initiates further calls. The range is 0 to 65535 seconds, and the default is 2. If you set this parameter to 0, the router waits for the modem to respond to the DTR drop by dropping CTS and DSR before it initiates the next call.

duplex

Specifies the duplex type of the line.

When full-duplex is configured, the RTS modem signal remains asserted once the dial connection has been established.

When half-duplex is configured, the router raises RTS when it is time to transmit and waits for CTS to be asserted by the modem. After CTS is asserted, the router transmits data packets and then drops RTS when the router is through transmitting to let the peer device respond.

Only configure half-duplex when using the V.25bis interface to handle switched SDLC and the attached modem requires the half-duplex mode of operation.

Notes:

1. Duplex must be full for PPP or Frame Relay circuits.

Valid values: full or half

Default value: full

hdlc cable *rs232 dte*

Specifies the type of cable connected to this interface. Setting this parameter allows you to view the cable type when you enter the **interface** command at the GWCON (+) prompt and when you enter the **statistics** command at the `V.25bis>` monitoring prompt. This parameter does not affect operation of the router.

hdlc encoding

Sets the HDLC transmission encoding scheme as NRZ (non-return to zero) or NRZI (non-return to zero inverted). Most configurations use NRZ. The configured encoding is used for the end-to-end connection.

Note: Although you might configure NRZI, the exchange between the DTE and the modem (as described by CCITT recommendation, *V.25bis*) uses NRZ as the encoding scheme.

Valid values: NRZ or NRZI

Default value: NRZ

hdlc speed

Specifies the line speed for this interface. Setting this parameter allows you to view the line speed when you enter the interface command at the GWCON (+) prompt and when you enter the statistics command at the `V.25bis>` monitoring prompt. The range is 2400 to 64 000 bps. The default is 9600 bps.

Note: This command does not affect the actual line speed but it sets the speed some protocols, such as IPX, use when calculating routing cost parameters for dial circuits mapped to the V.25bis interface.

local-address *address name*
Specifies the network address name of the local port. This address name must match one of the names that you defined at the `Config>` using the **add v25-bis-address** command.

Example: `set local-address line-1-local`

retries-no-answer *value*
Some telephone service providers impose restrictions on automatic recalling devices to limit the number of successive calls to an address that is inaccessible or that refuses those calls. This parameter specifies the maximum number of calls the router attempts to make to a non-responding address during the timeout period. The range is 0 to 10, and the default is 1.

Note: Government regulation may also impose limits on the modem manufacturer that would supersede this parameter.

timeout-no-answer *# of seconds*
After the router reaches the maximum number of **retries-no-answer** to a non-responding address, it does not initiate further calls to that address until this time has expired. This timeout period begins when the router attempts the first call to an address. The range is 0 to 65535 seconds, and the default is 0. If you set this parameter to 0, the modem controls the timeout period.

Accessing the Interface Monitoring Process

To access the interface monitoring process for V.25bis, enter the following command at the GWCON (+) prompt:

```
+ network #
```

Where # is the number of the V.25bis serial line. You cannot directly access the V.25bis monitoring process for dial circuits, but you can monitor the dial circuits that are mapped to the serial line interface.

Note: V.25bis interfaces also have ELS troubleshooting messages that you can use to monitor V.25bis related activity. See the *IBM Event Logging System Messages Guide* for further details.

V.25bis Monitoring Commands

This section summarizes and explains the V.25bis operating commands. These commands allow you to view the calls, circuits, parameters, and statistics of the V.25bis interfaces.

Enter the V.25bis monitoring commands at the `V.25bis>` prompt. Table 60 on page 508 shows the commands.

Table 60. V.25bis Monitoring Command Summary

Monitoring Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Calls	List the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.
Circuits	Shows the status of all data circuits configured on the V.25bis interface.
Parameters	Displays the current parameters for the V.25bis interface. (This command is similar to the `V.25bis Config>` list command.)
Statistics	Displays the current statistics for the V.25bis interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Calls

Use the **calls** command to list the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.

Syntax:

calls

Example:

```
calls
Net Interface  Site Name           In    Out   Rfsd  Blckd
1     PPP/0     v403               2      0      0      0

Unmapped connection indications:    0
```

Net Number of the dial circuit mapped to this interface.

Interface
Type of interface and its instance number.

Site Name
Network address name of the dial circuit.

In Number of inbound connections accepted for this dial circuit.

Out Number of completed connections initiated by this dial circuit.

Rfsd Number of connections initiated by this dial circuit that were refused by the network or the remote destination port.

Blckd Number of connection attempts that the router blocked. The router blocks connection attempts if the local port is already in use, the maximum number of retries to a non-responding address is reached, or a modem is not responding.

Unmapped connection indications:
Number of connection attempts that were refused by the router because there were no enabled dial circuits that were configured to accept the incoming calls.

Circuits

The **circuits** command shows the status of all dial circuits configured on the V.25bis port.

Syntax:

circuits

Example:

```
circuit
Net Interface  MAC/Data-Link    State     Reason      Duration
2   PPP/0      Point to Point   Avail     Rmt Disc     1:02:25
```

Net Number of the dial circuit mapped to this interface

Interface
Type of interface and its instance number.

MAC/DataLink
Type of datalink protocol configured for this dial circuit.

State Current state of the dial circuit:

Up - currently connected

Available - not currently connected, but is available

Disabled - dial circuit was disabled

Down - failed to connect because of a busy dial circuit or because the link-layer protocol is down

Reason
Reason for the current state:

nnn_Data - (where nnn is the name of a protocol) the circuit is Up because a protocol had data to send.

Remote Disconnect - the circuit is either Down or Available because the remote destination disconnected the call.

Operator Request - the circuit is Available because the last call was disconnected by a monitoring command.

Inbound - the circuit is Up because the circuit answered an inbound call.

Restoral - the circuit is Up because of a WAN Restoral operation.

Self Test - the circuit was configured as static (idle time=0) and successfully connected once it was enabled.

Duration
Length of time that the circuit has been in the current state.

Parameters

Use the **parameters** command to display the current V.25bis serial line configuration. Note that this is the same information displayed in the `V.25bis Config>` list command.

Syntax:

parameters

Example:

```
parameters
         V.25bis port Parameters

Local Network Address Name    = v402
Local Network Address         = 15088982402

Non-Responding addresses:
Retries             = 1
Timeout             = 0 seconds

Call timeouts:
Command Delay       = 0 ms
Connect             = 0 seconds
Disconnect          = 0 seconds
```

Local Network Address Name:
Network address name of the local port.

Local Network Address:
Network dial address of the local port.

Non-responding addresses:

Retries
Maximum number of calls the router attempts to make to a non-responding address during the timeout period.

Timeout
If the router reaches the maximum number of retries to a non-responding address, it does not attempt to establish the call until this time has expired. This timeout period begins when the router attempts the first call to an address.

Call timeouts:

Command Delay
Amount of time, in milliseconds, that the router waits to initiate or answer a call after it turns on DTR (Data Terminal Ready). If you set this parameter to 0, the router waits for the modem to respond to DTR with the CTS (Clear to Send) signal before it issues commands.

Connect
Number of seconds allowed for a call to be established. If this parameter is set to 0, the modem controls the connection establishment timeout.

Disconnect
After the routers drops DTR it waits this amount of time before it initiates further calls. If you set this parameter to 0, the router waits for the modem to respond to the DTR drop by dropping CTS and DSR before it initiates the next call.

Statistics

Use the **statistics** command to display the current statistics for this V.25bis interface.

Syntax:

statistics

Example:

```
statistics
         V.25bis port Statistics


  Adapter cable:               RS-232 DTE




   Nicknames:    RTS CTS DSR DTR DCD RI
   RS-232        CA  CB  CC  CD  CF  CE
   State:        OFF OFF OFF OFF OFF OFF

  Line speed:              4800
  Last port reset:         24 seconds ago

  Input frame errors:
   CRC error                     0   alignment (byte length)   0
   missed frame                  0   too long (>  2182 bytes)  0
   aborted frame                 0   DMA/FIFO overrun          0
   L & F bits not set            0
Output frame counters:
   DMA/FIFO underrun errors      0   Output aborts sent        0
```

Adapter cable:
Type of adapter cable being used.

Nicknames:
Common names for the circuits.

RS-232
EIA 232 (also known as RS-232) names for the circuits.

State: Current state of the circuits: ON, OFF, or ″---,″ which means that the state is undefined for this type of interface.

Line speed:
The transmit clock speed (approximate).

Last port reset:
Length of time since the port was reset.

Input frame errors:

CRC error
Number of packets received that contained checksum errors and as a result were discarded.

Alignment (byte length)
Number of packets received that were not an even multiple of 8 bits in length and as a result were discarded.

Missed Frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

too long (> nnnn bytes)
Number of packets received that were greater than the configured frame size (nnnn) and as a result were discarded.

aborted frame
Number of packets received that were aborted by the sender or a line error.

DMA/FIFO overrun
The number of times the serial interface card could not send data fast enough to the system packet buffer memory to receive packets from the network.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the L & F bits not set counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the L & F bits not set counter will be affected by traffic.

Output frame counters:

DMA/FIFO underrun errors
Number of times the serial interface card could not retrieve data fast enough from the system packet buffer memory to transmit packets onto the network.

Output aborts sent
Number of transmissions that were aborted as requested by upper-level software.

V.25bis and the GWCON Commands

While V.25bis has its own monitoring process for monitoring purposes, the router also displays configuration information and complete statistics for devices and circuits when you use the interface, statistics, and error commands from the GWCON environment. You can also use the GWCON **test** command to test DCEs and circuits.

Note: Issuing the **test** command to the V.25bis serial interface causes the current call to be dropped and re-dialed.

For more information on the GWCON command, see “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 111.

Statistics for V.25bis Interfaces and Dial Circuits

Use the **interface** command at the GWCON (+) prompt to display statistics for V.25bis serial line interfaces and dial circuits.

To display the following statistics for a V.25bis serial line interface, use the **interface** command followed by the *interface number* of the V.25bis serial line interface.

Example: `interface 10`

```
                                          Self-Test  Self-Test  Maintenance
Nt Nt'  Interface  Slot-Port              Passed     Failed     Failed
10 10   V.25/0     Slot: 4  Port: 0           1          0          0
  V.25bis Base Net MAC/data-link on EIA 232E/V.24 interface

  Adapter cable:             RS-232 DTE

   V.24 circuit: 105 106 107 108 109 125
   Nicknames:    RTS CTS DSR DTR DCD RI
```

```
 RS-232:       CA  CB  CC  CD  CF  CE
 State:        OFF OFF OFF ON  OFF OFF

Line speed:              19.200 Kbps
Last port reset:         55 minutes, 1 second ago

Input frame errors:
 CRC error                          6   alignment (byte length)           0
 missed frame                       1   too long (>  2054 bytes)          0
 aborted frame                     34   DMA/FIFO overrun                  0
Output frame counters:
 DMA/FIFO underrun errors           0   Output aborts sent                0
```

To display the following statistics for a dial circuit, use the **interface** command followed by the *interface number* of the dial circuit.

Example:

```
interface 29
                              Self-Test  Self-Test  Maintenance
Nt Nt'  Interface             Passed     Failed     Failed
29 10   PPP/20                     2          1          0
  Point to Point MAC/data-link on V.25bis Dial Circuit interface
```

The following list describes the output for both serial line interfaces and dial circuits.

Nt Serial line interface number or dial circuit interface number.

Nt′ If “Nt” is a dial circuit, this is the interface number of the V.25bis serial line interface to which the dial circuit is mapped.

Interface
Interface type and its instance number.

Slot The slot number of the interface running V.25bis.

Port The port number of the interface that is running V.25bis.

Self-Test Passed
Number of self-tests that succeeded.

Self-Test Failed
Number of self-tests that failed.

Maintenance: Failed
Number of maintenance failures.

Adapter cable:
Type of adapter cable that is being used.

V.24 circuit:
Circuit numbers as identified by V.24 specifications.

RS-232
EIA 232 (also known as RS-232) names for the circuits.

State Current state of the circuits (ON or OFF).

Line speed
The transmit clock speed (approximate).

Last port reset
Length of time since the port was reset.

Input frame errors:

CRC error
Number of packets received that contained checksum errors and as a result were discarded.

Alignment (byte length)
Number of packets received that were not an even multiple of 8 bits in length and as a result were discarded.

Missed Frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

too long (> nnnn bytes)
Number of packets received that were greater than the configured frame size and as a result were discarded.

DMA/FIFO overrun
The number of times the serial interface card could not send data fast enough to the system packet buffer memory to receive packets from the network.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the L & F bits not set counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the L & F bits not set counter will be affected by traffic.

aborted frame
Number of packets received that were aborted by the sender or a line error.

Output frame counters:

DMA/FIFO underrun errors
Number of times the serial interface card could not retrieve data fast enough from the system packet buffer memory to transmit packets onto the network.

Output aborts sent
Number of transmissions that were aborted as requested by upper-level software.

Chapter 38. Using the V.34 Network Interface

The V.34 interface allows routers to establish serial connections over switched telephone lines using externally attached modems that support the standard AT command set. This chapter describes how to use a V.34 interface. It includes the following sections:

- “Before You Begin”
- “Configuration Procedures”

Notes:

1. You can assign a destination name to a **connection list** and assign a destination number to each line in the list. When that destination name is called, the numbers in the list are tried one by one until a connection is made or the list is exhausted.
2. V.34 is supported only on the 8-port EIA 232 adapter.

Before You Begin

Before you configure V.34 on the router, make sure you have asynchronous modems that support the Hayes AT command set. Also, you must know the maximum DTE speed of each modem.

Configuration Procedures

This section describes how to configure your router for V.34. The tasks you need to perform are:

1. Adding V.34 addresses
2. Configuring V.34 parameters
3. Adding dial circuits
4. Configuring dial circuits

Note: You must restart the router for changes to the V.34 configuration to take effect.

Adding V.34 Addresses

A default V.34 address is created when V.34 interfaces are initially configured (called “default_address”). Dial circuits configured on the V.34 interface default to the same address allowing some dial-in applications to work without modification of the V.34 address.

You need to add a V.34 address (or modify the default_address) if you plan to use dial-out applications. The V.34 address includes:

- *Address Name.* The address name is a description of the address. You can use any string of up to 23 printable ASCII characters.
- *Network Dial Address.* Telephone number of the local or destination port. You can enter up to 31 characters that are in the valid dial characters for the connected modem.

  Note: The valid character set for telephone numbers as defined by the CCITT and supported by the IBM 2212 includes:

- The decimal digits 0 through 9
- Colon (:) – ″Wait Tone″
- Left-angled bracket (<) – ″Pause″, used for inserting a fixed delay (dependent on modem) between digit sequences. For example, when going through a PBX or PTN.
- Equal (=) – ″Separator 3″, which is ″for national use.″ (Consult your modem manual.)
- The letter P – ″Dialing to be continued in Pulse mode.″ (Not supported by some modems.)
- The letter T – ″Dialing to be continued in DTMF mode.″ (Not supported by some modems.)

V.34 addresses are not interface specific so they are added from the main Config> prompt. For example:

```
Config>add v34-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-20 digits][]? 1-909-555-1234
```

Configuring the V.34 Interface

This section explains how to configure the V.34 interface. To configure, do the following:

1. To set up a serial line interface for V.34, set the datalink protocol for the serial line interface. From the Config> prompt, use the **set data-link v34** command. For example:

   ```
   Config> set data-link v34
   Interface Number [0]? 2
   ```

2. Display the V.34 Config> prompt by entering the **network** command followed by the number of the interface. For example:

   ```
   Config>network 2
   V.34 Data Link Configuration
   V34 System Net Config    2>
   ```

   You can use the **list devices** command at the Config> prompt to display a list of interface numbers configured on the router.

3. Use the **set local-address** command to specify the network address name of the local port. You must enter one of the address names you defined using the **add v34-address** command. For example:

   ```
   V34 System Net Config   2>set local-address
   Local network address name  []? remote-site-baltimore
   ```

Note: You must restart the router for configuration changes to take effect.

Optional V.34 Parameters

The following are optional V.34 parameters you can set. For a complete description of these commands, see “V.34 Configuration Commands” on page 519.

- You can limit the number of successive calls to an address that is inaccessible or that refuses those calls. To do so, use the **set retries-no-answer**and the **set timeout-no-answer** commands.
- The **set disconnect-timeout** command controls the amount of time the router waits to initiate a call after dropping a signal from the previous call.
- The **set command-delay-timeout** command specifies the amount of time the router waits to initiate or answer a call after it turns on DTR.

- The **set connect-timeout** command specifies the number of seconds allowed for a call to be established.
- The **speed** command sets the maximum DTE speed for the modem.
- The **modem-init-string** command allows flexibility in modem configuration to accommodate user or external equipment requirements.
- When you have finished configuring the interface, you can use the **list** command to display your configuration.

Adding Dial Circuits

Dial circuits are mapped to V.34 serial line interfaces. You can map multiple dial circuits to one serial line interface.

The V.34 interface supports multiple types of dial circuits. To add a dial circuit use one of the following commands from the Config> prompt.

- **add device dial-circuit**

The software assigns an interface number to each circuit. You will use this number to configure the dial circuit.

Example:

```
Config> add device dial-circuit
Adding device as interface 6
```

Note: Dial circuits default to the Point-to-Point protocol (PPP). Although the **set data-link** command can be used to set the datalink of a dial circuit to Frame Relay, only PPP dial circuits are supported over V.34.

Configuring Dial Circuits

This section describes how to configure a dial circuit. For a complete description of the dial circuit commands, see “Chapter 42. Configuring and Monitoring Dial Circuits” on page 563. To configure the dial circuit, do the following:

1. Display the Circuit Config> prompt by entering the **network** command followed by the interface number of the dial circuit. You can use the **list devices** command at the Config> prompt to display a list of the dial circuits that you added. For example:

   ```
   Config>network 6
   Circuit configuration
   Circuit Config>
   ```

2. Map the dial circuit to a V.34 interface. The Base net is the V.34 interface number. For example:

   ```
   Circuit Config>set net
   Base net for this circuit [0]?  0
   ```

3. Specify the address name of the remote router to which the dial circuit will connect. You must use one of the names you defined using the **add v34-address** command. For example:

   ```
   Circuit Config>set destination
   Assign destination address name []? newyork
   ```

4. Configure the dial circuit to initiate outbound calls only, accept inbound calls only, or both initiate and accept calls.

   Use the **set calls** command. To avoid a conflict if both ends of the link attempt to establish a call at the same time, configure the dial circuit at one end of the link to accept inbound calls only, and configure the dial circuit at the other end of the link to initiate outbound calls only. For example:

```
Circuit Config>set calls outbound
Circuit Config>set calls inbound
```

Note: For WAN Restoral operations or another dial-on-demand application, you should set up the circuit for either inbound or outbound calls.

5. Specify the timeout period for the circuit.

   Use the **set idle** command. If there is no traffic over the circuit for this specified time period, the dial circuit hangs up. To configure the circuit as a dedicated circuit, set the idle timer to zero. To configure the circuit to dial on demand, set the idle timer to a value other than zero. The range is 0 to 65535 and the default is 60 seconds. For example:

   ```
   Circuit Config>set idle
   Idle timer (seconds, 0 means always active) [60]? 0
   ```

   Note: For WAN Restoral operations you must set the idle time to 0.

6. Optionally, you can delay the time between when a call is established and the initial packet is sent.

   Use the **set selftest-delay** command. Setting a self-test delay can prevent initial packets from being dropped. If your modems take extra time to synchronize, adjust this delay. For example:

   ```
   Circuit Config>set selftest-delay
   Selftest delay(milli-seconds,0 means no delay)[150]?200
   ```

7. Set the inbound address name.

   Use the **set inbound** command. You need to use this command only if you set up the circuit for both inbound and outbound calls and if the router's destination address is different from the destination address that the remote router dials. For example, the numbers would be different if one of the routers must go through a PBX, international, or inter-LATA exchange. For example:

   ```
   Circuit Config>set inbound
   Assign destination inbound address name []? newyork
   ```

   The inbound address name must match one of the names that you defined using the **add v34-address** command.

8. Optionally, you can enter the configuration process for the datalink layer protocol that is running on the dial circuit (PPP or Frame Relay). Use the **encapsulator** command. For example:

   ```
   Circuit Config>encapsulator
   ```

Chapter 39. Configuring and Monitoring the V.34 Network Interface

This chapter describes the V.34 configuration and operational commands and GWCON commands. It includes the following sections:

Accessing the Interface Configuration Process

Use the following procedure to access the V.34 configuration process.

1. At the OPCON prompt, enter the **talk** command and the PID for CONFIG. (For more detail on this command, refer to Chapter 3. The OPCON Process.) For example:

   ```
   * talk 6
   Config>
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter **CONFIG**, press **Return** again.
2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.
3. The V.34 interfaces are listed as "V.34 Base Net". Record the interface numbers of interfaces to configure.
4. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

   ```
   Config> network 1
   V.34 System Net Config >
   ```

   The V.34 configuration prompt now displays on the console.

V.34 Configuration Commands

Table 61 on page 520 summarizes and the rest of the section explains the V.34 configuration commands. These commands allow you to display, create, or modify a V.34 configuration. Enter the V.34 configuration commands at the `V.34 Config>` prompt.

Table 61. V.34 Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
List	Displays the V.34 configuration.
Set	Sets the local address, connect, disconnect, and no answer timeouts, number of retries after no answer, and command delay timeout.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

List

Use the **list** command to display the current V.34 configuration.

Syntax:

list

Example:

```
list
         V.34 System Net Configuration:

Local Network Address Name    = v403
Local Network Address         = 1-508-898-2403

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         = at&f&s1l1&d2&c1x3

Speed (bps)                   = 115200
```

Local Network Address Name:
Displays the network address name of the local port.

Local Network Address:
Displays the network dial address of the local port.

Non-responding addresses:

Retries
Maximum number of calls the router attempts to make to a non-responding address during the timeout period.

Timeout
If the router reaches the maximum number of retries to a non-responding address, it does not attempt to establish the call until this time has expired. This timeout period begins when the router attempts the first call.

Call timeouts:
Number of call timeouts.

Command Delay
Amount of time, in milliseconds, that the router waits to initiate or answer a call after it turns on DTR (Data Terminal Ready). If you

set this parameter to 0, the router waits for the modem to respond to DTR with the CTS (Clear to Send) signal before it issues commands.

Connect
Number of seconds allowed for a call to be established. If this parameter is set to 0, the modem controls the connection establishment timeout.

Disconnect
After the routers drops DTR it waits this amount of time before it initiates further calls. If you set this parameter to 0, the router waits for the modem to respond to the DTR drop by dropping CTS and DSR before it initiates the next call.

Modem strings:
Command strings sent to the attached modem.

Initialization string
This is the last AT command string sent to the modem during initialization (before a call is accepted or attempted). A default string is provided which should work for most modems.

Speed (bps)
This is the DTE speed. The default should work for most modems, but you may need to set the speed lower to operate properly or higher to achieve maximum data speeds supported by the modem.

Set

Use the **set** command to configure local addresses, timeouts and delays for calls, retries and timeouts for non-responding addresses, and the HDLC cable type.

Syntax:

set command-delay timeout . . .
connect-timeout . . .
disconnect-timeout . . .
speed . . .
local-address . . .
modem-init-string . . .
retries-no-answer . . .
timeout-no-answer . . .

command-delay-timeout *# of milliseconds*
After the router turns on DTR (Data Terminal Ready), it waits this amount of time before it initiates or answers a call. If you set this parameter to 0, the router waits for the modem to respond to DTR with the CTS (Clear to Send) signal before it issues commands. The range is 0 to 65535 milliseconds, and the default is 0.

connect-timeout *# of seconds*
Sets the number of seconds allowed for a call to be established. The range is 0 to 65535 seconds, and the default is 60. If you set this parameter to 0, the modem controls the connection timeout. You should initially set this parameter to 0 and then use ELS event V34B.027 to find out how long it

takes to establish connections to various destinations. You can then set this parameter to a number slightly higher than the longest connect time.

Note: Normally government regulation limits modem manufacturers to a maximum length for call setup. This value is merely an optimization, although inter-operation with some DSUs may require that you change this parameter.

disconnect-timeout *# of seconds*
Specifies the amount of time, in seconds, that the router waits after dropping DTR before it initiates further calls. The range is 0 to 65535 seconds, and the default is 2. If you set this parameter to 0, the router waits for the modem to respond to the DTR drop by dropping CTS and DSR before it initiates the next call.

speed *# bits per second*
Specifies the DTE speed in bits per second for the modem. You should try to use the maximum speed supported by the modem, although some modems may not autobaud properly at all supported speeds. If you suspect there is a problem, try a lower speed.

local-address *address name*
Specifies the network address name of the local port. This address name must match one of the names that you defined at the `Config>` using the **add v34-address** command.

modem-init-string *value*
This is an AT command string sent to the modem at the end of successful interface initialization. It can be used to tailor modem parameters for your application.

retries-no-answer *value*
Some telephone service providers impose restrictions on automatic recalling devices to limit the number of successive calls to an address that is inaccessible or that refuses those calls. This parameter specifies the maximum number of calls the router attempts to make to a non-responding address during the timeout period. The range is 0 to 10, and the default is 1.

Note: Government regulation may also impose limits on the modem manufacturer that would supersede this parameter.

timeout-no-answer *# of seconds*
After the router reaches the maximum number of **retries-no-answer** to a non-responding address, it does not initiate further calls to that address until this time has expired. This timeout period begins when the router attempts the first call to an address. The range is 0 to 65535 seconds, and the default is 0. If you set this parameter to 0, the modem controls the timeout period.

Accessing the Interface Monitoring Process

To access the interface monitoring process for V.34, enter the following command at the GWCON (+) prompt:

```
+ network #
```

Where # is the number of the V.34 interface. You cannot directly access the V.34 monitoring process for dial circuits, but you can monitor the dial circuits that are mapped to the serial line interface.

Note: V.34 interfaces also have ELS troubleshooting messages that you can use to monitor V.34 related activity. See the *IBM Event Logging System Messages Guide* for further details.

V.34 Monitoring Commands

This section summarizes and explains the V.34 monitoring commands. These commands allow you to view the calls, circuits, parameters, and statistics of the V.34 interfaces.

Enter the V.34 monitoring commands at the `V.34>` prompt. Table 62 shows the commands.

Table 62. V.34 Monitoring Command Summary

Monitoring Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Calls	List the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.
Circuits	Shows the status of all data circuits configured on the V.34 interface.
Reset	Clears connections and resets the interface.
Parameters	Displays the current parameters for the V.34 interface. (This command displays the same information as the interface configuration ″list″ command.)
Statistics	Displays the current statistics for the V.34 interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Calls

Use the **calls** command to list the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.

Syntax:

calls

Example:

```
calls
Net Interface  Site Name           In    Out   Rfsd  Blckd
1     PPP/0     v403               2      0      0      0

Unmapped connection indications:    0
```

Net Number of the dial circuit mapped to this interface.

Interface
Type of interface and its instance number.

Site Name
Network address name of the dial circuit.

In Number of inbound connections accepted for this dial circuit.

Out Number of completed connections initiated by this dial circuit.

Rfsd Number of connections initiated by this dial circuit that were refused by the network or the remote destination port.

Blckd Number of connection attempts that the router blocked. The router blocks connection attempts if the local port is already in use, the maximum number of retries to a non-responding address is reached, or a modem is not responding.

Unmapped connection indications:
Number of connection attempts that were refused by the router because there were no enabled dial circuits that were configured to accept the incoming calls.

Circuits

The **circuits** command shows the status of all dial circuits configured on the V.34 port.

Syntax:

circuits

Example:

```
circuit
Net Interface  MAC/Data-Link    State     Reason      Duration
2   PPP/0      Point to Point   Avail     Rmt Disc     1:02:25
```

Net Number of the dial circuit mapped to this interface

Interface
Type of interface and its instance number.

MAC/DataLink
Type of datalink protocol configured for this dial circuit.

State Current state of the dial circuit:

Up - currently connected

Available - not currently connected, but is available

Disabled - dial circuit was disabled

Down - failed to connect because of a busy dial circuit or because the link-layer protocol is down

Reason
Reason for the current state:

nnn_Data - (where nnn is the name of a protocol) the circuit is Up because a protocol had data to send.

Remote Disconnect - the circuit is either Down or Available because the remote destination disconnected the call.

Operator Request - the circuit is Available because the last call was disconnected by a monitoring command.

Inbound - the circuit is Up because the circuit answered an inbound call.

Restoral - the circuit is Up because of a WAN Restoral operation.

Self Test - the circuit was configured as static (idle time=0) and successfully connected once it was enabled.

Duration
Length of time that the circuit has been in the current state.

Parameters

Use the **parameters** command to display the current V.34 serial line configuration. Note that this is the same information displayed in the `V.34 Config>` list command.

Syntax:

parameters

Example:

```
parameters
         V.34 port Parameters

Local Network Address Name    = v402
Local Network Address         = 1-508-898-2402

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 0 seconds
Disconnect                    = 0 seconds

Modem strings:
Initialization string         = at&f&s1l1&c1x3
```

Local Network Address Name:
Network address name of the local port.

Local Network Address:
Network dial address of the local port.

Non-responding addresses:

Retries
Maximum number of calls the router attempts to make to a non-responding address during the timeout period.

Timeout
If the router reaches the maximum number of retries to a non-responding address, it does not attempt to establish the call until this time has expired. This timeout period begins when the router attempts the first call to an address.

Call timeouts:

Command Delay
Amount of time, in milliseconds, that the router waits to initiate or answer a call after it turns on DTR (Data Terminal Ready). If you set this parameter to 0, the router waits for the modem to respond to DTR with the CTS (Clear to Send) signal before it issues commands.

Connect
Number of seconds allowed for a call to be established. If this parameter is set to 0, the modem controls the connection establishment timeout.

Disconnect
After the routers drops DTR it waits this amount of time before it

initiates further calls. If you set this parameter to 0, the router waits for the modem to respond to the DTR drop by dropping CTS and DSR before it initiates the next call.

Statistics

Use the **statistics** command to display the current statistics for this V.34 interface.

Syntax:

statistics

Example:

```
statistics
         V.34 port Statistics
  Adapter cable:               RS-232 DTE

   V.24 circuit: 105 106 107 108 109 125 141

        Nicknames:    RTS CTS DSR DTR DCD RI
    RS-232        CA  CB  CC  CD  CF  CE
    State:        OFF OFF OFF OFF OFF OFF
   Line speed:              115.200 Kbps
   Last port reset:         24 seconds ago

 Input frame errors:
    CRC error                     0   alignment (byte length)   0
    missed frame                  0   too long (>  2182 bytes)  0
    aborted frame                 0   DMA/FIFO overrun          0
    L & F bits not set            0

 Output frame counters:
    DMA/FIFO underrun errors      0   Output aborts sent        0
```

Adapter cable:
Type of adapter cable being used.

Nicknames:
Common names for the circuits.

RS-232
EIA 232 (also known as RS-232) names for the circuits.

State: Current state of the circuits: ON, OFF, or ″---,″ which means that the state is undefined for this type of interface.

Line speed:
The transmit clock speed (approximate).

Last port reset:
Length of time since the port was reset.

Input frame errors:

CRC error
Number of packets received that contained checksum errors and as a result were discarded.

Alignment (byte length)
Number of packets received that were not an even multiple of 8 bits in length and as a result were discarded.

Missed Frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

too long (> nnnn bytes)
Number of packets received that were greater than the configured frame size (nnnn) and as a result were discarded.

aborted frame
Number of packets received that were aborted by the sender or a line error.

DMA/FIFO overrun
The number of times the serial interface card could not send data fast enough to the system packet buffer memory to receive packets from the network.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the L & F bits not set counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the L & F bits not set counter will be affected by traffic.

Output frame counters:

DMA/FIFO underrun errors
Number of times the serial interface card could not retrieve data fast enough from the system packet buffer memory to transmit packets onto the network.

Output aborts sent
Number of transmissions that were aborted as requested by upper-level software.

V.34 and the GWCON Commands

While V.34 has its own monitoring process for monitoring purposes, the router also displays configuration information and complete statistics for devices and circuits when you use the interface, statistics, and error commands from the GWCON environment. You can also use the GWCON **test** command to test DCEs and circuits.

Note: Issuing the **test** command to the V.34 serial interface causes the current call to be dropped and re-dialed.

For more information on the GWCON command, see “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 111.

Statistics for V.34 Interfaces and Dial Circuits

Use the **interface** command at the GWCON (+) prompt to display statistics for V.34 serial line interfaces and dial circuits.

To display the following statistics for a V.34 serial line interface, use the **interface** command followed by the *interface number* of the V.34 serial line interface.

Example:

```
interface 10
                                                  Self-Test  Self-Test  Maintenance
Nt Nt'  Interface  Slot-Port                      Passed     Failed     Failed
10 10   V.34/0     Slot: 4  Port: 0                   1          0          0

  V.34 Base Net MAC/data-link on EIA 232E/V.24 interface

  Adapter cable:             RS-232 DTE

   V.24 circuit: 105 106 107 108 109 125
   Nicknames:    RTS CTS DSR DTR DCD RI
   RS-232:       CA  CB  CC  CD  CF  CE
   State:        OFF OFF OFF ON  OFF OFF

  Line speed:              115.200 Kbps
  Last port reset:         55 minutes, 1 second ago

Input frame errors:
   CRC error                          6   alignment (byte length)            0
   missed frame                       1   too long (>  2054 bytes)           0
   aborted frame                     34   DMA/FIFO overrun                   0
Output frame counters:
   DMA/FIFO underrun errors           0   Output aborts sent               0
```

To display the following statistics for a dial circuit, use the **interface** command followed by the *interface number* of the dial circuit.

Example:

```
interface 29

                             Self-Test  Self-Test  Maintenance
Nt Nt'  Interface            Passed     Failed     Failed
29 10   PPP/20                    2          1          0

  Point to Point MAC/data-link on V.34 Dial Circuit interface
```

The following list describes the output for both serial line interfaces and dial circuits.

Nt Serial line interface number or dial circuit interface number.

Nt′ If “Nt” is a dial circuit, this is the interface number of the V.34 serial line interface to which the dial circuit is mapped.

Interface
Interface type and its instance number.

Slot The slot number of the interface running V.34.

Port The port number of the interface that is running V.34.

Self-Test Passed
Number of self-tests that succeeded.

Self-Test Failed
Number of self-tests that failed.

Maintenance: Failed
Number of maintenance failures.

Adapter cable:
Type of adapter cable that is being used.

V.24 circuit:
Circuit numbers as identified by V.24 specifications.

RS-232
EIA 232 (also known as RS-232) names for the circuits.

State Current state of the circuits (ON or OFF).

Line speed
The transmit clock speed (approximate).

Last port reset
Length of time since the port was reset.

Input frame errors:

CRC error
Number of packets received that contained checksum errors and as a result were discarded.

Alignment (byte length)
Number of packets received that were not an even multiple of 8 bits in length and as a result were discarded.

Missed Frame
When a frame arrives at the device and there is no buffer available, the hardware drops the frame and increments the missed frame counter.

too long (> nnnn bytes)
Number of packets received that were greater than the configured frame size and as a result were discarded.

DMA/FIFO overrun
The number of times the serial interface card could not send data fast enough to the system packet buffer memory to receive packets from the network.

L & F bits not set
On serial interfaces, the hardware sets input-descriptor information for arriving frames. If the buffer can accept the complete frame upon arrival, the hardware sets both the last and first bits of the frame, indicating that the buffer accepted the complete frame. If either of the bits is not set, the packet is dropped, the L & F bits not set counter is incremented, and the buffer is cleared for reuse.

Note: It is unlikely that the L & F bits not set counter will be affected by traffic.

aborted frame
Number of packets received that were aborted by the sender or a line error.

Output frame counters:

DMA/FIFO underrun errors
Number of times the serial interface card could not retrieve data fast enough from the system packet buffer memory to transmit packets onto the network.

Output aborts sent
Number of transmissions that were aborted as requested by upper-level software.

Configuring V.34

Chapter 40. Using the ISDN Interface

This chapter describes the Integrated Services Digital Network (ISDN) interfaces on the IBM 2212. It includes the following sections:

ISDN Overview

The ISDN interface software allows you to interconnect routers over ISDN. You can set up the interface to act as a dedicated link or to initiate and accept switched-circuit connections, either on demand, automatically from restart, or on command by the operator.

I.430, I.431, and Channelized T1/E1 are not switched. They are permanent leased-line type connections.

ISDN Adapters and Interfaces

The IBM 2212 supports the following ISDN adapters:

- 2-Port ISDN BRI (U and S/T)
- 1-Port E1 ISDN-PRI
- 1-Port T1/J1 ISDN-PRI
- 2-Port E1 ISDN-PRI
- 2-Port T1/J1 ISDN-PRI

The PRI/Channelized adapters have an integrated CSU/DSU, so an external CSU/DSU is not required.

The interfaces are:

- Basic Rate Interface (BRI)

  The Basic Rate Interface provides two 64-Kbps (Kilobits per second) bearer (B) channels and one 16-Kbps data (D) channel. The B-channels are used as HDLC frame delimited 64-Kbps pipes. The D-channel is used to set up calls. The D-channel can also be used for X.25 traffic.
- Primary Rate Interface (PRI)

  The Primary Rate Interface provides functions that are similar to those provided by the Basic Rate Interface. However, there are some important differences:
  - The PRI adapter does not support multipoint. The BRI adapter does.

- The PRI adapter provides T1/J1 or E1 support.
  - T1/J1 supports twenty-three 64-Kbps B-channels and one 64-Kbps D-channel.
  - E1 supports thirty 64-Kbps B-channels and one 64-Kbps D-channel.
- Channelized T1/E1
  - T1/J1 supports up to twenty-four 64-Kbps time slots.
  - E1 supports up to thirty-one 64-Kbps time slots.
  - You can group time slots in 64-Kbps chunks to aggregate bandwidth.

Note: If you are upgrading from BRI to PRI from talk 6, you must clear the ISDN and dial configurations first, then bring up PRI and configure for PRI.

Dial Circuits

There are four types of dial circuits:

- Static circuits (or link)

  Notes:

  1. I.430, I.431, and Channelized T1/E1 are leased line connections and therefore do not dial.
  2. ISDN considers X.25 traffic over the D-channel as a static circuit. However, you could configure the X.25 circuit as a PVC or SVC using the **encapsulator** command under the dial circuit configuration.
- Switched circuits that dial on demand and hang up after a specified idle time
- WAN restoral circuits that are used only when an assigned primary leased line fails
- Dial-in circuits are used to provide remote clients access to resources on the network.

When bridging over a dial on demand interface it is recommended that you disable spanning tree for that interface and create MAC filters to filter out all undesired traffic. (The MAC filters would drop all frames that are not destined specific MAC addresses.) This keeps the dial circuit from staying connected due to unwanted traffic.

Note: You don't need to add any MAC filters when running BAN traffic on a FR dial-on-demand interface. The BAN software always performs filtering such that the only bridging traffic that will keep a dial-on-demand circuit from hanging up is traffic whose destination MAC address matches the BAN DLCI MAC address.

Add a dial circuit for each potential destination. You can map multiple dial circuits to one ISDN interface. Each dial circuit is a normal serial line network, running Point-to-Point Protocol (PPP), Frame Relay or X.25 (for D-channels only). These protocols are configured to operate over the dial circuits.

Note: You can assign a destination name to a **connection list** (add ISDN address) and assign a destination number to each line in the list. When that destination name is called, the numbers in the list are tried one by one until a connection is made or the list is exhausted.

Routable protocols and bridging and routing features cannot communicate directly with an ISDN interface. You need to configure these protocols to run on the dial circuits. This implementation supports the following protocols and features for ISDN dial circuits:

- APPN
- Banyan VINES
- DECnet
- DLSw
- IP
- IPX
- AppleTalk 2
- Bridging (SRB, STP, SR-TB, and SRT)
- Bandwidth reservation
- WAN restoral
- DIALS

Addressing

To place an ISDN call, specify the telephone number of the destination. To identify yourself to the switch, you need to specify your own telephone number. For ISDN, telephone numbers are called network dial addresses and, for convenience, they are given names called network address names that represent the telephone number.

When you set up an ISDN interface, you add addresses for each potential destination as well as for your own telephone number, which is called the local network address. When you configure a dial circuit, the local network address is obtained from the physical interface configuration and you set a destination addresses for the circuit.

Oversubscribing and Circuit Contention

An ISDN PRI T1/J1 interface can support a maximum of 23 active calls, and an ISDN PRI E1 interface can support a maximum of 30 active calls. An ISDN BRI interface can support a maximum of two active calls. There can be more dial circuits configured on an ISDN interface than active calls supported. This is called oversubscribing. If a dial circuit attempts a call when the ISDN interface has all calls active, there are two possibilities: 1) If the dial circuit has a higher priority than a dial circuit with an active call, the active call will be terminated for the low priority dial circuit and a call will be attempted for the low priority dial circuit and a call will be attempted for the higher priority dial circuit. 2) If the dial circuit does not have a higher priority than any dial circuits with active calls, no call will be made. The router will drop packets sent by protocols on dial circuits that cannot connect to their ISDN destination.

Note: There is no circuit contention when you are running X.25 over the D-channel because the D-channel is always available for the X.25 connection.

See “Set” on page 566 for more information about priority.

Cost Control Over Demand Circuits

Dial-on-demand circuits always appear to be in the Up state to the protocols. Most protocols send out periodic routing information that could cause the router to dial out each time the routing information is sent over dial-on-demand circuits. To limit periodic routing updates, configure IP and OSI to use only static routes and disable the routing protocols (RIP, OSPF) over the dial circuits. If you are using IPX, configure static routes and services and disable the routing protocols (RIP, SAP) over the dial circuits. Another option is to configure low-frequency RIP and SAP update intervals, although this does not prevent RIP and SAP from broadcasting routing information changes as they occur. You should also enable IPX Keepalive filtering, which prevents keepalive and serialization packets from continually activating the dial-on-demand link.

Caller ID and LIDS

If the ISDN service provides the ANI or CallerID (CLID) service by providing the Calling Party Number (CPN) in the ISDN setup message, you can use it to match up dial circuits to the appropriate caller. Otherwise, you must either use a proprietary line identification protocol (LID) or provide circuits that are “ANY INBOUND”.

The LID protocol uses the inbound destination in the dial circuit configuration and LID received to match the calling dial circuit to the receiving dial circuit. The LID protocol is a brief identification protocol initiated by the caller and answered by the receiver. If the caller does not provide the LID message, the receiver may reject the call, if any_inbound dial circuit is not configured. LID exchanges occur on the B-channel.

When connecting to routes that do not support logical ids (LIDS), you can suppress the LID exchange using the config option under the individual dial circuit.

```
config> set lid_used no
```

On the incoming side, if `lid_used=no`, the call is completed and the IBM 2212 does not wait for the LID to come on the B_channel. Instead, the IBM 2212 tries to use the callerID received. If there is no match on the callerID the IBM 2212 checks to see if an any_inbound dail circuit is available. If no any_inbound circuit is available the call is rejected.

On the outgoing side, PPP/FR selftest starts immediately, after B-Channel is allocated.

ISDN Cause Codes

This ISDN implementation specifies a cause code that will stop the router from attempting to establish a connection through an ISDN interface. If the application retries, the router again attempts to establish a connection through this interface and will succeed if the original problem has been corrected. If during the retry the router encounters the same cause code, the application will not attempt further connection processing through this interface.

Cause code interpretations:

1. If cause0 is not ″0x5″ ignore the cause code.

2. If cause0 is ″0x5″ look at cause1. If the high-order (most significant) bit of cause1 is ON, set it to OFF.
3. Convert the result to decimal and look up the meaning in the following table, which is taken from *ITU-T Recommendation Q.850*.

Table 63. ISDN Q.931 Cause Codes

Code	Cause
1	Unallocated (unassigned number)
2	No route to specified transit network
3	No route to destination
6	Channel unacceptable
7	Call awarded and is being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format (address incomplete)
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
34	No circuit/channel available
38	Network out of order
41	Temporary Failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit/channel not available
47	Resource unavailable, unspecified
49	Quality of Service not available
50	Requested facility not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist

Table 63. ISDN Q.931 Cause Codes (continued)

Code	Cause
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
88	Incompatible destination
91	Invalid transit network selection
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type nonexistent or not implemented
98	Message not compatible with call state or message type nonexistent or not implemented
99	Information element nonexistent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiry
111	Protocol error, unspecified
127	Interworking, unspecified

Sample ISDN Configurations

The following topics show several typical ISDN configurations.

Frame Relay over ISDN Configuration

Figure 33 shows how you can connect to a Frame Relay network through an ISDN network. In this configuration, you set the data link on your dial circuits to Frame Relay.

Note: Dial circuits default to point-to-point (PPP) protocol. To change the protocol to Frame Relay, enter **set data-link fr** at the `Config>` prompt. A connection will only be usable if the data link on both ends matches (for example, either FR to FR, or PPP to PPP).

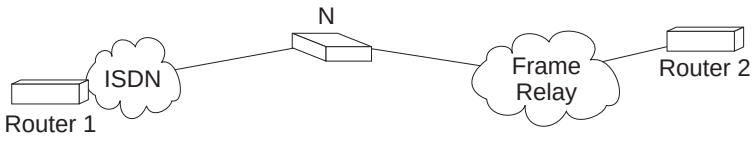

Figure 33. Frame Relay over ISDN Configuration

Note: N could be either an ISDN TA connected to the FR switch, or an ISDN card in a FR switch.

WAN Restoral Configuration

Figure 34 shows how you can use an ISDN connection to back up a failed dedicated WAN link (WAN restoral). In this example, Router A normally uses the WAN link to communicate with Router B. If that connection fails, the ISDN dial-up link reconnects the two routers. When the WAN link recovers, the secondary link automatically disconnects. For more information on how to configure the router for WAN restoral, see Using WAN Restoral in *Using and Configuring Features*.

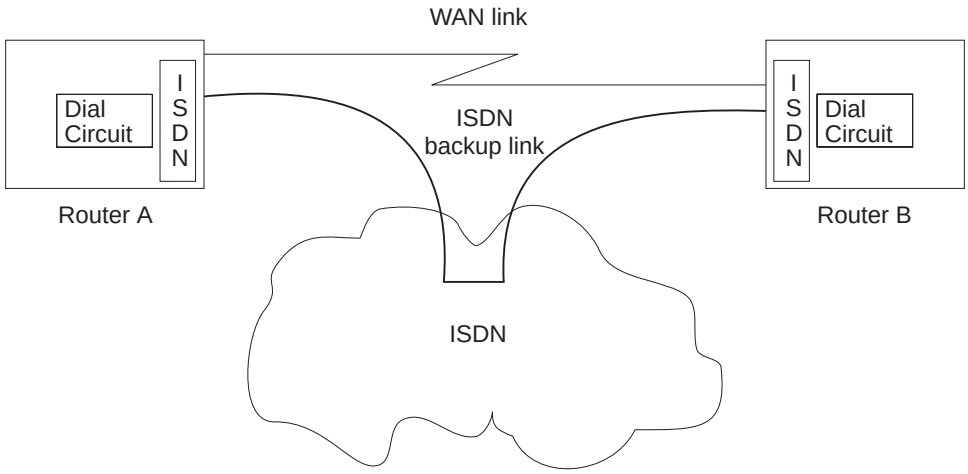

Figure 34. Using ISDN for WAN Restoral

For WAN Restoral, only dial circuits configured for PPP can be used as the secondary link. For WAN Reroute, either a PPP dial circuit or a FR dial circuit can be used as the alternate link.

Channelized T1/E1

When configured for channelized, the Channelized/PRI adapter allows you to get Fractional/Channelized T1/J1/E1 support. You can have channels of 56-Kbps or N*64-Kbps. This will let you multiplex multiple leased lines connections (for example: using V.35 at 56-Kbps) into one physical connection.

To configure a T1 or E1 Primary adapter as channelized:

1. Select “Channelized” as the switch variant for the ISDN interface.
2. Configure the time slots to be used for this ISDN interface when you configure the dial circuit. See “Set” on page 566 for more information.

Example of configuring a Channelized T1 interface:

```
Config>n 6
ISDN Config>set switch chan
ISDN Config>list


                  ISDN Configuration

Maximum frame size in bytes      = 2048
Switch Variant/Service Type      = Channelized
Available Timeslots: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24


Config>n 7
```

```
Circuit config:  7>set net 6
Circuit config:  7>set timeslot 2 3 4 24
Circuit config:  7>list

Base net                      = 6
Idle character                = 7E
Bandwidth                     = 64 Kbps
Timeslot                      = 2 3 4 24
```

Note: If this were an E1 circuit, the available timeslots would be 1 to 31.

Requirements and Restrictions for ISDN Interfaces

Switches/Services Supported

The ISDN Basic Rate Interface (BRI) supports the following switches/services:

- AT&T 5ESS (North America)
- DMS100 (North America)
- USNI1 (North America National ISDN1)
- USNI2 (North America National ISDN2)
- NET 3 (European ETSI)
- INS-Net 64 (Japan)
- VN3 (France Telecom)
- AUS TS 013 (Australia)
- I.430 (See “ISDN I.430 and I.431 Switch Variants” on page 544.)

The ISDN Primary Rate Interface (PRI) supports the following switches/services:

Switch names	Valid command
AT&T 5ESS (North America)	5ESS
AT&T 4ESS (North America	4ESS
Australia (AUSTEL)	AUSPRI
INS-Net 1500 (Japan, NTT)	INSPRI
National ISDN 2 (North America)	USNI2
NET 5 (Euro-ISDN, ETSI)	NET5
Northern Telecom DMS (DMSPRI)	DMSPRI
Native I.431	I431 (See “ISDN I.430 and I.431 Switch Variants” on page 544.)
Channelized T1/E1	CHANNELIZED

ISDN Interface Restrictions

- You cannot boot or dump the router over an ISDN interface.
- Except for BRI, which allows you to use the D-channel for X.25 packet data, you cannot use the D-channel for data traffic. Normally the D-channel is used only for setting up and taking down B-channel connections.

Dial Circuit Configuration Requirements

You need to consider the following when you configure PPP or Frame Relay with ISDN:

- The ISDN interface will not enforce transmit delay counters that you set in the PPP configurations.
- Do not enable psuedo-serial-ethernet on the dial circuit.

Before You Begin

Before you configure ISDN, you need the following information:

- Telephone number of the local ISDN port.
- Destination telephone numbers, including any telephone extensions.
- Type of switch to which the ISDN interface is connected. See “Switches/Services Supported” on page 538 for the list of switches.

Note: Additional parameters, such as TEI and SPID may be required based on your Switch Type and your service provider.

Configuration Procedures

This section describes how to configure your ISDN interface and its associated dial circuits. Specifically, the tasks you need to perform are:

1. Adding ISDN addresses
2. Configuring ISDN parameters
3. Configuring the ISDN Interface (PRI only)
4. Adding dial circuits
5. Configuring dial circuits

Note: You must restart the router for configuration changes to take effect.

Adding ISDN Addresses

You need to add an ISDN address for each ISDN interface as well as for each destination. The ISDN address includes:

- *Address Name*. The address name is a description of the address. You can use any string of up to 23 printable ASCII characters.
- *Network Dial Address*. Telephone number of the local or destination port. You can enter up to 25 numbers as well as 6 characters, including punctuation. The router uses only the numbers.
- *Network Subdial Address*. Optional. This is an additional part of telephone number, such as an extension, that is interpreted once the interface connects to a PBX. You can enter up to 20 numbers, as well as 11 additional spaces and punctuation. The router uses only the numbers.

To add an ISDN address, enter the **add isdn-address** command at the `Config>` prompt. For example:

```
Config>add isdn-address
Assign address name [23] chars []? baltimore
Assign network dial address [1-15 digits] []? 1-555-0983
Assign network subdial address [1-20 digits] []? 23
```

To see a list of your ISDN addresses, enter **list isdn-address** at the `Config>` prompt.

To delete an ISDN address from your list, enter the **delete isdn-address** command at the `Config>` prompt.

Configuring ISDN Parameters

Access the `ISDN Config>` prompt. To access the `ISDN Config>` prompt, enter the **network** command followed by the interface number of the ISDN interface at the `Config>` prompt. For example:

```
Config>network 3
ISDN user configuration
ISDN Config>
```

You can use the **list devices** command at the `Config>` prompt to display a list of interface numbers configured on the router. See “ISDN Configuration Commands” on page 547 for more information about configuration commands.

1. Specify the type of switch/service to which this ISDN interface is connected.

   Use the **set switch-variant** command to specify the type of switch to which this ISDN interface is connected. See “Switches/Services Supported” on page 538 for the list of switches/services. For example:

   ```
   ISDN Config>set switch net5
   ```

   This is the software type running at the switch (for example, DMS100 means running DMS100 Custom software).

2. Specify the network address name of the local port.

   Use the **set local-address-name** command to specify the network address name of the local port. You must use one of the address names you defined using the **add isdn-address** command. For example:

   ```
   ISDN Config>: set local-address-name
   Assign local address name []? baltimore
   ```

   Note: This is what we will send in the Calling Party Number field of the ISDN Setup message.

3. Set the directory number of the local port.

   DN0 is what the ISDN service provider is placing in the Called Party Number field in an ISDN setup message. This field is used for incoming calls only. If no DN0 is configured, the router will answer any call made to it without checking the DN0 field. If you have added a DN0 field, you must use the **remove dn0** command to remove it. You cannot just blank it out with another set command.

   ```
   ISDN Config>set dn0
   Enter DN0 (Directory-Number-0) [ ]?15550983
   ```

4. For BRI only, set the ISDN interface to either point-to-point (pp) or multipoint (mp).

   Point-to-point is one ISDN device on an ISDN line. Multipoint is two or more ISDN devices sharing an ISDN line. With some switch variants, you must configure the line as multipoint regardless of how many devices are on it. Check with your ISDN service provider.

   ```
   ISDN Config>set multi-point-selection
   Multipoint Selection [MP]? pp
   ```

   Note: PRI is not configurable, it is always point-to-point.

5. For BRI only, if you are connected to a U. S. switch variant, your service provider may require a Service Profile ID (SPID).

   The SPID is a number up to 20 digits long that uniquely identifies the ISDN device. Your ISDN service provider assigns SPIDs. You must get the SPID number from your service provider.

```
ISDN Config>set spid
Enter BChannel Number [1]? 1
Enter Service Profile ID (SPID) []? 91955555550101
```

6. For BRI only, set the Terminal Endpoint Identifier (TEI) to match the signalling TEI number of your ISDN switch.

   Check with your service provider to find out which TEI signalling the switch supports. The default TEI is auto. If the switch to which your ISDN interface is connected does not support automatic TEI signalling, you must set the TEI to a value from 0 to 63, assigned by your provider.

   If you are connected to a 5ESS or USNI1 BRI switch, you must set the TEI for each B-channel. The **set tei** command prompts you for a B-channel number.

   ```
   ISDN Config>set tei
   TEI [AUTO]? 10
   ```

   Note: TEI for a PRI is always 0.

   If you are using X.25 on the D-channel, you must configure a separate TEI for the D-channel. For example:

   ```
   ISDN Config>set tei 2
   TEI  2 []? 21
   ```

7. To set the frame size, use the **set framesize** command. For example:

   ```
   ISDN Config>set framesize
   Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
   ```

   Note: If you choose a frame size of 1024, PPP will not work over the ISDN dial circuit, since the minimum frame size for PPP is 1500.

   For more information about setting the ISDN framesize, see “Set” on page 549.

Optional ISDN Parameters

This section describes optional ISDN parameters you can set. For a complete description of these commands see “ISDN Configuration Commands” on page 547.

- For all ISDN switches except INS64, you can configure the limit for the number of calls to an address. Use the **set retries-call-address** command to set the number of calls to a non-responding destination. Use the **set timeout-call-address** command to set the time period to wait before trying the call again.

When you have finished configuring the ISDN interface, you can use the **list** command to display your configuration.

Configuring the ISDN Interface

For the ISDN PRI, you need to configure T1/J1 or E1 for each adapter, depending upon the adapter.

T1/J1 PRI Interface

Specify the following T1/J1 parameters:

1. For the T1/J1 PRI interface, line build out specifies the attenuation of the signal transmitted by the router’s T1 port. Specify the `lbo` (line build out) based on the information provided by the service provider.

   a= -00.0 dB

   b= -07.5 dB

c= -15.0 dB

d= -22.5 dB

For example:

```
set int lbo a
```

2. Specify the `code`, either B8ZS or AMI. B8ZS is default. The service provider provides this information.

   For example:

   ```
   set int code AMI
   ```

3. Specify `ZBTSI`- Zero Byte Time Slot Inversion, either ENABLED or DISABLED. The default is DISABLED. The service provider provides this information.

   For example:

   ```
   set int ZBTSI enabled
   ```

4. Specify the `esf-data-link`. Select one of the following based on the service subscription:

   ANSI-T1.403 ANSI-IDLE AT&T-IDLE

   Default is ANSI-T1.403

   For example:

   ```
   set int esf-data-link ansi-idle
   ```

E1 PRI Interface

For the E1 PRI interface, specify the following parameters:

1. Specify the `code`, either HDB3 or AMI. HDB3 is default. The service provider provides this information.

   For example:

   ```
   set int code HDB3
   ```

2. Specify the `crc4`, either ENABLED or DISABLED. Default is ENABLED. The service provider provides this information.

   For example:

   ```
   set int crc4 enabled
   ```

Adding Dial Circuits

Dial circuits are mapped to ISDN interfaces. You can map multiple dial circuits to one ISDN interface.

To add a dial circuit, enter the **add device dial-circuit** command at the `Config>` prompt. The software assigns an interface number to each circuit. You will use this number to configure the dial circuit. For example:

```
Config>add device dial-circuit
Enter the number of PPP Dial Circuit interfaces [1]?
Adding device as interface 6
Base net for the circuits(s) [0]?
```

The number of dial circuits that can be configured depends on the total number of parameters to be configured and the size of the resulting configuration file.

Note: Dial circuits default to point-to-point (PPP) protocol. To change the dial circuit protocol to Frame Relay, enter the **set data-link fr** command at the `Config>` prompt. . Except for X.25 over an ISDN BRI D-channel, other data-link types (SDLC and SRLY) are not supported over ISDN.

Configuring Dial Circuits

This section describes how to configure a dial circuit.

1. Display the `Circuit Config>` prompt by entering the **network** command followed by the interface number of the dial circuit. You can enter the **list devices** command at the `Config>` prompt to display a list of the interface numbers configured on the router. For example:

```
Config> network 6
Circuit configuration
Circuit Config>
```

2. Map the dial circuit to an ISDN interface. Use the **set net** command. The Base net is the ISDN interface number. (This is needed only if you are changing the base net.)For example:

```
Circuit Config> set net
Base net for this circuit [0]? 3
```

   Note: If the dial circuit data link type is X.25 or the base net switch variant is I.43x or channelized, the following steps (3-11 on page 544) do not apply.

3. Specify the address name of the remote router to which the dial circuit will connect. You must use one of the names you defined using the **add isdn-address** command. For example:

```
Circuit Config> set destination
Assign destination address name []? baltimore
```

4. Configure the dial circuit to initiate outbound calls only, accept inbound calls only, or to both initiate and accept calls.

   Use the **set calls** command. For example:

```
Circuit Config> set calls outbound
Circuit Config> set calls inbound
Circuit Config> set calls both
```

   Note: For WAN-Restoral operations or dial-on-demand applications, you should set up the circuit for either inbound or outbound calls.

5. Specify the timeout period for the circuit.

   Use the **set idle** command. If there is no traffic over the circuit for this specified time period, the dial circuit hangs up. To configure the circuit as a dedicated circuit, set the idle timer to zero. To configure the circuit to dial on demand, set the idle timer to a value other than zero. The range is 0 to 65535 and the default is 60 seconds. For example:

```
Circuit Config> set idle
Idle timer (seconds, 0 means always active) [0]? 0
```

   Note: WAN restoral/reroute must be fixed.

6. Optionally, you can provide a LID name to send (instead of the default LID, which is the destination name) by specifying a lid_out_addr.

   When more than one circuit is configured between two routers (parallel circuits), there must be a way to know which dial circuit connects them. For this purpose, a lid_out_addr is sent from the router at one end (the caller). The receiving router must have an inbound destination address that matches the lid_out_address on the sending router in order for the dial circuits to connect. The lid_out_addr must be an address name that has been previously added using “ADD ISDN-ADDRESS” at the **config>** prompt.

```
Circuit Config> set lid_out_addr  router2
```

7. Optionally, you can set the relative priority of dial circuits.

The priority field allows a circuit to preempt another when no channels are available. If an outbound call is made and all the channels are in use, then the priority of the requesting dial circuit is checked against all the active dial circuits. If there is one whose priority is lower than this, then that circuit is disconnected and a call is made for the higher priority dial circuit.

Note: Only outbound dial-on-demand circuits will be brought down.

See “Set” on page 566 for more information about priority.

```
Circuit Config> set priority 1
```

8. Optionally, you can delay the time between when a call is established and the initial packet is sent. Use the **set selftest-delay** command. Some ISDN switches start to send data before receiving a signal indicating the complete establishment of the circuit at the destination. Setting a selftest delay can prevent initial packets from being dropped. For example:

```
Circuit Config> set selftest-delay
Selftest delay(milli-seconds,0 means no delay)[150]?200
```

9. Set the inbound address name.

   Use the **set inbound** command. This command is for inbound circuits only. For example:

```
Circuit Config> set inbound
Assign destination inbound address name [ ]? newyork
```

   The inbound destination number is used to match the incoming LID or CallerID with the dial circuit. If there is a match that dial circuit gets the call.

10. Optionally, you can enter the configuration process for the data-link layer protocol that is running on the dial circuit (PPP or Frame Relay).

    Use the **encapsulator** command. For example:

```
Circuit Config> encapsulator
```

11. Optionally, you can use the **set bandwidth** command to set the line speed at which to make the call (either 56-Kbps or 64-Kbps). This provides per-call control for ISDN interfaces. For example:

```
Circuit Config> set bandwidth 56Kbps
```

ISDN I.430 and I.431 Switch Variants

To use the Native I.430 mode that is supported in Japan and is known as D64S in Germany, you must code the ISDN switch variant as I.430. This treats the ISDN interface like a leased line. There is no D-channel signalling traffic in this mode.

Code the switch variant as I.431 when running a leased line over ISDN PRI (T1/J1 only).

Native I.430 Support

Only one dial circuit is allowed per I.430 base net. You can configure the speed to either 64-Kbps, 80-Kbps, 128-Kbps, or 144-Kbps using the `set bandwidth` command. See “Set” on page 549 to configure the bandwidth command.

Example: `Base ISDN Net`

```
Config> n 6
ISDN Config> set switch i430
ISDN Config> list all
```

```
                                    ISDN Configuration

Maximum frame size in bytes      = 2048
Switch Variant                   = I430 BRI
PS1 detect                       = Enabled
```

Example: Dial Circuit

```
Config>n 7 ------------------ DIAL CIRCUIT (CAN ONLY BE ONE FOR I430)
Circuit config:   7>
Circuit config:   7>set net 6
Circuit config:   7>set bandwidth 128
Circuit config:   7>list all

Base net                        = 6
I430 BRI Bandwidth              = 128 kbs
```

Native I.431 Support

When configuring for Native I.431 support, only one dial circuit should be used. It should be attached to the base net. The I.431 only runs on the ISDN PRI T1 adapter. The speed is fixed at 1.5 Mbps.

Note: The multiport ISDN PRI adapters do not support the I.431 switch variant. To utilize a full PRI line, select the channelized variant and assign all the timeslots to one dial circuit.

Example: Base ISDN net

```
Config> n 5
ISDN Config> set sw i431
ISDN Config> list all
                   ISDN Configuration

Maximum frame size in bytes      = 2048
Switch Variant                   = I431 PRI
```

Example: Dial Circuit

```
Config> n 6
Circuit config:   6>set net 5
Circuit config:   6>list all


Base net                        = 5
```

X.31 Support

The ITU Standard X.31 is for transmitting X.25 packets over ISDN. This standard provides support for X.25 with Unconditional Notification on the ISDN BRI D-channel.

X.31 is available from service providers in several countries. It gives the router a 9600bps X.25 circuit. Since the D-channel is always present, this condition can be an X.25 PVC or SVC.

An X.31 example is, when a packet handler is provided by the ISDN service provider, the X.25 packets and LAP/B frames (RRs, SABMEs, etc.) will be transmitted and received on the D-channel along with the ISDN signaling (Q931/Q921) messages. The D-channel provides a connection that enables the ISDN user terminal to access the packet handler function within the ISDN by establishing a link layer connection (SAPI=16) to that function which can then be

used to support packet communications according to X.25 layer 3 procedures. Maximum frame transfer size is 260 bytes.

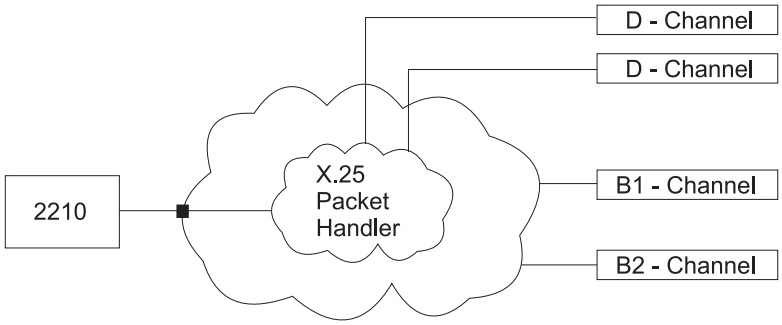

Figure 35. X.31 Support

Example:

```
Config>n 6
Config>set data x25 6
Circuit config:   6>set net 5
Circuit config:   6>list all


Base net                        = 5
```

Note: You should assign an X.25 TEI or specify Auto on the BRI base net. The default value is none.

Chapter 41. Configuring and Monitoring the ISDN Interface

This chapter describes the ISDN commands and GWCON commands. It includes the following sections:

Notes:

1. ISDN interfaces have both ELS messages and cause codes that you can use to monitor ISDN-related activity. See *Event Logging System Messages Guide*
2. The ISDN, Q931, CEME, LAPD, and DIAL ELS subsystems are available.

ISDN Configuration Commands

Table 64 describes the ISDN configuration commands, and the following sections explain the commands. Enter these commands at the `ISDN Config>` prompt.

Table 64. ISDN Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Block-calls	Blocks incoming calls from a specific caller.
Disable	Valid only for BRI. Disables Power Source 1 detection.
Enable	Valid only for BRI. Enables Power Source 1 detection.
List	Displays the ISDN configuration.
Remove	Removes DN0 entries from the ISDN configuration.
Set	Sets the frame size, local address, no-answer timeouts, number of retries after no answer, type of ISDN switch, directory numbers, SPIDS, TEI and bandwidth.
Cause Code	Stops further processing attempts to establish a connection through an interface.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Block-Calls

Use the **block-calls** commands to block incoming calls. Caller numbers to be blocked must be added to the authentication list. The maximum number of caller blocked calls is 16 per interface.

Call block can be used for:

- An unsolicited call being constantly received.
- Network bringup/test where you need to ignore certain calls.

Syntax:

block-calls add
list

remove

Add Adds a caller's number to be blocked.

List Lists the callers' numbers to be blocked.

Remove
Removes a caller's number for the list to be blocked.

Disable

The **disable** command disables Power Source 1 detection. If your switch does not supply Power Source 1, you should disable PS1.

Note: This command is valid only for BRI.

Syntax:

disable ps1

Note: On the U interface ISDN BRIs, there is no ps1 detect circuitry and the value of this field is ignored.

Enable

The **enable** command enables Power Source 1 detection. If your ISDN switch supplies Power Source 1 (PS1), you should enable PS1 on the interface. This causes the interface to detect when the switch shuts down and to clear all information about the last call before it reestablishes the connection. For Euro-NET3 switches supporting restricted power mode, PS1 must be enabled.

Do not enable PS1 if your switch does not supply Power Source 1.

Note: This command is valid only for BRI.

Syntax:

enable ps1

Note: On the U interface ISDN BRIs, there is no ps1 detect circuitry and the value of this field is ignored.

List

The **list** command displays the current ISDN configuration.

Syntax:

list

Example: `list`

```
                              ISDN Configuration
  Local Network Address Name    = line-1-local
  Local Network Address         = 1-508-555-1234
  Local Network Subaddress      = 21
  Maximum frame size in bytes   = 2048
  Outbound call address Timeout = 180  Retries =  2
  Switch-Variant-Model          = US National ISDN-1
  Multipoint Selection          = Point-to-Point
  DN0 (Directory Number 0)      = 5551234
```

```
DN1 (Directory Number 1)      = 5553456
Service Profile ID (B1)       = 91955555550100
Service Profile ID (B2)       = 91955555550101
TEI for B-Channel 1           = Automatic
TEI for B-Channel 2           = Automatic
TEI for X.25
= Automatic
PS1 detect                    = Disabled

No circuit address accounting information being kept.
```

Remove

The **remove** command lets you remove DN0 or DN1 entries that you set previously with the **set DN0** or **set DN1** command.

Syntax:

remove DN0-entry...

Example:

```
remove DN0
```

Set

The **set** command configures frame size, addresses, and timeouts. It also specifies the switch-variant and TEI number. For PRI, the terminal endpoint identifier (TEI) is always zero (0).

Syntax:

set
- framesize...
- frame-type[2]
- interface
- local-address-name...
- multipoint-selection[1]...
- RAI-type[2]
- retries-call-address...
- service-profile-id[1]...
- timeout-call-address[1]...
- switch-variant...
- dn0...
- dn1...[3]
- tei[1]...

framesize 1024 or 2048 or 4096 or 8192
Sets the size of the network layer portion of frames transmitted and received on the ISDN interface. Data link and MAC layer headers are not

1. BRI only
2. Channelized only
3. PRI only

included. You must set the ISDN frame size so that it is greater than or equal to the frame size configured for the dial circuits using the ISDN interface.

For PPP dial circuit interfaces, you can change the PPP MRU using the **set lcp options** command. The ISDN frame size must include enough bytes for the PPP MRU and the PPP header.

Note: If you choose a frame size of 1024, PPP will not work over the ISDN dial circuit, since the minimum frame size for PPP is 1500.

For FR dial circuit interfaces, you can change the frame size using the **set framesize** command. The ISDN frame size must be greater than or equal to the FR frame size.

If a dial circuit's frame size is greater then the ISDN frame size, then the dial circuit's frame size is decreased at router initialization.

Example:

```
set framesize
Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
```

frame-type

Choices are D4 or ESF. This specifies the T1 multiframe format. Only ESF is supported for non-channelized mode. Frame type is configured under the base ISDN net menu.

Example:

```
set frame-type
Circuit config: 10>set frame type
```

interface

For PRI only. Sets the following interface parameter values for T1 and E1 lines.

For T1 PRI:

lbo The attenuation of the signal transmitted by the router's T1 port. This information is provided by the service provider.

Valid Values:

a= -00.0 dB

b= -07.5 dB

c= -15.0 dB

d= -22.5 dB

Default Value: a

code This information is provided by the service provider.

Valid Values: B8ZS or AMI

Default Values: B8ZS

ZBTSI Zero Byte Time Slot Inversion. This information is provided by the service provider.

Valid Values: Enabled or Disabled

Default Value: Disabled

esf-data-link

The service subscription. This information is provided by the service provider.

Valid Values:

ANSI-T1.403

ANSI-IDLE

AT&T-IDLE

Default Value: ANSI-T1.403

For E1 PRI:

code This information is provided by the service provider.

Valid Values: HDB3 or AMI

Default Value: HDB3

crc4 Specifies whether the router's E1 port will transmit crc4 code words and check them in the received frames. This information is provided by the service provider.

Valid Values:Enabled or Disabled

Default Value:Disabled

local-address-name *address name*

This is the network address name of the local ISDN interface. This address name must match one of the names that you defined at the `Config>` prompt using the **add isdn-address** command.

Valid Values: Any valid address

Default Value: None

Example:

```
set local-address-name
Assign local address name []? line-1-local
```

multipoint-selection [mp or **pp]**

For BRI only. Sets the ISDN physical bus to either point-to-point (pp) or multipoint (mp) configuration. Point-to-point is one ISDN device on an ISDN line. Multipoint is two or more ISDN devices sharing an ISDN line.

Some service providers require that you configure the line as multipoint regardless of how many devices are on the line. Check with your ISDN service provider.

Example:

```
set multipoint-selection
Multipoint Selection [PP]? mp
```

RAI-type

Choices are ANSI or Japanese. This specifies the method of indicating RAI on the T1 line when using D4 framing. ANSI RAI is indicated by a value of 0 in bit 2 of all channels. Japanese RAI is indicated by a value of 1 in the S-bit position of frame 12. RAI type is configured under the base ISDN net menu.

retries-call-address *value*

Some telephone service providers impose restrictions on automatic recalling devices to limit the number of successive calls to an address that is inaccessible or that refuses those calls. **Retries-call-address** specifies the

maximum number of calls the router attempts to make at one time. Setting **retries-call-address** to 0 causes the router to bring up all circuits at once.

If you set the switch-variant to INS64, you cannot change the**retries-call-address** default. It is fixed at 2.

Valid Values: 0 to 30

Default Value: 23 (2 for BRI)

service-profile-id B-channel# spid#

For BRI only. Sets the service profile ID (SPID) for each B-channel. SPIDs are used in the United States to uniquely identify a particular ISDN device. This ID is a number up to 20 digits long and is assigned by ISDN service providers. SPIDs are used predominantly in a multipoint bus configuration where multiple ISDN devices share a single ISDN line. Check with your service provider to determine whether or not you are required to use a SPID.

Example:

```
set spid
Enter B-Channel Number [1]? 1
Enter Service Profile ID (SPID) [123]? 91955555550100
```

timeout-call-address # of seconds

After the router reaches the maximum number of **retries-call-address** to a non-responding address, it does not make further calls to that address until this time has expired. The timeout period begins when the router attempts the first call to an address. Setting **timeout-call-address** to 0 causes the router to retry until the call is established.

If you set the switch-variant to INS64, you cannot change **timeout-call-address**. It is fixed at 180.

Valid Values: 0 to 65535 seconds

Default Value: 180 seconds

Example:

```
set timeout-call-address
Outbound call address Time-out (secs) [0]? 180
```

switch-variant

Specifies the model of the switch to which this ISDN interface is connected. You can choose switch-variants/service type for the ISDN Basic Rate interface or the ISDN Primary Rate interface from the following lists.

Valid Values Basic Rate Interface (BRI):

- AT&T 5ESS (North America)
- DMS100 (North America)
- USNI1 (North America National ISDN1)
- USNI2 (North America National ISDN2)
- NET 3 (European ETSI)
- INS 64 (Japan)
- VN3 (France Telecom)
- AUS TS 013 (Australia)
- Native I.430

Default Value: NET 3

Valid Values ISDN Primary Rate Interface (PRI)/Channelized T1/E1:

- AT&T 5ESS (North America)
- AT&T 4ESS (North America)
- Australia (AUSTEL)
- INS-Pri (Japan, NTT)
- National ISDN 2 (North America)
- NET 5 (Euro-ISDN, ETSI)
- Northern Telecom 250 (DMSPRI)
- Native I.431
- Channelized T1/E1

Default Value: DMSPRI

dn0 *directory number 0*

To accept inbound calls **DN0** must match the network dial address (telephone number) you configured using the **set local-address-name** command. If DN0 is not configured no check is made and all calls will be accepted. If the switch does not provide the called party number in the incoming setup message, DN0 should not be configured. See on page 553 for additional information.

Example:

```
set dn0
Enter DN0 (Directory-Number-0) [ ]? 5088981234
```

dn1 *directory number 1*

DN1 is a secondary directory number supported by NET3, VN3 and AUS, switch variants. If DN1 is not configured no check is made and all calls will be accepted. If the switch does not provide the called party number in the incoming setup message, DN1 should not be configured. See on page 553 for additional information.

tei *auto* **or** *none* **or** *value*

For BRI or X.25 over D-Channel only. This command sets the signalling TEI (terminal endpoint identifier) for the ISDN interface. This setting must match the signalling TEI of your switch. For PRI, the TEI is always set to zero (0). Check with your service provider to find out the correct TEI signal. The default is auto. Change this setting only if your switch does not support automatic TEI signalling. The valid settings for TEI are auto or a value from 0 to 63. If you set the TEI to none, you will disable the ISDN interface.

USNI-1 and 5ESS switches require that you set the TEI for each B-channel. If you set the switch variant to one of those switches, the **set tei** command prompts you for a B-channel number. See on page 553 for additional information.

Example 1:

```
set tei
TEI  [AUTO]? 60
```

Example 2:

```
set tei
TEI 0 or TEI 1 [1]? 1
TEI [AUTO]?
```

Example 3:

```
set tei 2
TEI []? 21
```

Note: This applies to all Basic Rate ISDN switch variants:

- DN0, and DN1 are used to verify that the incoming call is being delivered to the correct ISDN destination.
- If the destination number (Called Party Number) in the ISDN call being delivered does not match either DN0 or DN1, then the call is rejected.
- If the user wishes to bypass the destination verification checking, then do not configure either DN0, or DN1. If the ISDN line provisioning has only one DN, and the user wishes to use the destination verification then you must configure DN0. Do not configure DN1 unless the ISDN line is provisioned for two DNs.
- When configuring the SPIDs and TEIs, always be sure to configure the first SPID (SPID[0]) and TEI (TEI[0]). It will cause errors it you have a SPID[1] or TEI[1] configured without SPID[0] or TEI[0] configured.

Cause Code

Use the **Cause Code** command to prevent the router from retrying to establish a connection through the ISDN interface when it receives a "specified" (valid value) response. Enter these commands at the `Cause Config>` prompt.

Syntax:

cause code ? (Help)
add
list
remove
exit

Table 65. ISDN Cause Codes Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Add	Adds cause code entries to the ISDN configuration.
List	Displays the cause code lists for the ISDN configuration.
Remove	Removes cause code entries from the ISDN configuration.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Add Use the **add** command to add a cause code to an ISDN configuration.

Valid Values: Any hexadecimal value between 01 and FF

Default Value: None

Syntax: cause code add *value*

Example: `add FF`

List Use the **list** command to show the cause code list of an ISDN configuration.

Syntax: cause code list

Remove

Use the **remove** command to remove a cause code from an ISDN configuration.

Valid Values: Any hexadecimal value between 01 and FF

Default Value: None

Syntax: cause code remove *value*

Example: `remove FF`

Accessing the Interface Monitoring Process

To access the interface monitoring process for ISDN, enter the following command at the GWCON (+) prompt:

```
+ network #
```

Where # is the number of the ISDN interface. You cannot directly access the monitoring process for dial circuits, but you can monitor the dial circuits that are mapped to the ISDN interface.

ISDN Monitoring Commands

The following sections explain the ISDN operating commands which allow you to view the accounting entries, calls, circuits, parameters, and statistics of the ISDN interfaces. Enter these commands at the ISDN> prompt.

Table 66. ISDN Monitoring Command Summary

Monitoring Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Block-calls	Blocks incoming calls from a specific caller.
Calls	Displays the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.
Channels	Displays the statistics for the channels on the ISDN Primary Rate Interface.
Circuits	Displays the status of all data circuits configured on the ISDN interface.
Dial-dump	Displays the operation characteristics of the specified dial circuit.
L2_counters	Lists the L2/L1 states along with some L2 counters.
L3_counters	Lists counters of set ups sent/received/accepted.
TEI	Lists status of TEI's (BRI only)
Parameters	Displays the current parameters for the ISDN interface.
Signaling-L3	This command is to be used only by product support personell.
Statistics	Displays the current statistics for the ISDN interface.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 13.

Block-Calls

Use the **block-calls** commands to block incoming calls. Caller numbers to be blocked must be added to the authentication list. The maximum number of caller blocked calls is 16 per interface.

Syntax:

block-calls add

list

remove

Add Adds a caller's number to be blocked.

List Lists the callers' numbers to be blocked.

Remove
Removes a caller's number for the list to be blocked.

Calls

Use the **calls** command to list the number of completed and attempted connections made for each dial circuit mapped to this interface since the last time statistics were reset on the router.

Syntax:

calls

Example:

```
calls
Net Interface  Site Name           In    Out   Rfsd  Blckd
  4     PPP/1  v403                2      0      0      0

Unmapped connection indications:    0
```

Net Number of the dial circuit mapped to this interface.

Interface
Type of interface and its instance number.

Site Name
Network address name of the dial circuit.

In Inbound connections accepted for this dial circuit.

Out Completed connections initiated by this dial circuit.

Rfsd Connections initiated by this dial circuit that were refused by the network or the remote destination port.

Blckd Connection attempts that the router blocked. The router blocks connection attempts if all available channels are in use, if the maximum retries are used up and the router is waiting for the timer to count down, or if layer 1 is up, but layer 2 is down.

Unmapped connection indications:
Connection attempts that were refused by the router because there were no enabled dial circuits that were configured to accept the incoming calls.

Channels

The **channels** command lists the statistics for a channel on the ISDN Primary Rate Interface.

Syntax:

channels

Circuits

The **circuits** command shows the status of the dial circuits configured on the ISDN interface that are in the state of "Up" or "Available".

Syntax:

circuits

Example:

```
circuit
Net Interface  MAC/Data-Link    State     Reason      Duration
4     PPP/1   Point to Point    Up B1     SelfTest    91:24:03
5     PPP/2   Point to Point    Up B2     Inbound     91:24:00
```

Net Number of the dial circuit mapped to this interface

Interface
Type of interface and its instance number.

MAC/Data-Link
Type of data-link protocol configured for this dial circuit.

State Current state of the dial circuit:

Up Currently connected.

Available
Not currently connected, but available.

Disabled
Dial circuit disabled.

Down Failed to connect because of a busy dial circuit or because the link-layer protocol is down.

Reason
Reason for the current state:

nnn_Data
(Where nnn is the name of a protocol.) The circuit is up because a protocol had data to send.

Rmt Disc
Remote Disconnect. The circuit is either down or available because the remote destination disconnected the call.

Opr Req
Operator Request. The circuit is available because the last call was disconnected by a monitoring command.

Inbound
The circuit is up because the circuit answered an inbound call.

Restoral
The circuit is up because of a WAN-Restoral operation.

Self Test
The circuit was configured as static (idle time=0) and successfully connected once it was enabled.

Duration
Length of time that the circuit has been in the current state.

Dial-dump

Use the **dial-dump** command to display the operation characteristics of the specified dial circuit.

Syntax:

dial-dump *ciruitname*

L2_Counters

Use the **L2_counters** command to list the L2/L1 states along with some L2 counters.

Syntax:

L2_counters

L3_Counters

Use the **L3_Counters** command to list counters of set ups sent/received/accepted.**Syntax:**

L3_counters

TEI

Use the **TEI** command to list the status of TEIs. For BRI only.

Syntax:

parameters

Example:

```
parameters
ISDN Port parameters:

Local Address Name:        vl233
Local Network Address:     20
Local Network Subaddress:
Frame Size:          2048
TEI 0:               Automatic
TEI 1:               Automatic
X.25 TEI:               21
Switch Variant:      AT&T 5ESS (United States)
Multipoint Selection:    Multipoint
Directory Number 0:      20
Outbound call address Timeout:     180       Retries:     0
```

Parameters

Use the **parameters** command to display the current ISDN configuration.

Syntax:

parameters

Example:

```
parameters
ISDN Port parameters:

Local Address Name:        vl233
Local Network Address:     20
Local Network Subaddress:
Frame Size:          2048
TEI 0:               Automatic
```

```
TEI 1:              Automatic
X.25 TEI:              21
Switch Variant:     AT&T 5ESS (United States)
Multipoint Selection:    Multipoint
Directory Number 0:      20
Outbound call address Timeout:     180       Retries:     0
```

Statistics

Use the **statistics** command to display the current statistics for this ISDN interface.

Syntax:

statistics

Example for BRI:

```
statistics
Link:   Active    ISDN Firmware:   1.0    Handler State: Running

                     D Channel     B1 Channel     B2 Channel

Total Transmits          32788         230217         164336
Total Receives           32789         164342         208255
Transmit Bytes          196767       22797579        6572177
Receive Bytes           196785        6572411        9517221
Invalid Interrupts           0              0              0

Transmit:     D       B1       B2    Receive:        D       B1       B2

Error         0        0        0    Error           0        5        0
Overflow      0        0        0    Overflow        0        0        0
Underrun      0        0        0    Overrun         0        0        0
Abort         0        0        0    Abort           0        5        0
                                     CRC Error       0        0        0
```

Example for BRI using I.430:

```
statistics
Link:   Active    ISDN Firmware:   0.0    Handler State: Running


Total Transmits          32788
Total Receives           32789
Transmit Bytes          196767
Receive Bytes           196785
Invalid Interrupts           0

Transmit:                           Receive:

Error         0                     Error           0
Overflow      0                     Overflow        0
Underrun      0                     Overrun         0
Abort         0                     Abort           0
                                    CRC Error       0
```

This display shows the current state of the link, the firmware revision, and the state of the dial circuit. It also shows statistics on what was transmitted and received on the interface.

Example for PRI with E1:

```
  statistics
  Link:   Active    ISDN Firmware:   1.0    Handler State: Running

Transmit    D  Channel     Receive    D  Channel

Packets          68422     Packets          68419
Bytes           411656     Bytes           413592
Overflow            23     Overflow            3
Underrun             0     Too Long            6
                           Abort               4
                           CRC error           8
                           Misaligned          3

Transmit    B  Channels    Receive    B  Channels

Packets        1499094     Packets        1499228
Bytes         59955660     Bytes         59951780
Overflow             0     Overflow            90
```

```
Underrun             0     Too Long          171
                           Abort             139
                           CRC error         232
                           Misaligned         72

E1 Status Register         E1 Error Count Registers

Receive AIS         : Off  CRC6 Errors:        4
Receive RAI         : Off  LCV  Errors:       38
Receive Carrier Loss: Off  FEB  Errors:       11
Receive Loss of Sync: Off  FAS  Errors:       24
```

Example for PRI with T1 using I.431:

```
statistics
Transmit                   Receive

Packets              0     Packets             0
Bytes                0     Bytes               0
Overflow         68480     Overflow            0
Underrun             0     Too Long            0
                           Abort               0
                           CRC error           0
                           Misaligned          0

 T1 Status Register         T1 Error Count Registers

Receive AIS         : Off  LCV  Errors:           0
Receive RAI         : Off  CRC6 Errors:           0
Receive Carrier Loss: Off  Sync Errors:    47937328
Receive Loss of Sync: On

T1 PRM Events                 Local       Remote

CRC Error                         0            0
Controlled Slip                   0            0
Line Code Violation               0            0
Frame Sync Bit Error              0            0
Severely Errored Frame            0            0
Payload Looback Active            0            0
PRMs Processed (1/sec)            0            0
```

Example for Channelized T1:

```
  statistics
  Link:   Active    ISDN Firmware:   0.0    Handler State: Running

Transmit                   Receive

Packets             44     Packets            40
Bytes             1600     Bytes            1520
Overflow             0     Overflow            0
Underrun             0     Too Long            0
                           Abort               0
                           CRC error           0
                           Misaligned          0

T1 Status Register         T1 Error Count Registers

Receive AIS         : Off  LCV  Errors:           0
Receive RAI         : Off  CRC6 Errors:           0
Receive Carrier Loss: Off  Sync Errors:           0
Receive Loss of Sync: Off
Payload Loopback    : Off
Line    Loopback    : Off

T1 PRM Events                 Local       Remote

CRC Error                         0            0
Controlled Slip                   0            0
Line Code Violation               0            0
Frame Sync Bit Error              0            0
Severely Errored Frame            0            0
Payload Looback Active            0            0
PRMs Processed (1/sec)           46           46
```

ISDN and the GWCON Commands

While ISDN has its own monitoring process for monitoring purposes, the router also displays configuration information and complete statistics for devices and circuits when you use the **interface, statistics,** and **error** commands from the GWCON environment. You can also use the GWCON **test** command to test DCEs and circuits.

Note: Issuing the **test** command to the ISDN interface causes the current calls to be dropped and re-dialed.

Interface — Statistics for ISDN Interfaces and Dial Circuits

Use the **interface** command at the GWCON prompt (+) to display statistics for ISDN interfaces and dial circuits.

To display statistics for a dial circuit, enter the **interface** command followed by the interface number of the dial circuit. For ISDN interfaces, information is displayed on a D and B channel basis. (This is the same information that is displayed by the ISDN **statistics** command.)

Example:

```
interface 2

                                        Self-Test  Self-Test  Maintenance
Nt Nt'  Interface  Slot-Port            Passed     Failed     Failed
2  2    ISDN/0     Slot: 8  Port: 1          1          0          0

  ISDN Base Net MAC/data-link on ISDN Primary Rate interface
  Link:   Active    ISDN Firmware:   1.0    Handler State: Running

Transmit    D  Channel     Receive    D  Channel

Packets              36     Packets             36
Bytes               214     Bytes              214
Overflow              0     Overflow             0
Underrun              0     Too Long             0
                            Abort                0
                            CRC error            0
                            Misaligned           0

Transmit    B  Channels    Receive    B  Channels

Packets               0     Packets              0
Bytes                 0     Bytes                0
Overflow              0     Overflow             0
Underrun              0     Too Long             0
                            Abort                0
                            CRC error            0
                            Misaligned           0

T1 Status Register          T1 Error Count Registers

Receive AIS         : Off  LCV  Errors:           0
Receive RAI         : Off  CRC6 Errors:           0
Receive Carrier Loss: Off  Sync Errors:           0
Receive Loss of Sync: Off

T1 PRM Events                 Local       Remote

CRC Error                         0            0
Controlled Slip                   0            0
Line Code Violation               0            0
Frame Sync Bit Error              0            0
Severely Errored Frame            0            0
Payload Looback Active            0            0
PRMs Processed (1/sec)          365          367
```

To display the following statistics for a dial circuit, use the **interface** command followed by the interface number of the dial circuit.

Example:

```
interface 3
                                  Self-Test  Self-Test  Maintenance
Nt Nt'  Interface                 Passed     Failed     Failed
3  2    PPP/1                         1          0          0

  Point to Point MAC/data-link on ISDN Primary Rate interface
```

The following list describes the output for both ISDN and dial circuits.

Nt Serial line interface number or dial circuit interface number.

Nt' If *Nt* is a dial circuit, this is the interface number of the ISDN interface to which the dial circuit is mapped.

Interface
Interface type and its instance number.

Slot The slot that contains the ISDN adapter

Port The port number on the ISDN adapter.

Self-Test Passed
Number of self-tests that succeeded.

Self-Test Failed
Number of self-tests that failed.

Maintenance: Failed
Number of maintenance failures.

Configuration - Information on Router Hardware and Software

Enter the **configuration** command at the GWCON (+) prompt to display information about the router hardware and software. It includes a section that displays the interfaces configured on the router along with the state of the interface.

If a dial circuit is configured to dial-on-demand, the state of the dial circuit is always displayed as Up whether or not it is connected. In this case Up means that the dial circuit is either connected or available.

If a dial circuit is configured as a static circuit, the state indicates Up only if the dial circuit is connected. (Refer to “Configuration” on page 114 for a sample output from the **configuration** command.

Chapter 42. Configuring and Monitoring Dial Circuits

This chapter describes how to configure dial circuits on a dial circuit interface mapped to a V.25bis, V.34,or ISDN interface. It contains the following sections:

- "Dial Circuit Configuration Commands"
- "Dial Circuit Monitoring Commands" on page 570

Dial-in and Dial-out interfaces are special types of dial circuit interfaces.

Notes:

1. PPP dial circuit interfaces can use an ISDN, V.25bis, or V.34 network as the base-network interface.
2. FR dial circuit interfaces can use an ISDN or a V.25bis network as the base network interface.
3. Switched SDLC Call-In dial circuit interfaces use a V.25bis network as the base-network interface.
4. X.25 circuits can be used over ISDN D-channels for BRI.
5. Dial-Out circuit interfaces use a V.34 network as the base-network interface.
6. Dial-In circuit interfaces can use an ISDN network as the base-network interface.

For information on how to configure dial circuits for use with:

- ISDN interfaces, see "Chapter 40. Using the ISDN Interface" on page 531.
- V.25bis interfaces, see "Chapter 36. Using the V.25bis Network Interface" on page 499 .
- V.34 interfaces, see "Chapter 38. Using the V.34 Network Interface" on page 515.

Dial Circuit Configuration Commands

Table 67 describes the dial circuit configuration commands. Enter the dial circuit configuration commands at the `Circuit Config>` prompt. You must restart the router for configuration changes to take effect.

To access the `Circuit Config>` prompt, enter the **network** command followed by the interface number of the "dial circuit". (The dial circuit number was assigned when you entered the **add device dial-circuit** command.) You can enter the **list devices** command at the `Config>` prompt to display a list of the dial circuits that you added.

Table 67. Dial Circuit Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 12.
Delete	Deletes the inbound call settings from the dial circuit configuration.
Encapsulator	Allows you to change the data-link protocol configuration.
List	Displays the dial circuit configuration parameters.

Table 67. Dial Circuit Configuration Commands Summary (continued)

Command	Function
Set	Configures the dial circuit for inbound or outbound calls, maps the dial circuit to a serial line interface, and sets addresses, idle timeout, priority, lid_out address, inbound destination, and self-test delay.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Delete

Use the **delete** command to remove the inbound call settings from the dial circuit configuration.

Syntax:

delete inbound *destination*

inbound *destination*
Removes both the INBOUND destination and the ANY_INBOUND settings from the dial circuit configuration. This causes the dial circuit to accept calls only from callers that have a phone number that matches the *destination* parameter.

Encapsulator

Use the encapsulator command to enter the configuration process for the link-layer protocol (for example. PPP, Frame Relay, X.25 , dial-out, SDLC) that is running on the dial circuit interface.

Note: The default for a dial circuit interface created via the **add device dial-circuit** command is PPP. To change the link layer type, at the `Config>` prompt:

- For Frame Relay, enter **set data-link frame-relay**.
- For SDLC, enter **set data-link sdlc**.
- For X.25 on the ISDN BRI D-channel, enter **set data-link x25**.

Syntax:

encapsulator

The following example shows that the PPP configuration process is entered when the encapsulator command is used for a PPP dial circuit or dial-in interface.

Example:

```
encapsulator
Point-to-Point user configuration
PPP Config>
```

Be aware of the following when you configure a dial circuit that uses a V.25bis interface as the base network:

- The V.25bis interface pre-defines clocking as external. The modem (DCE) controls the clock speed. You cannot configure clocking, encoding, and other HDLC parameters as part of the dial circuit configuration.

Be aware that you cannot configure HDLC parameters of the dial circuit configuration when you configure PPP or Frame Relay for ISDN. Physical layer parameters are configured on the ISDN interface.

For information on configuring the PPP protocol, refer to “Chapter 20. Configuring Serial Line Interfaces” on page 239 or refer to “Chapter 27. Using Point-to-Point Protocol Interfaces” on page 371.

For information on configuring the Frame Relay protocol, see “Chapter 25. Using Frame Relay Interfaces” on page 309 or “Chapter 26. Configuring and Monitoring Frame Relay Interfaces” on page 327.

For information on configuring or monitoring SDLC interfaces, see “Chapter 32. Using SDLC Interfaces” on page 459 or “Chapter 33. Configuring and Monitoring SDLC Interfaces” on page 461.

For more information on configuring dial-in and dial-out interfaces, see “Using a Dial-In Access to LANs (DIALs) Server” in the *Using and Configuring Features*.

For information on configuring or monitoring X.25 interface, see “Chapter 22. Configuring and Monitoring the X.25 Network Interface” on page 249.

To return to the `Circuit Config>` prompt, use the **exit** command.

List

Use the **list** command to display the current dial circuit configuration.

For more information about I.430 and I.431, see “ISDN I.430 and I.431 Switch Variants” on page 544.

Syntax:

list

Example:

Note: Options listed depend upon the type of interface used. All options may not be shown for all interface types.

```
list
Any inbound             set
Bandwidth:              64
Base net:               1
Callback:               yes
Calls:                  inbound
Destination name:       remote-site-sanfrancisco
Idle char:              7E
Idle timer:             = 60 sec
Inbound calls           allowed
Inbound dst name:       local-1
LID out address:        1234
LID used:               enabled
Net #:                  2
Outbound calls          allowed
Priority:               8
SelfTest Delay Timer:   = 0 ms
Time slot:              1 4 5 8
```

Any inbound

Displays this setting when inbound calls that do not match any other dial circuit are mapped to this circuit and accepted as inbound calls.

Bandwidth
Displays the bandwidth value in Kbps.

Base net
Displays the name of the serial line interface to which this dial circuit is mapped.

Callback
Displays the setting of this option.

Calls Displays the setting of this option.

Destination name
Displays the network address name to be called for outbound circuits, and the default comparison address used by the LID mechanism for inbound calls.

Idle char
Displays the idle character used for I.43x or channelized circuits.

Idle timer
Displays the idle timer setting in seconds. The range is 0 to 65535; 0 indicates that this is a dedicated circuit (leased line).

Inbound calls allowed
Displays this parameter when the circuit is configured to accept inbound calls.

Inbound dst name
Displays this parameter if the circuit is configured to accept inbound calls that do not match any other addresses. This is an alternate comparison address name used by the LID mechanism for inbound calls.

LID out address
Displays the name of the dial circuit connecting the routers.

LID used
Displays the setting of this option.

Net # Displays the base circuit number.

Outbound calls allowed
Displays this parameter when the circuit is configured to initiate outbound calls.

Priority
Displays the setting of this parameter.

SelfTest Delay Timer
Displays the self-test delay timer setting in milliseconds. The range is 0 to 65535; 0 indicates no delay.

Time slot
Displays the list of slots to use for this dial circuit.

Set

Use the **set** command to map the dial circuit to an interface (for example: ISDN or V.25bis), configure the dial circuit for inbound and/or outbound calls, and set destination addresses, inbound addresses, idle timeout, and self-test delay.

Note:

Notes:

1. If you are running SDLC, I.430, I.431, Channelized, or X.25 on a dial circuit, you will be unable to use the **set** command to change the following parameters as the software will use specific defaults:
   - Any_inbound - any_inbound is set
   - Calls - inbound
   - Destination - default address
   - Inbound destination - no destination inbound address
   - Idle - 0
   - Lid_out_addr - no LID name
   - Lid_used - disabled
   - Priority - 8
   - Self_test_delay
2. If you are running a dial circuit on V.34, you will be unable to change the following parameters:
   - Bandwidth
   - Callback
   - Idle-char
   - lid_out_addr
   - timeslot

Syntax:

set
- any_inbound
- bandwidth...
- callback...
- calls...
- destination...
- idle...
- idle-char...
- inbound destination...
- lid_out_addr...
- lid_used...
- net...
- priority...
- selftest-delay...
- timeslot...

any_inbound

Specifies that inbound calls that do not match any other dial circuit will be mapped to this circuit and accepted as inbound calls.

bandwidth *kbps*

Sets the bandwidth, in Kbps, for ISDN, I.430, and Channelized T1/E1 circuits.

Valid values:

For I.430: 64 or 128

For Channelized: 56 or 64

For ISDN: 56 or 64

Default value: 64

callback [*Yes* **or** *No***]**

The callback feature uses the callers telephone number to verify the call against an authentication table and then disconnects the incoming call. Callback then makes an outgoing call to the same caller. Callback should always be disabled. The default is no.

calls [*outbound* **or** *inbound* **or** *both***]**

Restricts this dial circuit to initiating outbound calls only, accepting inbound calls only, or both initiating and accepting calls. The default is both.

destination *address_name*

This parameter is required for the dial circuit to operate. It specifies the network dial address of the remote router to which this dial circuit will connect. The LID protocol uses this parameter as the default comparison address for incoming calls. This parameter must match an address name that you assigned using the `Config>` prompt with either the **add isdn address** command, the **add v25-bis address** command, or the **add v34-address** command.

Example: `set destination remote-site-sanfrancisco`

idle *# of seconds*

Specifies a timeout period for the circuit. If there is no protocol traffic over the circuit for this specified time period, the dial circuit hangs up. The range is 0 to 65535, and the default is 60 seconds. A setting of zero specifies that there is no timeout period and that this is a dedicated circuit.

Notes:

1. For WAN Restoral operations, you must set the idle timeout to 0.
2. On a I.43x, X.25 or Channelized circuit, you cannot set this parameter.

idle-char

Specifies the idle character used for I.43x or channelized circuits.

Note: You cannot configure this parameter for regular ISDN circuits.

Valid values: 7E or FF

Default value: 7E

Example: `set idle-char 7E`

inbound-destination *address_name*

Set this parameter if the dial circuit is set up for both inbound and outbound calls and if this router's local dial address is different from the destination dial address that the remote router dials. For example, the numbers would be different if one of the routers must go through a PBX, international, or inter-LATA exchange. This parameter must match an address name that you assigned at the `Config>` prompt with either the **add isdn address** command, the **add v25-bis address** command, or the **add v34-address** command. The inbound destination number is used to match the incoming LID or CallerID with the dial circuit. If there is a match that dial circuit gets the call.

Example: `set inbound remote-site-1`

lid_out_addr *address_name*
The lid_out_addr is the name of a dial circuit between two routers. When more than one circuit is configured between two routers (parallel circuits), then there needs to be a way to unambiguously know which dial circuit connects between them. For this purpose, a lid_out_addr is sent from the router at one end (the caller). At the receiving end the other router configures the same string as the inbound destination name. The lid_out_addr must be an address name that has previously been added using **ADD ISDN-ADDRESS** from the config> prompt.

lid_used [enabled or disabled]
Suppresses the exchange of logical ids for circuits to devices that do not support logical ids.

Valid values: Enabled or disabled

Default value: Disabled

net *#*
Sets the base network number of the interface to the *#* of the serial line interface to which you want to map this circuit.

Note: The interface must be a V.34 net for dial-out interfaces. You are prompted for this if you add the device.

Example:

```
Circuit Config> set net
Base net for this circuit [ ]? 2
```

priority
The priority field allows an outbound dial-on-demand circuit to preempt another when no channels are available. If a call request is made and all the channels are in use, then the priority of the requesting dial-on-demand circuit is checked against all the active dial-on-demand circuits. If there is an outbound dial-on-demand circuit with lower priority, then that circuit is disconnected and a call is made for the higher priority dial-on-demand circuit. Only the priority on the outbound end of a connection is considered. An inbound dial-on-demand call will not be taken down in favor of a higher priority outbound call. An inbound dial-on-demand call cannot cause a lower priority call to be taken down.

selftest-delay *# of milliseconds*
Use this parameter to delay the time between when the call is established and the time when the initial packet is sent. Setting a selftest-delay can prevent initial packets from being dropped. The range is 0 to 65535, and the default is 150.

For V.25bis dial circuits, adjust this setting if your modems take extra time to synchronize.

For ISDN dial circuits, you may need to adjust this setting for dial-on-demand links because some ISDN switches start to deliver data before signalling the complete establishment of the circuit at the destination end.

timeslot *list of slots*
Specifies a slot or list of slots to use for this dial circuit. Your service

provider will issue the number of the slots you can use for the circuit. Specify the list as slot numbers separated by blanks.

Note: You can only use this parameter for Channelized T1/E1 circuits.

Valid values:

For Channelized T1: 1 to 24

For Channelized E1: 1 to 31

Default value: None

Example: `set timeslot 1 4 5 8`

Dial Circuit Monitoring Commands

Table 68 describes the dial circuit monitoring commands. Enter the dial circuit monitoring commands at the `Circuit Config>` prompt. You must restart the router for monitoring changes to take effect.

Table 68. Dial Circuit Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 12.
Callback	Adds, deletes, or lists the information in the authentication cache.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 13.

Callback

Use the **callback** command to add, delete or list the information in the authentication cache.

Syntax:

callback add
delete
list

add Adds a callback number to the athentication lists.

delete Deletes a callback number from the authentication lists

list Lists the callback numbers and other information in the authentication list.

Appendix A. Quick Configuration Reference

Important

If you are attempting to configure or monitor your IBM 2212 and your service terminal is unreadable, see “Service Terminal Display Unreadable” in IBM 2212 Access Utility Service and Maintenance Manual.

Quick Configuration Tips

Before starting the Quick Configuration process, read these notes:

1. Attach an ASCII terminal to the service port to run the Quick Configuration program. See the *Installation and Initial Configuration Guide*.
2. Any existing configuration for a particular item will be removed if that item is configured through Quick Configuration.
3. Configuration is done at the level of the *interface*, which corresponds to a single *port* on an adapter.
4. Using the **add device** command, you must “add” all desired network interfaces or virtual interfaces for the adapters installed in your IBM 2212. This must be done prior to running Quick Configuration. To add an interface, see “Add” on page 76 .
5. Using the **network** command, you must enter the network interface configuration information. See “Network” on page 96.

Making Selections

On the panels that you view when using the Quick Configuration program, the information shown in brackets, [ ], is the default. For example:

```
Configure Bridging? (Yes, No, Quit): [Yes]
```

- To use the default `Yes`, press **Enter**.
- To use a value other than the default, such as `No` or `Quit`, choose from the values in the parentheses.
- If no value appears in the brackets, there is no default and you must type a value.

Exiting and Restarting

- To restart the current Quick Configuration section at any time, type **r**. For example, if you are in the Interface Configuration section, type **r** and press **Enter** to return to the beginning of that section.
- To exit Quick Configuration, type **q** and press **Enter**. The `Config>` prompt will appear.
- To restart Quick Configuration from the `Config>` prompt, type **qc** and press **Enter**.

When You’re Done

- Once you have completed your configuration, you must restart the IBM 2212 for the configuration to take effect. At the end of the Quick Configuration program, you are given this option.

Starting the Quick Configuration Program

The following sections describe sample configurations using the Quick Configuration program (**qconfig**).

To start the quick configuration program, enter **qc** at the Config> prompt.

The program displays the following panel after starting.

```
Router Quick Configuration for the following:

o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP, and SNMP)
        IPX
        DNA (DECnet)

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note: Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

Event logging records system activity, status changes, data transmission and reception, data and internal errors, and service requests. The logging level is set to standard (the default). For more information about error logging, refer to the *Event Logging System Messages Guide*.

During Quick Configuration you can:

1. Configure bridging
2. Configure protocols
3. Restart the router

Configuring Bridging

```
*********************************************
Bridging Configuration
*********************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes]
```

1. In response to Configure Bridging, take one of the following actions:
   - Enter **y** to display the bridging configuration prompts. The prompts that appear depend on your network configuration.
   - Enter **n** to skip the bridging configuration and continue with quick configuration.
   - Enter **q** to exit quick configuration. This displays the Config> prompt. To reenter quick configuration, enter **qc** after this prompt.
2. If you choose to configure bridging, Spanning Tree Bridging (STB) will be enabled on all LAN interfaces. You will see the following panels:

```
Type 'r' any time at this level to restart Bridging Configuration

STB will be enabled on all LAN interfaces
```

Enter **y** to configure SRT bridging. Otherwise, enter **n**. For each Token-Ring interface in the configuration, you will be prompted to enable Source Routing on the interface.

```
Configure SRT Bridging? (Yes, No): [Yes]
You are now configuring the Source Routing part of SRT Bridging
Bridge Number (hex) of this Router (1-F): [A]
```

3. Enter a bridge number, which is a hexadecimal value from 1 to F that is unique between two parallel segments.

```
Interface 0 (Port 1) is of type Token Ring
Configure Source Routing on this interface (Yes, No): [Yes]
```

4. Enter **y** to configure source routing on the interface. The console displays the next two lines.

```
Configuring Interface 0 (Port 1)
Segment Number (hex) of this Interface (1-FFF): [A1]
```

Note: The port number increases by one because source routing bridging does not allow a port number of zero.

A unique hexadecimal value from 1 to FFF is assigned to each interface. The interfaces on each ring (segment) have the same segment number, but the segment number is unique to each ring.

These prompts appear for each Token Ring interface.

```
Interface 1 (Port 2) is of type Token Ring
Configure Source Routing on this interface? (Yes, No): [Yes]
Configuring Interface 1 (Port 2)
Segment Number (hex) of this Interface (1-FFF): [A2]
```

If more than two interfaces are configured for source routing, enter a unique hexadecimal value from 1 to FFF unique for the internal virtual segment.

```
Virtual Segment Number (hex) of this Router (1-FFF): [A4]
```

5. A panel similar to the following is displayed:

```
This is all configured bridging information:

       Interfaces configured for STB:

       Interface #    Port #     Interface Type

           0          1          Token Ring
           1          2          Token Ring

The Source Routing part of SRT Bridging has been enabled

Bridge Number of this Router: A

Interfaces configured for Source Routing:

       Interface #     Port#      Segment #   Interface Type

           0             1          A1        Token Ring
           1             2          A2        Token Ring

Virtual Segment Number of this Router:  A4

Save this Configuration? (Yes, No): [Yes]
```

6. Enter **y** to save the bridging configuration and continue with quick configuration. Enter **n** to re-display the bridging configuration prompts.

   If you enter **y**, the following message appears:

```
Bridging configuration saved
```

Configuring Protocols

After you save the bridging configuration, you will see the following panel:

```
*********************************************
Protocol Configuration
*********************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
```

Take one of the following actions:

- Enter **y** to configure the protocols.
- Enter **n** to skip protocol configuration and continue with quick configuration.
- Enter **q** to exit quick configuration.

You will first configure IP, then IPX, and then DECnet.

Configuring IP

When you answer **y** to the Configure Protocol panel, quick configuration displays the following messages:

```
Type 'r' any time at this level to restart Protocol configuration

Configure IP? (Yes, No): [Yes]
```

1. Take one of the following actions:
   - Enter **y** to configure IP.

- Enter **n** to skip IP configuration and continue with quick configuration.

The following lines appear for each interface.

```
Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [ ] 128.185.141.1
Address Mask: [255.255.0.0]
```

2. Enter the IP address in decimal notation for example, 128.185.142.20. The console displays one of the following error messages if you enter an invalid IP address:

   ```
   Bad address, please try again.

   This address has already been assigned.  Enter a different address
   ```

   Address mask is a decimal value that reflects the IP network or subnetwork to which this interface is attached.

   For more information about IP addressing or address masks, refer to the *Protocol Configuration and Monitoring Reference*, or consult your network administrator.

   ```
   Per-Interface IP Configuration complete

   Configuring IP Routing Information
   Enable Dynamic Routing (Yes, No): [Yes]
   ```

3. Enter **y** if you want the routing protocols (RIP or OSPF) to build the routing tables. Enter **n** to manually add IP address destinations to the routing tables (static routes).

   ```
   Enable OSPF? (Yes, No): [Yes]
   ```

4. Enter **y** to enable the OSPF routing protocol as the primary dynamic IP routing protocol. RIP will be enabled only to send advertisements, not to receive them. Enter **n** if you do not want to use OSPF. RIP will be enabled to send and receive advertisements.

   ```
   OSPF Enabled with Max routes = 1000  and Max routers = 50
   ```

   Max routes is the maximum number of autonomous system (AS) external routes imported into the OSPF routing domain. Max routers is the maximum number of OSPF routers in the routing domain.

```
Routing Configuration Complete

SNMP will be configured with the following parameters:

Community: public
Access:    READONLY

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No):  [Yes]


This is the information you have entered:

          Interface #        IP Address     Address Mask

             0               128.185.141.1  255.255.255.0
             1               128.185.142.1  255.255.255.0
             2               128.185.143.1  255.255.255.0

OSPF is configured, and RIP is configured only for 'sending'

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

     Community: dana
     Access:    read_write_trap

Save this configuration? (Yes, No): [Yes]
```

5. Enter **y** to save the IP configuration and continue with quick configuration. Enter **n** to re-display the protocol configuration prompts.

Configuring IPX

After you save the IP configuration, you will see the following messages:

```
Configure IPX? (Yes, No): [Yes]
```

1. Enter **y** to configure IPX. Enter **n** to skip IPX configuration and continue with quick configuration.

   You will see messages similar to the following:

   ```
   Type 'r' any time at this level to restart IPX Configuration
   IPX Configuration is already present
   Configure IPX anyway? (Yes, No): [No] yes
   ```

2. Enter **y** to replace the existing configuration. Enter **n** to keep the current configuration and continue.

   ```
   Configuring Per-Interface IPX Information

   Configuring Interface 0 (Token Ring)
   Configure IPX on this interface? (Yes, No): [Yes]
   ```

3. The next messages and your responses depend on whether you are configuring Token-Ringor Ethernet.

   Configuring IPX for Token-Ring:

   a. The following prompt is displayed:

```
Token Ring encapsulation (frame) type? (TOKEN–RING MSB, TOKEN–RING LSB,
    TOKEN–RING_SNAP MSB, TOKEN–RING_SNAP LSB): [TOKEN–RING MSB]
```

b. Enter the encapsulation type used by the IPX protocol on your Token-Ring end stations.

`Token–Ring MSB:`	Most common encapsulation type and the default. The IBM 2212 builds outgoing packets with a 3-byte 802.2 header, (0xE0, 0xE0, 0x03). It sends the source and destination addresses in MSB (most significant bit), or noncanonical, format, which is the native address format for Token-Ring.
`Token–Ring LSB`	Same as Token-Ring MSB except the IBM 2212 sends the addresses in LSB (least significant bit), or canonical, format.
`Token-Ring SNAP MSB`	The IBM 2212 builds outgoing packets with an 8-byte 802.2/SNAP header (0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37). It sends the source and destination addresses in most significant bit (MSB), or noncanonical, format.
`Token-Ring SNAP LSB`	Same as Token-Ring SNAP MSB except the IBM 2212 sends the addresses in LSB, or canonical, format.

Configuring IPX for Ethernet:

a. The following prompts are displayed:

```
Ethernet encapsulation type? (ETHERNET_8022, ETHERNET_8023, ETHERNET_ii,
ETHERNET_SNAP): [ETHERNET_8023]
```

b. Enter the encapsulation type used by the IPX protocol on your Ethernet end stations.

`Ethernet_8022`	Packet includes an 802.2 header.
`Ethernet_8023`	Uses an IEEE 802.3 packet format without the 802.2 header. This is the default and the default for NetWare versions prior to 4.0. Ethernet 802.3 does not conform to the IEEE 802 standards because it does not include an 802.2 header. It may cause problems with other nodes on the network.
`Ethernet_II`	Uses Ethernet type 8137 as the packet format. This format is required if you are using NetWare VMS on the Ethernet. This is the default for NetWare Versions 4.0 and higher.
`Ethernet_SNAP`	Uses the 802.2 format with a SNAP header. This encapsulation type is meant to be compatible with token-ring SNAP encapsulation. However, it violates IEEE standards and is not interoperable across conformal bridges.

4. Assign an IPX network number to the associated directly connected network. Every IPX interface must have a unique network number.

```
Configuring Interface 1 (WAN PPP)
Configure IPX on this interface? (Yes, No): [Yes]
Network Number (hex) (1-FFFFFFFD): [1] 2

Enable IPXWAN? (Yes, No): [No] yes

Configuring Interface 2 (WAN PPP)
Configure IPX on this interface? (Yes, No): [Yes]
Network Number (hex) (1-FFFFFFFD):[1] 3

Enable IPXWAN? (Yes, No): [No] yes

Host Number for Serial Lines: (000000000000) 1

Configure IPXWAN NodeID? (Yes, No): [Yes]
NodeID (hex) (1 - FFFFFFFD): [1] 4
```

If enabled, the IPXWAN protocol negotiates routing parameters to be used on the PPP serial interface before IPX packet forwarding begins. IPXWAN is not required to forward IPX packets on PPP serial interfaces. The IPXWAN Node ID is a unique IPX network number that identifies the router, and is required if IPXWAN is enabled on any network interfaces.

5. Host number is a unique 12-digit hexadecimal value assigned to an IPX router. It is required because serial lines do not have hardware node addresses from which to build a host number.

```
This is the information you have entered:

               Per-Interface Configuration Information

Cir   Ifc   IPX Net(hex)   Encapsulation       IPXWAN

1     1     10            ETHERNET_8023       Not Configured
2     3     300                               Not Configured
3     5     400                               Not Configured
4     6     600                               Enabled


  Host Number for Serial Lines: 0002210A0000
  IPXWAN Node ID = 2210A
  IPX Router Name = ipxwan_router-2210A


Save this configuration? (Yes, No): [Yes]
```

6. Enter **y** to save the IPX configuration and continue with quick configuration. Enter **n** to re-display the IPX configuration prompts.

   If you enter **y**, the following message appears:

```
IPX configuration saved
```

Configuring DECnet (DNA)

After you save the IPX configuration, you will see the following messages.

```
IPX Configuration saved

Configure DNA? (Yes, No): [Yes]
```

1. Enter **y** to configure DNA. Enter **n** to skip DNA configuration and continue with quick configuration.

```
Type 'r' any time at this level to restart DNA Configuration

Configuring Global DNA information

Highest Node Number (decimal) (1-1023): [32]
Router Level (Level1, Level2, DEC Level1, DEC Level2):
  [ Level2]
Highest Area (decimal) (1-63): [63]
Node Address (area.node): (63.32)
```

The above configuration fields are configured with the following considerations:

Highest Node Number
Is the highest node address in the router's area. Setting it excessively high will affect the routers efficiency and require excess storage.

Router Level
Identifies whether the router is a Level 1 or Level 2 router. A Level 1 router keeps track of all nodes in its area and does not care about nodes outside its area. A Level 2 router routes traffic between areas.

Normally you should select Level1 or Level2 with the following exception: select DEC Level1 or DEC Level2 only when this router must communicate over X.25 networks with routers conforming to the DEC X.25 standard.

Highest Area
This number should be at least as high as the highest area number in the overall network.

Node Address
Is the node ID of this router and must be unique in the network.

When you press Enter, the following is displayed:

```
Configuring Per-Interface DNA Information

Configuring Max Routers on each interface

Configuring Interface 0 (Ethernet)
Configure DNA on this interface? (Yes, No) [YES]
Max Routers (decimal) (1-33): [16]

Configuring Interface 1 (WAN PPP)
Configure DNA on this interface? (Yes, No) [Yes]

Configuring Interface 2 (Token Ring)
Configure DNA on this interface? (Yes, No) [Yes]
Max Routers (decimal) (1-33): [16]
```

2. Enter **y** for every interface that will be connected to the DECnet network. For LANs, Max Routers specifies how many other routers may be on this circuit. For router efficiency and memory requirements set this argument to a few more than the total number of adjacent routers on this circuit.

   The following panel is displayed:

```
This is the information you have entered:

        Global Configuration Information

           Highest Node Number:       32
           Router Level:              Level2
           Highest Area:              63
           Node Address:              63.32

        Pre-Interface Configuration Information
      Interface Number           Max Routers

              0                          16
              1                          1
              2                          16

Save this configuration? (Yes, No): [Yes]
```

3. Enter **y** to save the DECnet configuration and continue with the quick configuration. Enter **n** to re-display the DECnet configuration prompts.

   If you enter **y**, the following message appears:

```
DNA Configuration Saved
```

Restarting the IBM 2212

After configuring the protocols, you will receive the following message:

```
Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
```

Enter **y** to save your changes and display the following information:

```
Default config file written successfully.

Configuration was written.
The system must be restarted for this configuration to take effect.
```

Enter **restart** at the OPCON prompt (*) to restart the IBM 2212 with the new configuration. To change or view the current configuration, enter **qc**.

Appendix B. X.25 National Personalities

This appendix lists the default settings for GTE-Telenet and DDN.

GTE-Telenet

The following parameters are the default settings for GTE-Telenet:

- Callreq: 20
- Clearreq:
  - Retries: 1
  - Timer: 18
- Disconnect: Passive
- DP-timer: 500 milliseconds
- Frame window size: 7
- Network Type: CCITT
- N2 timeouts: 20
- Packet:
  - Default size: 128
  - Maximum size: 256
  - Window size: 2
- Reset
  - Retries: 1
  - Timer: 18
- Restart
  - Retries: 1
  - Timer: 18
- Standard: 1984
- T1-timer: 4
- T2-timer: 2

DDN

The following parameters are the default settings for DDN:

- Callreq: 20
- Clearreq:
  - Retries: 1
  - Timer: 18
- Disconnect: Passive
- DP-timer: 500 milliseconds
- Frame window size: 7
- Network Type: CCITT
- N2 timeouts: 20
- Packet:
  - Default size: 128
  - Maximum size: 256

  - Window size: 2
- Reset
  - Retries: 1
  - Timer: 18
- Restart
  - Retries: 1
  - Timer: 18
- Standard: 1984
- T1-timer: 4
- T2-timer: 2

Appendix C. Making a Router Load File from Multiple Disks

If a software load arrives on multiple disks, use the procedure in the following sections to combine the loads into one load file that the router can use at the time of booting.

The first disk contains the following four files that you need if you want to fragment an existing load for transport on multiple diskettes.

cutup.c
(UNIX C source file that can be compiled using a standard C compiler)

cutup.exe
(DOS)

Use the following files for reassembling the load fragments onto a DOS or UNIX server.

kopy.bat
(DOS)

kopy (UNIX shell script)

Assembling a Load File Under DOS

To assemble a load from the two diskettes, use the DOS batch file provided on diskette 1 (KOPY.BAT) using the following syntax:

kopy <*installation_drive***><***destination_directory***>**

Before assembling the load make sure that you have created a destination directory, and that you have inserted the first diskette in the drive specified by the installation_diskette_drive parameter. The following example illustrates this procedure.

```
B:\>kopy b: c:\source\cutup\tmp
B:\>copy c:\gw0/B c:\source\cutup\tmp\gw.tmp
1 file(s) copied
.
Please mount the second diskette
Press any key to continue . . .
Copying the second load file fragment
B:\>
B:\>copy c:\source\cutup\tmp\gw.tmp/B + b:\gw1
c:\source\cutup\tmp\gw.tmp  c:\SOURCE\CUTUP\TMP\GW.TMP
B:\GW1
1 file(s) copied
B:\>rename c:\source\cutup\tmp\gw.tmp  gw.ldc
Load file reassembly was successful
B:>
```

Assembling a Load File Under UNIX

To assemble a load from two UNIX diskettes, you can use the UNIX Bourne shell script (kopy) provided on diskette 1 using the following syntax:

kopy<*installation_drive*><*diskette_directory*><*destination_directory*

Before assembling the load make sure that you have created the mount and destination directories, and that you have inserted the first diskette in the drive specified by the installation_diskette_drive parameter. The following example illustrates this procedure.

```
kopy /dev/fd0 /kew /pcfs

Please insert the first diskette

Copying the first load file fragment

Please mount the second diskette

Copying the second load file fragment

Load file reassembly was successful

# ls /kew

gw0   gw1   gw.ldc
```

If you can't use the UNIX Bourne shell script, you can assemble the load manually using the following procedure:

1. Copy the load fragments on the two diskettes (gw0 and gw1) into a directory on the UNIX file system.
2. Type the following UNIX command:

   ```
   cat gw0 gw1 > gw.ldc
   ```

   The resulting file (gw.ldc) is the assembled router load.

Disassembling a Load File Under DOS

To disassemble a load under DOS, use the CUTUP.EXE file as follows:

cutup<*file_extension*><*file_name*><*cut_length*>

The file_extension is attached to the front of each slice needed to cut. The file_name is the DOS file name of the file to be disassembled. The cut_length is the length that CUTUP.EXE makes each fragment as it disassembles the file. The following example illustrates this procedure.

```
C: \source\cutup>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      LDC 10225660728931:22p
CUTUP   EXE   105410902939:38a
2 file(s)   1033107 bytes
14811136 bytes free
C: \source\cutup>cutup gw.ldc gw 1000000
.....................................................
.................
.........................
c: \SOURCE\CUTUP>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      0 10000000801931:22p
GW      LDC     10225660728931:22p
CUTUP   EXE   105410902939:38a
GW      1   225660801931:22p
4 file(s)   2055673 bytes
14811136 bytes free
```

Disassembling a Load File Under UNIX

To disassemble a load under use cutup.c. Begin by compiling the program using your UNIX compiler to make a cutup executable file. Then use the following syntax:

cutup<*file_extension*><*file_name*><*cut_length*>

The file_extension is attached to the front of each slice needed to cut. The file_name is the DOS file name of the file to be disassembled. The cut_length is the length CUTUP.EXE that is used to disassemble the file. The following example illustrates this procedure.

```
#  ls -la
total 658
drwxrxrx   2 root    512 Aug  114:41  .
drwxrxrx  26 root   1024 Aug  114:41  ..
drwxrxrx   2 root  24576 Aug  114:41  cutup
drwxrxrr   2 root1022566 Aug  114:41  gw.ldc

#  cutup gw.ldc gw 100000

#  ls -la

total 658
drwxrxrx   2 root    512 Aug  114:41  .
drwxrxrx  26 root   1024 Aug  114:41  ..
drwxrxrx   2 root  24576 Aug  114:41  cutup
drwxrxrr   2 root1022566 Aug  114:41  gw.ldc
drwxrxrr   2 root1000000 Aug  114:41  gw0
drwxrxrr   2 root  22566 Aug  114:41  gw1
```

List of Abbreviations

AARP AppleTalk Address Resolution Protocol

ABR area border router

ack acknowledgment

AIX Advanced Interactive Executive

AMA arbitrary MAC addressing

AMP active monitor present

ANSI American National Standards Institute

AP2 AppleTalk Phase 2

APPN Advanced Peer-to-Peer Networking

ARE all-routes explorer

ARI/FCI
address recognized indicator/frame copied indicator

ARP Address Resolution Protocol

AS autonomous system

ASBR autonomous system boundary router

ASCII American National Standard Code for Information Interchange

ASN.1 abstract syntax notation 1

ASRT adaptive source routing transparent

ASYNC
asynchronous

ATCP AppleTalk Control Protocol

ATP AppleTalk Transaction Protocol

AUI attachment unit interface

ayt are you there

BAN Boundary Access Node

BBCM Bridging Broadcast Manager

BECN backward explicit congestion notification

BGP Border Gateway Protocol

BNC bayonet Niell-Concelman

BNCP Bridging Network Control Protocol

BOOTP
BOOT protocol

BPDU bridge protocol data unit

bps bits per second

BR bridging/routing

BRS bandwidth reservation

BSD Berkeley software distribution

BTP BOOTP relay agent

BTU basic transmission unit

CAM content-addressable memory

CCITT Consultative Committee on International Telegraph and Telephone

CD collision detection

CGWCON
Gateway Console

CIDR Classless Inter-Domain Routing

CIP Classical IP

CIR committed information rate

CLNP Connectionless-Mode Network Protocol

CPU central processing unit

CRC cyclic redundancy check

CRS configuration report server

CTS clear to send

CUD call user data

DAF destination address filtering

DB database

DBsum
database summary

DCD data channel received line signal detector

DCE data circuit-terminating equipment

DCS Directly connected server

DDLC dual data-link controller

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir directly connected

DL data link

DLC data link control

DLCI data link connection identifier

DLS data link switching

DLSw data link switching

DMA direct memory access

DNA Digital Network Architecture

DNCP DECnet Protocol Control Protocol

DNIC Data Network Identifier Code

DoD Department of Defense

DOS Disk Operating System

DR designated router

DRAM Dynamic Random Access Memory

DSAP destination service access point

DSE data switching equipment

DSE data switching exchange

DSR data set ready

DSU data service unit

DTE data terminal equipment

DTR data terminal ready

Dtype destination type

DVMRP
Distance Vector Multicast Routing Protocol

E1 2.048 Mbps transmission rate

EDEL end delimiter

EDI error detected indicator

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAN Emulated LAN

ELAP EtherTalk Link Access Protocol

ELS Event Logging System

ELSCon
Secondary ELS Console

ESI End system identifier

EST Eastern Standard Time

Eth Ethernet

fa-ga functional address-group address

FCS frame check sequence

FECN forward explicit congestion notification

FIFO first in, first out

FLT filter library

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

GMT Greenwich Mean Time

GOSIP
Government Open Systems Interconnection Profile

GTE General Telephone Company

GWCON
Gateway Console

HDLC high-level data link control

HEX hexadecimal

HPR high-performance routing

HST TCP/IP host services

HTF host table format

IBD Integrated Boot Device

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID identification

IDP Initial Domain Part

IDP Internet Datagram Protocol

IEEE Institute of Electrical and Electronics Engineers

Ifc# interface number

IGP interior gateway protocol

InARP Inverse Address Resolution Protocol

IP Internet Protocol

IPCP IP Control Protocol

IPPN IP Protocol Network

IPX Internetwork Packet Exchange

IPXCP IPX Control Protocol

ISDN integrated services digital network

ISO International Organization for Standardization

Kbps kilobits per second

LAN local area network

LAPB link access protocol-balanced

LAT local area transport

LCS LAN Channel Station

LCP Link Control Protocol

LED light-emitting diode

LF largest frame; line feed

LIS Logical IP subnet

LLC logical link control

LLC2 logical link control 2

LMI local management interface

LRM LAN reporting mechanism

LS link state

LSA link state advertisement

LSA Link Services Architecture

LSB least significant bit

LSI LAN shortcuts interface

LSreq link state request

LSrxl link state retransmission list

LU logical unit

MAC medium access control

Mb megabit

MB megabyte

Mbps megabits per second

MBps megabytes per second

MC multicast

MCF MAC filtering

MIB Management Information Base

MIB II Management Information Base II

MILNET
military network

MOS Micro Operating System

MOSDBG
Micro Operating System Debugging Tool

MOSPF
Open Shortest Path First with multicast extensions

MPC Multi-Path Channel

MPC+ High performance data transfer (HPDT) Multi-Path Channel

MSB most significant bit

MSDU MAC service data unit

MRU maximum receive unit

MTU maximum transmission unit

nak not acknowledged

NAS Nways Switch Administration station

NBMA Non-Broadcast Multiple Access

NBP Name Binding Protocol

NBR neighbor

NCP Network Control Protocol

NCP Network Core Protocol

NDPS non-disruptive path switching

NetBIOS
Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Network Protocol Data Unit

NRZ non-return-to-zero

NRZI non-return-to-zero inverted

NSAP Network Service Access Point

NSF National Science Foundation

NSFNET
National Science Foundation NETwork

NVCNFG
nonvolatile configuration

OPCON
Operator Console

OSI open systems interconnection

OSICP
OSI Control Protocol

OSPF Open Shortest Path First

OUI organization unique identifier

PC personal computer

PCR peak cell rate

PDN public data network

PING Packet internet groper

PDU protocol data unit

PID process identification

P-P Point-to-Point

PPP Point-to-Point Protocol

PROM programmable read-only memory

PU physical unit

PVC permanent virtual circuit

RAM random access memory

RD route descriptor

REM ring error monitor

REV receive

RFC Request for Comments

RI ring indicator; routing information

RIF routing information field

RII routing information indicator

RIP Routing Information Protocol

RISC reduced instruction-set computer

RNR receive not ready

ROM read-only memory

ROpcon
Remote Operator Console

RPS ring parameter server

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS request to send

Rtype route type

rxmits retransmissions

rxmt retransmit

s second

SAF source address filtering

SAP service access point

SAP Service Advertising Protocol

SCR Sustained cell rate

SCSP Server Cache Synchronization Protocol

sdel start delimiter

SDLC SDLC relay, synchronous data link control

seqno sequence number

SGID sever group id

SGMP Simple Gateway Monitoring Protocol

SL serial line

SMP standby monitor present

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol

SNPA subnetwork point of attachment

SPF OSPF intra-area route

SPE1 OSPF external route type 1

SPE2 OSPF external route type 2

SPIA OSPF inter-area route type

SPID service profile ID

SPX Sequenced Packet Exchange

SQE signal quality error

SRAM static random access memory

SRB source routing bridge

SRF specifically routed frame

SRLY SDLC relay

SRT source routing transparent

SR-TB
source routing-transparent bridge

STA static

STB spanning tree bridge

STE spanning tree explorer

STP shielded twisted pair; spanning tree protocol

SVC switched virtual circuit

TB transparent bridge

TCN topology change notification

TCP Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

TEI terminal point identifier

TFTP Trivial File Transfer Protocol

TKR token ring

TMO timeout

TOS type of service

TSF transparent spanning frames

TTL time to live

TTY teletypewriter

TX transmit

UA unnumbered acknowledgment

UDP User Datagram Protocol

UI unnumbered information

UTP unshielded twisted pair

VCC Virtual Channel Connection

VINES VIrtual NEtworking System

VIR variable information rate

VL virtual link

VNI Virtual Network Interface

VR virtual route

WAN wide area network

WRS WAN restoral/reroute

X.25 packet-switched networks

X.251 X.25 physical layer

X.252 X.25 frame layer

X.253 X.25 packet layer

XID exchange identification

XNS Xerox Network Systems

XSUM checksum

ZIP AppleTalk Zone Information Protocol

ZIP2 AppleTalk Zone Information Protocol 2

ZIT Zone Information Table

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems* , ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines* , Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with:
This refers to a term that has an opposed or substantively different meaning.

Synonym for:
This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with:
This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also:
This refers the reader to terms that have a related, but not synonymous, meaning.

A

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in the following standards:

- ITU-T Recommendation X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994

See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device.

active monitor. In a token-ring network, a function performed at any one time by one ring station that initiates the transmission of tokens and provides token error recovery facilities. Any active adapter on the ring has the ability to provide the active monitor function if the current active monitor fails.

address. In data communication, the unique code assigned to each device, workstation, or user connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. (1) A method for mapping network-layer addresses to media-specific addresses. (2) See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). (1) In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. (2) See also *Reverse Address Resolution Protocol (RARP)*.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Administrative Domain. A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

agent. A system that assumes an agent role.

alert. A message sent to a management services focal point in a network to identify a problem or an impending problem.

all-stations address. In communications, synonym for *broadcast address*.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital*.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that (a) translates AppleTalk node addresses into hardware addresses and (b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node*.

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by

definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

backbone network. A central network to which smaller networks, normally of lower speed, connect. The backbone network usually has a much higher capacity than the networks it helps interconnect or is a wide-area network (WAN) such as a public packet-switched datagram network.

backbone router. (1) A router used to transmit data between areas. (2) One in a series of routers that is used to interconnect networks into a larger internet.

Bandwidth. The bandwidth of an optical link designates the information-carrying capacity of the link and is related to the maximum bit rate that a fiber link can support.

basic transmission unit (BTU). In SNA, the unit of data and control information passed between path control components. A BTU can consist of one or more path information units (PIUs).

baud. In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

bootstrap. (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage. (T) (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few instructions are sufficient to bring the rest of itself into the computer from an input device. (A)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems.

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridge identifier. An 8-byte field, used in a spanning tree protocol, composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. (3) Contrast with *multicast*.

broadcast address. In communications, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

canonical address. In LANs, the IEEE 802.1 format for the transmission of medium access control (MAC) addresses for token-ring and Ethernet adapters. In canonical format, the least significant (rightmost) bit of each address byte is transmitted first. Contrast with *noncanonical address*.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier detect. Synonym for *received line signal detector (RLSD)*.

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (T) (A)

CCITT. International Telegraph and Telephone Consultative Committee. This was an organization of the International Telecommunication Union (ITU). On 1 March 1993 the ITU was reorganized, and responsibilities for standardization were placed in a subordinate organization named the Telecommunication Standardization Sector of the Telecommunication Union (ITU-TS). “CCITT” continues to be used for recommendations that were approved before the reorganization.

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal’s performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier’s office channel unit. See also *data service unit (DSU)*.

channelization. The process of breaking the bandwidth on a communication line into a number of channels, possibly of different size. Also called ***time division multiplexing*** (TDM).

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

class A network. In Internet communications, a network in which the high-order (most significant) bit of the IP address is set to 0 and the host ID occupies the three low-order octets.

class B network. In Internet communications, a network in which the two high-order (most significant and next-to-most significant) bits of the IP address are set to 1 and 0, respectively, and the host ID occupies the two low-order octets.

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

Committed information rate. The maximum amount of data in bits that the network agrees to deliver.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

compression. (1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. (2) Any encoding to reduce the number of bits used to represent a given message or record.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration database (CDB). A database that stores the configuration parameters of one or several devices. It is prepared and updated using the configuration program.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

configuration report server (CRS). In the IBM Token-Ring Network Bridge Program, the server that accepts commands from the LAN Network Manager (LNM) to get station information, set station parameters, and remove stations on its ring. This server also collects and forwards configuration reports generated by stations on its ring. The configuration reports include the new active monitor reports and the nearest active upstream neighbor (NAUN) reports.

congestion. See *network congestion*.

connection. In data communication, an association established between functional units for conveying information. (I) (A)

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT)*.

D

D-bit. Delivery-confirmation bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data carrier detect (DCD). Synonym for *received line signal detector (RLSD)*.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection*. (3) See also *physical circuit* and *virtual circuit*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal

conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T)

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level*. (2) In X.25 communications, synonym for *frame level*.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing*.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready (DSR). Synonym for *DCE ready*.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. (3) See also *packet* and *segment*.

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

DCE ready. In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that the local data circuit-terminating equipment (DCE) is connected to the communication channel and is ready to send data. Synonymous with *data set ready (DSR)*.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

dependent LU requester (DLUR). An APPN end node or an APPN network node that owns dependent LUs, but requests that a dependent LU server provide the SSCP services for those dependent LUs.

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination port. The 8-port asynchronous adapter that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP)*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies. (3) See *Administrative Domain* and *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is `ralvm7.vnet.ibm.com`, each of the following is a domain name:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

domain name server. In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses. Synonymous with *name server*.

Domain Name System (DNS). In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

dynamic reconfiguration (DR). The process of changing the network configuration (peripheral PUs and LUs) without regenerating complete configuration tables or deactivating the affected major node.

Dynamic Routing. Routing using learned routes rather than routes statically configured at initialization.

E

echo. In data communication, a reflected signal on a communications channel. For example, on a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EIA 232. In data communication, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

EIA unit. A unit of measure, established by the Electronic Industries Association, equal to 44.45 millimeters (1.75 inches).

encapsulation. (1) In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. (2) See also *data link switching*.

encode. To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T)

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response*.

exchange identification (XID). A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

explorer frame. See *explorer packet*.

explorer packet. In LANs, a packet that is generated by the source host and that traverses the entire source routing part of a LAN, gathering information on the possible paths available to the host.

exterior gateway. In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with *interior gateway*.

Exterior Gateway Protocol (EGP). In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. An example of an EGP is the Border Gateway Protocol (BGP). Contrast with Interior Gateway Protocol (IGP).

F

fax. Hardcopy received from a facsimile machine. Synonymous with ***telecopy.***

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

flash memory. A data storage device that is programmable, erasable, and does not require continuous power. The chief advantage of flash memory over other programmable and erasable data storage

devices is that it can be reprogrammed without being removed from the circuit board.

flow control. (1) In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. (2) See also *pacing*.

fragment. See *fragmentation*.

fragmentation. (1) The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. (2) See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. Synonymous with *data link level*. See *link level*.

frame relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

front-end processor. A processor such as the IBM 3745 or 3174, that relieves a main frame from the communication control tasks.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (3) In TCP/IP, synonym for *router*.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

heap memory. The amount of RAM used to dynamically allocate data structures.

Hello. A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello message. (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

heuristic. Pertaining to exploratory methods of problem solving in which solutions are discovered by evaluation of the progress made toward the final result.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

high-performance routing (HPR). An addition to the Advanced Peer-to-Peer Networking (APPN) architecture that enhances data routing performance and reliability, especially when using high-speed links.

hop. (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

hop count. (1) A metric or measure of distance between two points. (2) In Internet communications, the number of routers that a datagram passes through on its way to its destination. (3) In SNA, a measure of the number of links to be traversed in a path to a destination.

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

hub (intelligent). A wiring concentrator, such as the IBM 8260, that provides bridging and routing functions for LANs with different cables and protocols.

hysteresis. The amount the temperature must change past the set alert threshold before the alert condition is cleared.

I

I-frame. Information frame.

information (I) frame. A frame in I format used for numbered information transfer.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

Integrated Digital Network Exchange (IDNX). A processor integrating voice, data, and image applications. It also manages the transmission resources, and connects to multiplexers and network management support systems. It allows integration of equipment from different vendors.

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

International Telecommunication Union (ITU). The specialized telecommunication agency of the United Nations, established to provide standardized communication procedures and practices, including frequency allocation and radio regulations worldwide.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internetwork Packet Exchange (IPX). (1) The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. (2) See also *Xerox Network Systems (XNS)*.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

intra-area routing. In Internet communications, the routing of data within an area.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IPPN. The interface that other protocols can use to transport data over IP.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPXWAN. A Novell protocol that is used to exchange router-to-router information before exchanging standard Internetwork Packet Exchange (IPX) routing information and traffic over wide area networks (WANs).

J

jitter. (1) Short-term non-cumulative variations of the significant instants of a digital signal from their ideal positions in time. (2) Undesirable variations of a transmitted digital signal. (3) Variations in the network delay.

L

LAN bridge server (LBS). In the IBM Token-Ring Network Bridge Program, the server that keeps statistical information about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Network Manager (LNM). An IBM licensed program that enables a user to manage and monitor LAN resources from a central workstation.

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

line switching. Synonym for *circuit switching*.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

link access protocol balanced (LAPB). A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

link-attached. (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Contrast with *channel-attached*. (3) Synonymous with *remote*.

link connection. (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). (2) In SNA, synonymous with *data circuit*.

link level. (1) A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. (2) See *data link level*.

link-state. In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol's topological database is formed from the collected link-state advertisements.

link station. (1) The hardware and software components within a node representing a connection to

an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. (2) See also *adjacent link station (ALS)*.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*. (3) Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local bridging. A function of a bridge program that allows a single bridge to connect multiple LAN segments without using a telecommunication link. Contrast with *remote bridging*.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T) The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

loopback test. A test in which signals from a tester are looped at a modem or other network element back to the tester for measurements that determine or verify the quality of the communications path.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

low-entry networking (LEN) node. A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

M

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T)

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN)*.

MIB. (1) MIB module. (2) Management Information Base.

MIB object. Synonym for *MIB variable*.

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of data defined in a MIB module. Synonymous with *MIB object*.

MIB view. In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

module. In the Nways Switch, a packaged functional hardware unit containing logic cards, connectors, and lights. The modules are used to package adapters, line interface couplers, voice server extensions, and other components. All modules are ***hot pluggable*** in the logic subracks.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multipath channel (MPC). A channel protocol that uses multiple unidirectional subchannels for VTAM-to-VTAM bidirectional communication.

multiple-domain support (MDS). A technique for transporting management services data between

management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk IP address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *Domain Name System (DNS)*.

name server. In the Internet suite of protocols, synonym for *domain name server*.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

Network Access Server (NAS). A device providing temporary, on-demand network access to users. This access is point-to-point using PSTN or ISDN lines.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier. (1) In TCP/IP, that part of the IP address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management station. In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). See *Advanced Peer-to-Peer Networking (APPN) network node*.

network support station. The processor used to locally operate and service the Nways Switch. It is used by the Nways Switch administrator or service personnel.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

noncanonical address. In LANs, a format for the transmission of medium access control (MAC) addresses for token-ring adapters. In noncanonical format, the most significant (leftmost) bit of each address byte is transmitted first. Contrast with *canonical address*.

Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1). A recording method in which the ones are represented by a change in the condition of magnetization, and zeros are represented by the absence of change. Only the one signals are explicitly recorded. (Previously called ***non-return-to-zero inverted***, NRZI, recording.)

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

Nways Switch. Synonymous with IBM 2220 Nways BroadBand Switch.

Nways Switch configuration station. A dedicated OS/2 station running a stand-alone version of the Nways Switch Configuration Tool (NCT). It is used to generate a network configuration database and should be installed as a remote console.

O

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

orphan circuit. A non-configured circuit whose availability is learned dynamically.

P

pacing. (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. (2) See also *flow control*, *receive pacing*, *send pacing*, *session-level pacing*, and *virtual route (VR) pacing*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet loss ratio. The probability that a packet will not reach its destination or not reach it within a specified time.

packet mode operation. Synonym for *packet switching*.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

parallel bridges. A pair of bridges connected to the same LAN segment, creating redundant paths to the segment.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC)*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also *peripheral PU* and *subarea PU*.

ping command. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

port number. In Internet communications, the identification of an application entity to the transport service.

private branch exchange (PBX). A private telephone exchange for transmission of calls to and from the public telephone network.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components.

Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

pulse code modulation (PCM). A standard adopted for the digitalization of an analog voice signal. In PCM, the voice is sampled at a rate of eight kHz and each sample is coded in an 8-bit frame.

R

Rapid Transport Protocol (RTP) connection. In high-performance routing (HPR), the connection established between the endpoints of the route to transport session traffic.

reachability. The ability of a node or a resource to communicate with another node or resource.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

real-time processing. The manipulation of data that are required, or generated, by some process while the process is in operation. Usually the results are used to influence the process, and perhaps related processes, while it is occurring.

reassembly. In communications, the process of putting segmented packets back together after they have been received.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with *carrier detect* and *data carrier detect (DCD)*.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with *local bridging*.

remote console. A station running OS/2, TCP/IP, and the remote Nways Switch Resource Control program. It can be connected to any network support station to operate and service the Nways Switch remotely. The connection may be through:

- A switched line using a modem

Any network support station can be used as a remote console of another network support station.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset request packet. In X.25 communications, a packet transmitted by the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE) to request that a virtual call or a permanent virtual circuit be reset. The reason for the request can also be specified in the packet.

resource. In the Nways Switch, an hardware element or a logical entity created by the Control Program. For example, the adapters, LICs, and lines are physical resources. The control points and connections are logical resources.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See *LAN segment*.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes

information about the user's environment (for example, terminal type) to the remote machine.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

root bridge. The bridge that is the root of a spanning tree formed between other active bridges in the bridging network. The root bridge originates and transmits bridge protocol data units (BPDUs) to other active bridges to maintain the spanning tree topology. It is the bridge with the highest priority in the network.

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*. (5) Contrast with *bridge*.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing domain. In Internet communications, a group of intermediate systems that use a routing protocol so that the representation of the overall network is the same within each intermediate system. Routing domains are connected to each other by exterior links.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing loop. A situation that occurs when routers circulate information among themselves until convergence occurs or until the networks involved are considered unreachable.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP)*.

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

S

SAP. See service access point.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router*.

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of

transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

Serial Line Internet Protocol (SLIP). A protocol used over a point-to-point connection between two IP hosts over a serial line, for example, a serial cable or an RS232 connection into a modem, over a telephone line.

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

socket. (1) An endpoint for communication between processes or application programs. (2) The abstraction provided by the University of California's Berkeley Software Distribution (commonly called Berkeley UNIX or BSD UNIX) that serves as an endpoint for communication between processes or applications.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source routing. In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the

final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

standard MIB. In the Simple Network Management Protocol (SNMP), a MIB module that is located under the management branch of the Structure of Management Information (SMI) and that is considered a standard by the Internet Engineering Task Force (IETF).

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP)*.

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use `$AA` as their service access point (SAP) value.

subnetwork mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line. Contrast with *permanent virtual circuit (PVC)*.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). (1) A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) (2) Contrast with *binary synchronous communication (BSC)*.

synchronous optical network (SONET). A US standard for transmitting digital information over optical interfaces. It is closely related to the synchronous digital hierarchy (SDH) recommendation.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system configuration. A process that specifies the devices and programs that form a particular data processing system.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control,

with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) A UNIX-like/Ethernet-based system-interconnect protocol originally developed by the US Department of Defense. TCP/IP facilitated ARPANET (Advanced Research Projects Agency Network), a packet-switched research network for which layer 4 was TCP and layer 3, IP.

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a “threshold exceeded” occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

time division multiplexing (TDM). See ***channelization***.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

topology database update (TDU). A message about a new or changed link or node that is broadcast among APPN network nodes to maintain the network topology database, which is fully replicated in each network node. A TDU contains information that identifies the following:

- The sending node
- The node and link characteristics of various resources in the network
- The sequence number of the most recent update for each of the resources described.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

transceiver (transmitter-receiver). In LANs, a physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and that sense collisions.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG)*. A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes. (4) See also *parallel transmission groups*.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit*.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

transport layer. In the Open Systems Interconnection reference model, the layer that provides a reliable end-to-end data transfer service. There may be relay open systems in the path. (T) See also *Open Systems Interconnection reference model*.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

trunk line. A high-speed line connecting two Nways Switches. It can be a coaxial cable, fiber cable, or radio wave, for example, and may be leased from telecommunication companies.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps.

U

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.24. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.25. In data communication, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

V.34. An ITU-T Recommendation for modem communication over standard commercially available voice-grade 33.6-Kbps (and slower) channels.

V.35. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

V.36. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates of 48, 56, 64, or 72 kilobits per second.

version. A separately licensed program that usually has significant new code or new function.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual connection. In frame relay, the return path of a potential connection.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.

VIrtual NEtworking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also *StreetTalk*.

virtual route (VR). (1) In SNA, either (a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or (b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route

between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). (2) Contrast with *explicit route (ER)*. See also *path* and *route extension (REX)*.

W

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

wildcard character. Synonym for *pattern-matching character*.

X

X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. (1) An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. (2) See also *packet switching*.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *Internetwork Packet Exchange (IPX)*.

Z

zone. In AppleTalk networks, a subset of nodes within an internet.

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Readers' Comments — We'd Like to Hear from You

Access Integration Services
Software User's Guide
Version 3.2

Publication No. SC30-3988-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SC30-3988-00

IBM®

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

SC30-3988-00

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC30-3988-00

Spine information:

Access Integration Services AIS V3.2 Software User's Guide SC30-3988-00