Access Integration Services

使用和配置功能部件版本 3.2

SC84-0713-00

Access Integration Services

使用和配置功能部件版本 3.2

SC84-0713-00

注意

使用此文档前，请阅读第xv页的『声明』中的一般信息。

第一版 (1998 年 11 月)

除在新版本或技术通讯中另有说明之外，本版本适用于 IBM Access Integration Services 的 Version 3.2 及所有的后续发行版和修订版。

如果要订购这些出版物，请与当地的 IBM 代表或 IBM 分部联系。这些出版物在以下地址中并未提供。

IBM 真诚欢迎您提出宝贵意见。该出版物的背面附有读者意见表。如果表格已被拆去，您可将意见寄到:

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

您向 IBM 发出信息后，IBM 便对该消息拥有非独家专有权。在不侵犯您的权利的情况下，IBM 有权以其认为适当的方式，使用或分发此信息。

目录

图

表

声明

本出版物中引用 IBM 公司的产品、程序或服务，并不意味着向所有有 IBM 公司业务的国家提供这些产品、程序或服务。对这些产品、程序或服务的引用，也不说明或默示只可使用 IBM 公司的产品、程序或服务。只要不侵犯 IBM 公司的知识产权或其它受法律保护的合法权利，任何功能相当的产品、程序或服务都可代替 IBM 的产品、程序或服务。与其它产品一起使用时，除了那些由 IBM 公司明确指定的的产品外，其评估和验证均由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项应用程序专利。提供本文档并不表示允许用户使用这些专利。用户可以书面形式将特许查询寄往: IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A。

本文档中涉及的许可程序和所有许可材料由 IBM 根据 IBM 客户协议提供。

此书并不用于生产目的，按“仅此状态”提供，不作任何形式的保证，包括用于特定的商用性或适用性的保证。

对本书联机版本用户的声明

在本书的联机版本中，授权用户:

- 在每一副本及部分副本上复制版权声明、所有警告声明和其它所需声明后，复制、修改和打印介质中包含的文档，以便在企业中使用。
- 传送相关IBM产品(产品可以是自己的机器，在程序许可条款允许传送的情况下，也可以是自己的程序)时，同时传送原始文档的未修改副本。同时必须毁坏该文档的其他版本。

用户需要支付由些授权引起的所有税款，包括个人财产税。

本文档无任何明示或暗示的保证，其中包括用于特定目的的适销性和适用性保证。

某些法律不允许免除暗示保证，所以以上免除条款可能不适用于您。

不遵守以上条款将使授权终止。一旦授权终止，您就必须销毁机器可读的文档。

商标

下列术语是 IBM 公司在美国和/或其它国家中的商标:

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

UNIX 是 X/Open Company Limited 所独有的在美国和其他国家的注册商标。

Microsoft、Windows、Windows NT 和 Windows logo 都是 Microsoft 公司的商标或注册商标。

其他公司、产品和服务名称可能是其他公司的商标或服务商标。

前言

当您使用此路由器的用户接口配置或更换 IBM 2212 上安装的功能部件时，本手册所包含的信息是必需的。特定的 IBM 2212 可能不支持本手册中描述的所有功能部件。如果某个功能部件是设备专用的，则会有以下提示:

- 相关章节中的声明
- 前言中的某一部分列出所支持的功能部件和设备

本手册支持 IBM 2212 ，并称之为“路由器”或“设备”。本手册中的 IBM 2212 配置实例可能与实际的输出结果有所不同。这些实例可作为配置设备时用户所看到内容的指南。

本手册的阅读对象

本手册的读者应是安装和管理计算机网络的人员。具有计算机网络软件和硬件经验是会有所帮助，但不必一定有使用协议软件的编程经验。

要获取其他信息: 可以在打印书籍后进行更改。如果书籍打印后，需要添加其他信息或需要更改，则更改应写入配置程序软盘 1 上名为 README 的文件中。可以用 ASCII 文本编辑器查看该文件。

关于软件

IBM Access Integration Services 是支持 IBM 2212 (许可程序号 5639-F73)的软件。该软件包括:

- 基本码，包括:
  - 提供设备路由、桥接、数据链接交换和 SNMP 代理功能的代码。
  - 路由器用户接口，它允许配置、监视并使用在设备上安装的 Access Integration Services 基本码。路由器用户接口可通过连接到服务端口的 ASCII 终端或仿真器进行本地访问，也可以通过 Telnet 会话或通过连接调制解调器的设备进行远程访问。

  出厂时已在 2212 上安装了基本码。
- IBM Access Integration Services 的 Configuration Program (在本书中引用为 *Configuration Program*) 是一种图形用户界面，通过它可从独立工作站配置设备。Configuration Program 包括错误检查和联机帮助信息。

  出厂时并不预装 Configuration Program; 它作为软件订单的一部分，与设备分开，单独提供。

  也可以从 IBM 网络技术支持主页获得 IBM Access Integration Services 的 Configuration Program。请参阅 *Configuration Program User's Guide for Multiprotocol and Access Services Products*, GC30-3830，以获取服务器地址和目录。

说明书中使用的约定

本手册中使用下列约定说明命令语法和程序响应。

1. 缩略的命令形式标有下划线，如下例所示:

   ```
   reload
   ```

   在此例中，您可使用命令的完整形式 (reload)，也可使用缩略形式 (rel)。

2. 参数的关键选项以 [] 括住，相互之间以 or 分开。例如:

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

   表示选择其中的一个关键字作为参数值。

3. 选项之后的三个句点表明您在该选项后面输入了附加数据 (如变量)。例如:

   ```
   time host ...
   ```

   按照对命令的说明，在此例中可输入主机的 IP 地址以替代句点。

4. 命令执行后显示的信息中，紧随该选项后的缺省值以 [] 括起。例如:

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

   此例中，如果您未指定 STP，则介质缺省为 UTP。

5. 键盘上的组合键以如下文本方式指明:

   - **Ctrl-P**
   - **Ctrl -**

   组合键 **Ctrl -** 表示您应同时按下 Ctrl 键和连字符。这种组合键在某些情况下可更改命令行提示符。

6. 键盘的键名以这样的方式表示: **Enter**

7. 变量(即用于代表所定义的数据的名称)以斜体的形式表示。例如:

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

库概述

下表显示在 IBM 2212 中按任务编排的书目。

信息更新和更正: 要在打印本书后，仍能继续了解技术更改、说明和修改内容，则可参阅 IBM 2212 主页:

```
http://www.networking.ibm.com/2212/2212prod.html
```

规划

GA27-4215

IBM 2212 Introduction and Planning Guide

本书与 IBM 2212 一起提供。其中说明了如何安装并执行初始配置。

安装

GA27-4216

IBM 2212 Access Utility Installation and Initial Configuration Guide

本手册与 IBM 2212 一起提供。它说明了如何安装 IBM 2212，并检验安装结果。

GX27-4048

2212 Hardware Configuration Quick Reference

该标记卡用于输入并保存硬件配置信息，以确定正确的 IBM 2212 状态。

诊断和维护

GY27-0362

IBM 2212 Access Utility Service and Maintenance Manual

本书与 IBM 2212 一起提供。其中提供了对诊断和维修 IBM 2212 的问题的指导。

操作和网络管理

下表显示了支持 Access Integration Services 程序的书目。

SC30-3988

Software User's Guide

本书说明如何:

- 配置、监视和使用 Access Integration Services 软件。
- 使用 Access Integration Services 命令行路由器用户界面，配置并监视网络接口和与 IBM 2212 一起提供的链接层协议。

SC30-3989

Using and Configuring Features

SC30-3990

Protocol Configuration and Monitoring Reference Volume 1

SC30-3991

Protocol Configuration and Monitoring Reference Volume 2

这些书说明了如何访问并使用 Access Integration Services 命令行用户界面，来配置并监视与本产品一起提供的路由协议软件。

还包括设备支持的所有协议的信息。

SC30-3682

Event Logging System Messages Guide

本书列出可能出现的错误代码、错误说明和更改错误的建议操作。

配置

GC30-3830

Configuration Program User's Guide for Multiprotocol and Access Services Products

本书讨论了如何使用配置程序。

安全

SD21-0030

注意: 首先阅读安全信息

本书与 IBM 2212 一起提供，其中有警告的译本，以及可应用于 IBM 2212 安装和维护的危险注意事项。

购买

URL: **http://www.networking.ibm.com/2212/2212prod.html**

此 IBM Web 页通过 World Wide Web 网提供了产品信息。

IBM 2212 软件库更改总结

IBM 2212 是新产品；但使用所用代码。以下列示了在版本 3.2 中对所用代码所做的更改。

- **新功能**:
  - IP 版本 6
    - TCP6、UDP6、Telnet、PING-6 和 traceroute-6、ICMPv6 和 IPsec
    - 主机自动配置的 Neighbor discovery 协议 (NDP)
    - 静态路由、RIPng、协议独立多址发送紧凑模式 (PIM-DM) 和多址发送侦听发现 (MLD)
    - 在 IPv4 网络上配置或自动传输 IPv6 包
  - 资源保留协议(RSVP)
    - 是这样一些发送信号机制，它使 IPv4 网络上的应用程序保留网络资源，以达到期望的包传输服务品质。
  - 瘦服务器支持
    - 作为网络工作站的引导服务器
    - 所支持的服务器包括 OS/400 上的 Network Station Manager (NSM) R2.5 和 3.0 以及 NFS 服务器上的 NSM R3.0，如 Windows NT、OS/390、AIX 和 VM 的 NSM R3.0
  - 二进制同步中继 (BRLY) 支持对 BSC 接口

    二进制同步中继 (BRLY) 支持将二进制同步 (BSC) 传输信息通过 IPv4 网络传送到对方 2210 或 2212 路由器
- **增强功能**:
  - 基本服务
    - 事件记录系统 (ELS) 增强功能，能够俘获、格式化和卸载大量 ELS 消息
    - 支持对多个压缩转储文件的维护
    - 来自配置工具的定时配置更改支持，这种更改在重新装入或重新启动时都会发生
    - 对 PPP、帧中继和 V.34 接口的包跟踪支持。
  - 多路访问桥接端口的桥接支持，用于通过帧中继的源路由桥接。多路访问端口将许多 DLCI 结合在一个桥接端口，从而提高了适用范围。
  - DIAL
    - DIAL 支持 Microsoft 拨号网络客户机支持的功能
      - 支持回呼控制协议 (CBCP)
      - 支持 Microsoft 点到点加密 (MPPE) 和 Microsoft PPP CHAP (MS-CHAP)

- 虚拟连接，以便使用 Shiva 口令认证协议 (SPAP) 时暂挂然后再恢复连接。

– IP 项
  - IP 优先/TOS 过滤器增强功能
  - 基于策略的路由选择
  - 通过接口配置 IP MTU 配置
  - OSPF 增强功能，可以简便地移植 IBM 6611 路由器网络
  - BGP-4 支持每个邻居策略及路径选择的附加属性
  - DVMRPv3 支持
  - IGMP 修剪和接枝支持
– 以呼叫方 ID 为基础的回呼和呼叫阻塞的 ISDN 支持
– L2TP 客户机模型的 L2TP 支持，以使 2212 创建其本身与另一路由器之间的 L2TP 隧道。隧道可用于任何进入 2212 的流量。同时也增强了 L2TP 网络服务器 (LNS) 功能，以启动到 L2TP 网络访问集中器 (LAC) 的出网呼叫。
– 网络调度程序项
  - 支持无状态的 UDP 应用程序
  - 网络新闻传输协议 (NNTP)、邮局协议 (POP3)、简单邮件传输协议 (SMTP) 和 Telnet 的新协议顾问
  - 当平衡 TN3270 服务器时，其中一个 TN3270 服务器可能与网络调度程序功能在同一个 2212 中
– 支持使用 ACE/Server 进行 PPP 认证
– 安全增强功能
  - 可创建多达两个安全关联嵌套级别的 IPsec 隧道内隧道支持
  - IPsec ESP NULL 算法支持
  - IPsec 支持设置*不分段*位并传播路径 MTU
  - 改进了 IPsec 动态重新配置
– 用于集束 PPP 租用线、ISDN、V.25bis 和 V.34 连接的混合介质多链路 PPP 支持
– APPN 增强功能
  - APPN SDLC 次级多点支持
  - 所有链接工作站类型的 APPN 传输组 (TG) 数目的配置
  - 支持对于 Talk 5 中 APPN Ping (APING) 命令
  - 新跟踪选项
– TN3270 增强功能

  注: 在初始的 V3.2 版本中没有 TN3270 增强功能，但不迟于 12/31/98 ，这些增强功能在 2212 Web 服务器上可用。

  - TN3270 LU 分池支持，此支持允许将 SNA LU 分成多个有命名的存储池
  - TN3270 IP 地址到 LU 名称的映射
  - 自定义从属 LU(SDDLU) 和动态定义从属 LU(DDDLU) 支持
  - 多 TCP 端口支持
– DLSw 增强功能

- 支持复制的 MAC 地址
- 支持延迟对 SDLC 设备的轮询，直到与远程 SDLC 设备连接

– X.25 增强功能
- 配置支持定义一系列 PVC
- 支持多达 2500 个 PVC

– 对交换虚拟电路的帧中继支持
– 在帧中继永久性虚拟电路 (PVC) 上的 IPXWAN 支持，包括对编号的 RIP、未编号的 RIP 和静态路由选择的支持

- **说明和更改**

  技术更改和添加内容在更改内容的左侧标有竖线 (|)。

获得帮助

在命令提示处，可以以列表的形式获得这一级别可用命令的帮助。为此，应输入 **?(帮助命令)**，然后按下 **Enter** 键。使用 **?**，列出当前级别可用的命令。通常在特定命令名称后键入 **?**，即可列出该命令的选项。例如，如果在 * 提示处输入 **?**，则显示以下信息:

```
*?

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
```

退出较低级别的环境

在配置或操作 2212 时，软件的多级性将使用户处于第二、第三或更低的级别。要回到较高级别，可输入 **exit** 命令。要进入第二级别，可继续输入 **exit**，直到出现第二级提示 (Config> 或 +)。

例如，要退出 IP 协议配置进程，可输入:

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

如果需要进入主级别 (OPCON)，则可输入截取字符(缺省为 **Ctrl P**)。

第1章 使用带宽保留和优先级排队

本章说明了当前可用于帧中继和 PPP 接口的带宽保留系统和优先级队列功能部件。该章节包括以下部分:

带宽保留系统

在网络连接中，当需求量(通信量)超过供应量(吞吐量)时，带宽保留系统允许您决定要丢弃哪些信息包。当带宽使用率达到 100% 时，BRS 可依据您的配置决定哪些通信量应丢弃。

带宽保留系统为指定的通信类“保留”传输带宽。各通信类都分配了连接带宽的最低百分比。请参阅第2页的图1和第2页的图2。

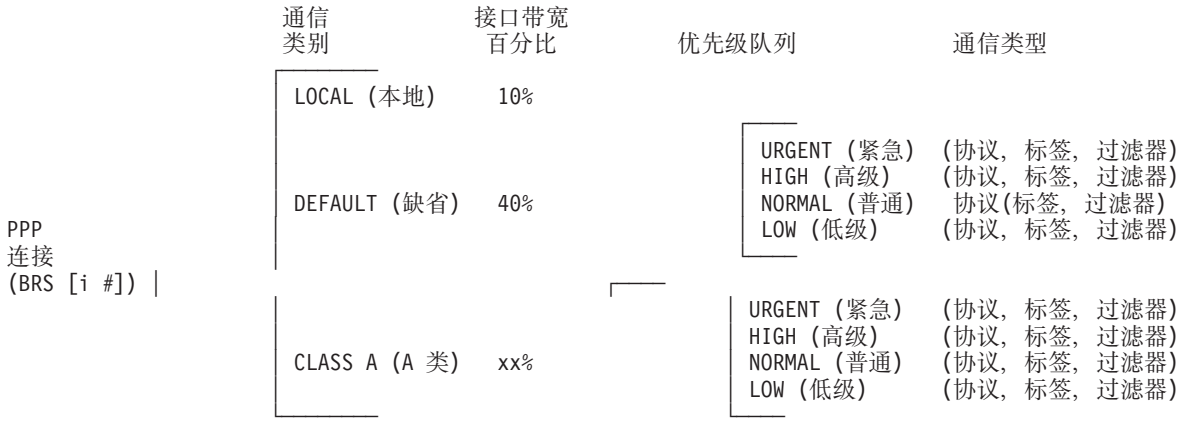
在 PPP 接口上，您可定义通信类 (t 类)，各通信类都分配了 PPP 接口带宽一定的百分比。通信类至少有两种:

1. LOCAL 类，其分配的带宽主要供路由器从本地发出的信息包(如 IP RIP 信息包)使用
2. DEFAULT 类，初始，所有其它通信都分配到这一类别

您也可创建附加的通信类，并在通信类内为优先级队列指定协议、路由器及标签。请参阅第2页的图1。

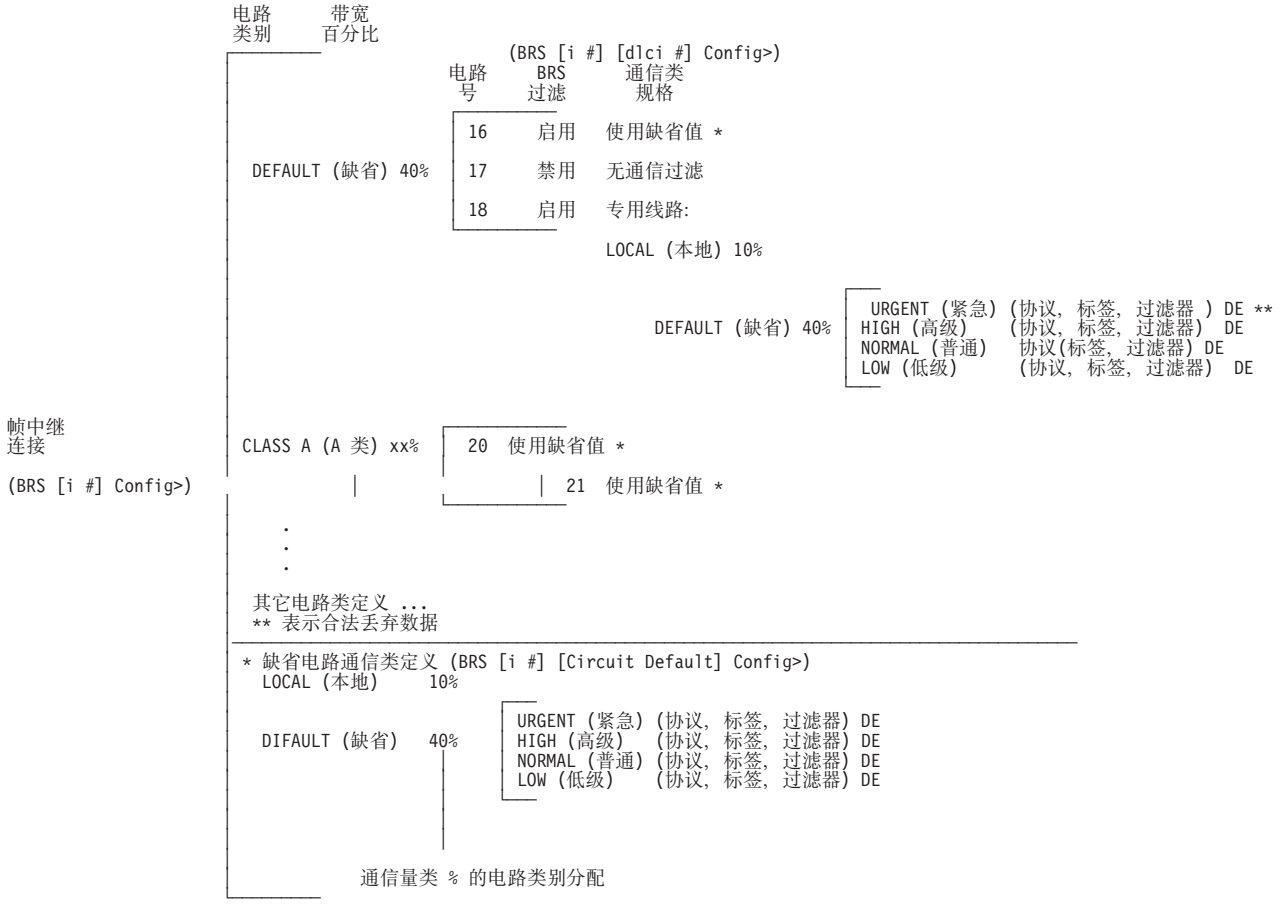
您可在帧中继接口上定义电路类 (c 类)，各电路类都分配有一定的帧中继接口的带宽百分比。至少有一种电路类: DEFAULT 电路类，初始，所有电路都分配到此电路类。您可创建附加的电路类并向这些 c 类指定电路。在各帧中继电路上，您可定义通信类 (t 类)，各通信类都分配有一定的帧中继电路的带宽百分比。帧中继电路的通信类支持类似于 PPP 接口的通信类支持。关于帧中继电路类和通信类的关系，请参阅第2页的图2。

使用 BRS 和优先级排队



注: 初始所有的协议指定到 DEFAULT 通信类的 NORMAL (普通) 优先级队列上。您也可将协议、过滤器或标记指定到一个通信类中的任何优先级队列上。

图 1. PPP BRS 通信类与通信类优先级队列的关系



注: 所有的协议都初始指定到 DEFAULT 通信类的正常级优先级队列上。您也可将协议、过滤器或标记指定到一个通信类中的任何优先级队列上。

图 2. 帧中继 BRS 电路类与通信类的关系

这些保留的百分比只占网络连接带宽的最小部分。如果网络开通到最大限度，任何类的消息都可传送，直到这些报文使用了分配给该类的配置带宽。这种情形下，在满足了其它的带宽传送之前，不可进行附加的传送。在通信线路不拥挤的情况下，如果没有其它通信，则信息包流使用的带宽可以超过其允许的最小百分比，直至 100%。

带宽保留起到很好的保护作用。一般情况下，设备使用的速度不能超过线路速度的 100%。如果速度要超过该线路的 100%，则可能需要一条传输速度更快的线路。然而，通信本身所具有的“猝发”性质，可在短时间内使所请求的传输速率超过 100%。在这些情况下，要启用带宽预留，确保更高优先级通信的传输(即不废弃更高优先级通信)。

带宽保留在以下连接类型上运行:

- 帧中继(串行线路或拨号电路接口)
- PPP (串行线路或拨号电路接口)

帧中继上的带宽保留

带宽保留允许您在两个层次上保留带宽:

- 在接口层次上，您可为电路类 (*c* 类)分配一定的接口带宽百分比。每个电路类有一条或多条电路组成。
- 在电路层上，您可定义通信类并为其分配一定的电路带宽百分比。

根据包协议类型和任何已配置的 BRS 过滤器，对包进行过滤，并排列成 BRS t 类。然后，基于 DLCI 的编号，将这些信息包排列到 BRS c 类中。

带宽保留实际可用的带宽量取决于您是如何配置接口和电路的:

- 如果您启用帧中继 CIR 监控，则电路可用的带宽严格按照电路的传输信息速率 (CIR)、可传输的猝发大小及其超量猝发大小来分配。
- 如果您禁用 CIR 监控，则电路可使用的接口带宽可达到 100%。

孤立电路和 BRS 未明确启用的电路使用缺省的 BRS 排队环境，此环境中，信息包按缺省的 t 类和优先级及缺省的 c 类排列。

您可使用几条带宽保留监控命令，显示指定接口电路类的保留计数器:

- clear-circuit-class
- counters-circuit-class
- last-circuit-class

有关监控 BRS 的详细信息，请参阅第19页的『第2章 配置和监控保留带宽』。

指定的接口即为在带宽监控命令提示符下所显示出来的接口。例如，`BRS [i 5]` 就是接口 5 的提示符。

如果您不想使用 BRS 电路类，则使所有的电路保持为缺省电路 c 类，不要再创建其它的电路类。

排队支持

通过帧中继上的带宽保留，各电路能在拥塞状态下对帧进行排队，甚至带宽保留没有启用的接口和电路也可对帧进行排列。

合法废弃

帧中继网络可能会废弃在 PVC 上超过 CIR 的传送数据。路由器可设置 DE 位，指示应将一些通信视为“合法废弃”。如果条件允许，帧中继网络将标有“合法废弃”的帧废弃，从而可能使未标有“合法废弃”的帧从网上顺利通过。当向通信类分配协议、过滤器或标签时，您可指定协议、过滤器或标签通信是否是“合法废弃”。有关如何将通信量配置为“合法废弃”的详细信息，请参阅第24页的『Assign』。

处理通信类的缺省电路定义

帧中继接口可对许多电路进行定义。为避免对每条电路全面配置通信类定义，BRS 允许您定义一个由通信类定义、协议、过滤器及标签赋值组成的缺省集，此缺省集称为缺省电路定义，接口上的任何电路都可以使用。当 BRS 在电路上初始启用时，则要初始化电路以使用缺省电路定义。如果某一电路不能使用缺省电路定义处理通信类，那么您使用命令: **add-class**、**change-class**、**assign**、**deassign**、**tag** 和 **untag** 可创建电路专用定义。

如果电路使用的是电路专用定义，而您想让它使用缺省电路定义，则您可在电路的 BRS 提示符下输入 **use-circuit-defaults** 命令。

处理通信类的缺省电路定义是通过在 BRS 帧中继接口提示符下使用 **set-circuit-defaults** 命令来定义的。该命令使您可在 BRS 电路缺省提示符下添加、更改及删除通信类，并且，允许您指定和取消指定协议、过滤器及标签，以及允许您创建 BRS 标签。对通信类的缺省电路定义的更改，可以导致动态地修改所有电路(使用缺省电路定义的电路)的通信类处理。

优先级排队

带宽保留向指定的通信类或用户定义的 *t 类*分配总连接带宽的不同百分比。BRS t 类是一组由相同名字标识的信息包; 例如，称为“ipx”的类指定了所有的 IPX 信息包。

使用优先级队列，可将下列之一的优先级设置指定到各带宽的 t 类:

- Urgent (紧急)
- High (高级)
- Normal (普通) (缺省设置)
- Low (低级)

所有指定为 Urgent 优先级的信息包将首先在它们的通信类中得到发送。随后发送的分别是 High 和Normal，然后是 Low 消息。传输了所有的 Urgent 信息包后，再传输 High 信息包，直到传输完毕(或者直到排列新的 Urgent 消息)。仅当没有 Urgent、High 或 Normal 信息包时，才开始传输 Low 优先级的信息包。如果未指定优先级设置，则缺省值设置为 Normal。

此外，对于各带宽 t 类中的每个优先级，您可设置正在队列中等待的信息包数目。BRS **queue-length** 命令设置可在各 BRS 优先级队列中进行排列的输出缓冲区最大数目，

以及在缺少路由器输出缓冲区时，可设置在各 BRS 优先级队列中进行排列的输出缓冲区最大数目。对于 PPP 和帧中继，均可设置优先级队列的长度。

警告: 如果您设置的排列长度数值太大，则可能会严重降低路由器的性能。

对于 BRS，您可设置 PPP 和帧中继 WAN 连接的优先级队列长度。有关 **queue-length** 命令的说明，请参阅 第35页的『Queue-length』。

在一个带宽 t 类中的优先级设置并不影响其它的带宽类。不存在一个带宽类的优先级超过其它带宽类的优先级。

没有带宽保留的优先级排队

当优先级队列没有配置带宽保留时，则首先传送具有最高优先级的通信。在高优先级通信拥挤的情况下，则忽略较低的优先级。然而，如优先级队列配置有保留带宽，则可为所有的通信类型分配信息包传输。

配置通信类

您首先使用 **add-class** 命令创建通信类，然后使用 **assign** 命令向该类指定通信类型。基于通信类的*协议类型*或基于进一步标识特定*协议通信*(如 SNMP IP 信息包)类型的过滤器，通信被分配到通信类。

支持的协议类型有:

- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR
- HPR/IP

BRS 过滤器

使用带宽保留，您可将特定的协议通信看作不同于其它通信，尽管它们使用相同协议类型。例如，您可将 SNMP IP 通信量指定到不同于其它 IP 通信的通信类和和优先级中。在此例中，SNMP 起到了 BRS 过滤器的作用，因为它“过滤”(即唯一标识)特定的协议通信量。IP、ASRT (桥接)和 APPN-HPR 协议通信量能由带宽保留“过滤”，以下的过滤器受支持:

- IP 隧道连接
- 通过 IP 的 SDLC 隧道连接 (SDLC 中继)
- 通过 IP 的 BSC 隧道连接 (BSC 中继)

- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- IP 多址发送
- DLSw
- MAC 过滤器
- NetBIOS
- Network-HPR
- 高级 HPR
- 中等 HPR
- 低级 HPR
- XTP
- TCP/UDP 端口号或套接字
- TOS 字节
- precedence bit 优先位

BRS 和过滤

下列章节说明如何使用配置有不同类型过滤系统的 BRS。

MAC 地址过滤和标签

通过使用标签，带宽保留和 MAC 过滤 (MCF) 共同处理 MAC 地址过滤。例如，配置有带宽保留的用户能通过在桥接通信量上加标签，从而对其进行归类。

在 MAC 过滤配置主控制台中创建一过滤器项，再指定一标签号，就完成了设置标签进程。此标签号用于建立一个与此标签相关的所有信息包的通信类。当前标签数值必须在 1 到 64 之间。有关 MAC 过滤的详细信息，请参阅第41页的『第3章 使用 MAC 过滤』。

注: 标签**仅**适用于桥接信息包。在 PPP 或帧中继连接上，可指定为带宽保留过滤器的加标签 MAC 多达 5 个，并按 TAG1 到 TAG5 对其进行指定。首先搜索的是 TAG1，然后是 TAG2 ，按照顺序一直搜索到 TAG5。 一个 MAC 过滤器标签可由在 MCF 中设置的任何数目的 MAC 地址组成。

如果在 MAC 过滤配置进程中创建了加标签的过滤器，则可使用 BRS 标签配置命令给 MAC 过滤器标签号指定 BRS 标签名 (TAG1、TAG2、TAG3、TAG4、TAG5)。然后，在 BRS 指定命令中使用 BRS 标签名来向带宽通信类和优先级指定相应的 MAC 过滤器。

如 IP 隧道实例所示，标签也可称为“组”。 IP 隧道端点可归属任何组。通过 MAC 地址过滤的加标签功能，可将信息包指定到特定的组。有关 MAC 过滤的详细信息，请参阅第41页的『第3章 使用 MAC 过滤』和第45页的『第4章 配置和监控 MAC 过滤』。

如果要将带宽保留和排列优先级应用于加有标签的信息包，则:

1. 在 `filter config>` 提示符下，使用 MAC 过滤配置命令，对通过桥接器所传送的信包进行标签设置。详细情况，请参阅 第41页的『第3章 使用 MAC 过滤』。
2. 使用带宽保留的 **tag** 命令为带宽保留引用标签。
3. 使用带宽保留的 **assign** 命令，向 t 类分配 BRS 标签。**assign** 命令同时提示您输入 BRS t 类中的排队优先级。

TCP/UDP 端口号过滤

基于信息包的 UDP 或 TCP 端口号和套接字(可选)，您可将来自一系列的 TCP 或 UDP 端口的信息包指定到 BRS t 类及优先级中。您可指定多达 5 个 UDP/TCP 端口号过滤器，其中过滤器或指定了单一的 TCP 或 UDP 端口号、一系列的 TCP 或 UDP 端口号，或指定了套接字标识符(即端口号和 IP 地址的组合)。然后，您可在通信类中向 BRS 通信类和优先级指定过滤器。

如果启用 UDP/TCP 端口过滤，则 BRS 查看各 TCP 或 UDP 信息包，以检查信宿或信源端口号是否与您为过滤而指定的端口号之一相匹配。同时，如果您将 IP 地址定义为 BRS UDP/TCP 过滤器地址的一部分，且信宿或信源 IP 地址与您定义的过滤器地址相匹配，则 BRS 将信息包分配给端口号过滤器的通信量和优先级中。

例如，您可对范围为在 25 到 29 的 UDP 端口号配置 UDP 端口号过滤器，并且，将过滤器指定到通信类 'A'，该通信类的优先级是 'Normal'。 BRS 将带有信源或信宿端口号(从 25 到 29)的 UDP 信息包排列在通信类 'A' 的 Normal 优先级队列上。

同时，您也可为 IP 地址 5.5.5.25 的 TCP 端口号配置一个 TCP 端口号过滤器，并且，将过滤器指定到优先级为 ' Urgent ' (紧急)的通信 'B' 中。BRS 在通信 'B' 的 Urgent 优先级队列中，对任何信源或信宿端口号是 50 及信源或信宿 IP 地址是 5.5.5.25 的 TCP 信息包进行排队。

IPv4 TOS 位过滤

您可创建基于服务类型 (TOS) 位的设置来区分不同 IP 通信类型的过滤器。这些 TOS 过滤器可用来将有特殊 TOS 位设置的 IPv4 通信量分配给不同于其它 IP 通信的通信类和优先级中。对于 TOS 字节值与已配置的 TOS 过滤器定义相匹配的 IPv4 通信量，各过滤器允许对其指定唯一的通信类和优先级。 TOS 过滤器的配置含有掩码值说明(对要匹配 TOS 字节内的哪些位进行定义)及在掩码范围内位值的上下限说明。过滤机制仅仅基于 IPv4 TOS 的数值；因此，它并不像大多数其它的 IP 过滤器那样，取决于 IPv4 的协议类型或端口号信息。

此过滤器在其应用方面，比 BRS IPv4 优先级过滤的范围更广，BRS IPv4 优先级过滤仅过滤 TOS 字节的高序 3 位。当结合了 IP 存取控制支持以设置 TOS 位时，通过 BRS TOS 位过滤器支持您过滤通过安全通道传送的、分段传送的或不能使用 BRS UDP 和 TCP 端口过滤器支持的通信量。同时，在 IP 存取控制支持下，您可将 TOS 位设置成用户定义的数值，而不必为与 BRS IPv4 优先位过滤相关的 APPN 和 DLSw 使用硬编码优先位数值。因此，建议使用 IP 存取控制和 BRS TOS 过滤器支持，而不要使用 BRS IPv4 优先位过滤。

使用 BRS 和优先级排队

正如第10页的『过滤优先顺序』所示，在检查 IPv4 优先级过滤器和其它特定的 IP 过滤器之前，先检查 TOS 过滤器的匹配性。从 TOS1 开始，按顺检查从 TOS1 到 TOS5 过滤的匹配性。可定义的 TOS 过滤器多达 5 个。

要点: 请记住: 要按照数值匹配的第一个 TOS 过滤器定义，来处理有特殊 TOS 值的信息包。设置过滤器时要注意: 特殊的 TOS 字节应由您指定的过滤器来过滤，避免被编号较低的过滤器过滤的情况发生。详细信息，请参阅*Using and Configuring Features*中的『使用 IP』。

将 IP 版本 4 优先位处理用于 IP 安全隧道和次级分段中的 SNA 通信

BRS 一般是按照端口号来区分 IP TCP 和 UDP 通信量的。然而，在两次封装通信量后，BRS 不能对不能标识端口，如通过 IP 安全隧道传输的 IP 通信或在次级 UDP 或 TCP 分段中的 IP 通信量。BRS 中已添加了 IP 版本 4 优先权位处理，可使 BRS 过滤 IP 安全隧道的信息包或过滤 TCP 和 UDP 次级分段的信息包。

注: 建议您使用 BRS IPv4 TOS 位过滤以取代优先位处理。有关细节，请参阅第7页的『IPv4 TOS 位过滤』。

当 APPN/HPR 通信量通过 IP 进行传递时，各 APPN-HPR 的传输优先级 (网络、高级、中等 和 低级) 映射到三位 IP 版本 4 的优先位特殊数值上。

- HPR 网络传输优先级映射到 IPv4 优先值 '110'b 上。
- HPR 高级传输优先级映射到 IPv4 优先值 '100'b 上。
- HPR 中等传输优先级映射到 IPv4 优先值 '010'b 上。
- HPR 低级传输优先级映射到 IPv4 优先值 '001'b 上。

当在 BRS 中启用 IPv4 优先过滤时，并且当 IP 信息包内的优先位同 APPN/HPR 通信量所使用的数值之一相匹配时，则信息包在指定了相应 HPR 传输优先级的 BRS t 类优先级队列上进行排列。例如，如果 IP 信息包的优先权值是 '110'b，并且，BRS HPR-Network 指定到 t 类 A 的 normal 优先级中，那么信息包则在 t 类 A 的正常级优先级队列中排列。如果没有配置 BRS HPR 传输优先级过滤器，但配置有 APPN-HPR 过滤器，那么信息包则在指定有 APPN-HPR 过滤器的优先级队列和 t 类中排列。

下面的三种通信量映射到 IPv4 优先值 '011'b 上:

- 当 APPN/HPR 通过 IP 路由时发送的 APPN/HPR XID 通信量
- DLSw 通信量
- TN3270 通信量

因为在一数值上映射了几种类型的通信量，因此，当基于 IPv4 优先位上的过滤器启用 BRS 时，BRS 不能区别这些通信量。因而，当 BRS 遇到优先值是 '011'b 的 IP 信息包时, BRS 按下列顺序估计 BRS 过滤器，以确定是否启用。当 BRS 发现已配置了 BRS 过滤器时，则信息包在分配有 BRS 过滤器的优先级队列和 t 类中排列:

- SNA/APPN-ISR (用于 APPN/HPR XID 交换)
- DLSw
- Telnet

如果信息包有经过 BRS 过滤的优先值之一，但并未配置任何可应用的 BRS 过滤器类型，则信息包在分配有 IP 协议的优先级队列和 BRS t 类中排列。

当某客户机在启用了 BRS 的广域网上将 TN3270 通信量发送到 2212 时，则 BRS 不能将来自客户机的通信量列入到优先级，除非客户机将优先位设置为 '011'b。

您必须在多个位置配置 IPv4 优先位处理:

1. 在 BRS 中，配置 BRS 是否应基于 IPv4 优先位来过滤。BRS 仅对 IP 安全隧道的信息包或 TCP 和 UDP 次级分段的信息包进行这种类型的过滤。
2. 在配置 DLSw、IP 上的 HPR 和 TN3270 时，须指定 2212 是否设置信息包的 IPv4 优先位，这些信息包是为以上的各协议类型而由 2212 产生的。

执行下面的三个步骤，使用 IPv4 优先位过滤:

1. 在 BRS 中激活 IPv4 优先过滤。
2. 如果对未在安全隧道传输的 SNA 通信量或未分段的 SNA 通信量进行配置和指定那样，为各种类型的 SNA 通信量配置 BRS t 类并分配协议类型及过滤器。
3. 在配置 DLSw、IP 上的 HPR 及 TN3270 协议时，启用 IPv4 优先位设置。
4. 配置 IPsec 以创建 DLSw、IP 上的 HPR 及 TN3270 通信量流动的安全隧道。

桥接通信量的 SNA 和 APPN 过滤

SNA/APPN-ISR 过滤器允许您将正在桥接的 SNA 和 APPN-ISR 通信量分配给 BRS 通信类。SNA 和 APPN-ISR 通信量被标识为信宿和信源 SAP 为 0x04、0x08 或 0x0C 的任意桥接包，其 LLC (802.2) 控制字段表明该通信量不是未编号的信息 (UI) 帧。

注: 帧中继 BAN 信息包属于此类

APPN-HPR 过滤器允许您将正在被桥接的 HPR 通信量分配到 BRS t 类。SNA 和 APPN-ISR 通信量被标识为信宿和信源 SAP 为 XX'04'、XX'08'、XX'0C' 或 XX'C8' 的任意桥接包，其 LLC (802.2) 控制字段表明该通信量不是未编号的信息 (UI) 帧。

可按照 HPR 传输优先级，使用 Network-HPR、High-HPR、Medium-HPR 和 Low-HPR 过滤器进一步过滤 HPR 桥接通信量。例如，如果您想将使用 network 传输优先级的 HPR 通信量分配到某一 t 类和优先级，而将所有其它的 HPR 桥接通信量指定到另一不同的 t 类或优先级，则您须将 Network-HPR 过滤器分配到相应的 t 类和优先级，并且利用 APPN-HPR 过滤器，将剩余的 HPR 通信量分配到 t 类或优先级。

使用为网络、高级、中等和低级 HPR 传输优先级而指定的 UDP 端口号，过滤通过 IP 传送的 APPN-HPR 通信量。对于 XID 交换，使用附加的 UDP 端口号。用于支持通过 IP 的 APPN-HPR 的所有 UDP 端口号都可配置。

如果在 IP 网络的中间路由器中不能启用 APPN，则您可在 `BRS Config>` 命令提示符下，为通过 IP 的 HPR 配置 UDP 端口号。如果 APPN 在该设备中已经启用，则 BRS 将使用在 `APPN Config>` 命令提示符下配置的数值。

其它的过滤器也可能有助于您分配通信量。例如，DLSw 过滤器允许您将通过 TCP 连接传送的 SNA-DLSw 通信量指定到 BRS t 类。

对于 SNA/APPN-ISR 和 APPN-HPR 过滤器，如果您想查找 SAP 而不是以上的通信量，则使用 MAC 过滤创建滑动窗口，并且为此过滤器加上标签。然后，将加标签的 MAC 过滤器分配给 BRS t 类。

过滤优先顺序

一个信息包与多个 BRS 过滤器类型相匹配是可能的。例如，含有 SNA 数据的 IP 隧道网桥信息包可与 IP 隧道过滤器及 SNA/APPN-ISR 过滤器相匹配。判断过滤器以决定信息包是否与 BRS 过滤器类型相匹配的顺序如下:

1. TOS 过滤器 (IP)
2. IPv4 优先权处理
3. 与桥接信息包相匹配的 MAC 过滤器标签 (IP/ASRT)
4. 用于桥接的 NetBIOS (IP/ASRT)
5. 用于桥接的 SNA/APPN-ISR (IP/ASRT)
6. HPR-Network (IP/ASRT/APPN-HPR)
7. HPR-High (IP/ASRT/APPN-HPR)
8. HPR-Medium (IP/ASRT/APPN-HPR)
9. HPR-Low (IP/ASRT/APPN-HPR)
10. APPN-HPR (IP/ASRT)
11. UDP/TCP 端口号过滤器 (IP)
12. IP 隧道 (IP)
13. SDLC/BSC 中继 (IP)
14. DLSw (IP)
15. 多址发送 (IP)
16. SNMP (IP)
17. Rlogin (IP)
18. Telnet (IP)
19. XTP (IP)

注: 圆括号中所示的是过滤器应用的协议

样本配置

将缺省电路定义用于帧中继电路的通信类处理

注释:

1 配置功能部件 BRS。

2 在接口 1 上启用 BRS。

3 在电路 16、17、18 上启用 BRS。在这些电路上使用通信类处理的缺省电路定义。

4 进入 set-circuit-defaults 菜单以定义通信类处理的缺省电路定义。

5 添加通信类并对其指定协议和过滤器。

6 列出并显示电路 16 的 BRS 定义。由于电路 16 使用缺省电路定义，所以显示由缺省电路定义所定义的通信类和协议及过滤器的分配情况。

7 通过创建唯一通信类 CIRC171，更改电路 17，使其不再使用缺省电路定义，而使用通信类处理的电路特定定义。可以为该类分配协议、过滤器或标签。

8 更改缺省电路定义，使 DEF1 和 DEF2 通信类各保留 10% 的带宽，然后显示出这些更改是针对电路 16 而不是针对 17 的，原因是电路 17 正在使用电路专用定义。

9 修改电路 17，使它使用通信类处理的缺省电路定义，以而不使用电路专用定义。

```
t 6
 Gateway user configuration
 Config>feature brs      1
 Bandwidth Reservation User Configuration
 BRS Config>interface 1     2
 BRS [i 1]Config>enable
 Please reload router for this command to take effect.
 BRS [i 1] Config>circuit 16    3
 BRS [i 1][dlci 16] Config>enable
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1][dlci 16] Config>exit
 BRS [i 1]Config>circuit 17
 BRS [i 1][dlci 17] Config>enable
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1][dlci 17] Config>exit
 BRS [i 1]Config>circuit 18
 BRS [i 1][dlci 18] Config>enable
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1][dlci 18] Config>
 *reload
 Are you sure you want to reload the gateway? (Yes or [No]): yes



 *t 6
 Gateway user configuration
 Config>feature brs
 Bandwidth Reservation User Configuration
 BRS Config>interface 1
 BRS[i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
       16  using defaults.
       17  using defaults.
       18  using defaults.

 default class is DEFAULT



BRS [i 1] Config>?
 ENABLE
 DISABLE
 SET-CIRCUIT-DEFAULTS
 CIRCUIT
 ADD-CIRCUIT-CLASS
 DEL-CIRCUIT-CLASS
 CHANGE-CIRCUIT-CLASS
 DEFAULT-CIRCUIT-CLASS
 ASSIGN-CIRCUIT
 DEASSIGN-CIRCUIT
 QUEUE-LENGTH
 LIST
 SHOW
```

```
CLEAR-BLOCK
EXIT
BRS [i 1] Config>set-circuit-defaults     4
BRS [i 1] [circuit defaults] Config>?
ADD-CLASS
DEL-CLASS
CHANGE-CLASS
DEFAULT-CLASS
TAG
UNTAG
ASSIGN
DEASSIGN
LIST
EXIT
BRS [i 1] [circuit defaults] Config>add    5
Class name [DEFAULT]?DEF1
Percent bandwidth to reserve [10]? 5
BRS [i 1] [circuit defaults] Config>add
Class name [DEFAULT]?DEF2
Percent bandwidth to reserve [10]?5
BRS [i 1] [circuit defaults] Config>assign ip
Class name [DEFAULT]?DEF1
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS [i 1] [circuit defaults] Config>assign asrt
Class name [DEFAULT]? DEF2
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS[i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.



class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS  [i 1] [circuit defaults] Config>exit
BRS  [i 1] Config>circuit 16     6
BRS  [i 1][dlci 161] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.
```

```
  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL



 BRS  [i 1] [dlci 16]
Config>show

  BANDWIDTH RESERVATION currently in RAM
  interface number 1, circuit number 16 using defaults.
  maximum queue length 10, minimum queue length 3
  4 current defined classes:
    class LOCAL has 10% bandwidth allocated
    class DEFAULT has 40% bandwidth allocated
    class DEF1 has 5% bandwidth allocated
    class DEF2 has 5% bandwidth allocated

  protocol and filter assignments:

  Protocol/Filter      Class              Priority    Discard Eligible
  ---------------      -----              --------    ----------------
  IP                   DEF1                 NORMAL             NO
  ARP                  DEFAULT              NORMAL             NO
  DNA                  DEFAULT              NORMAL             NO
  VINES                DEFAULT              NORMAL             NO
  IPX                  DEFAULT              NORMAL             NO
  OSI                  DEFAULT              NORMAL             NO
  AP2                  DEFAULT              NORMAL             NO
  ASRT                 DEF2                 NORMAL             NO

  BRS [i 1] [dlci 16] Config>exit


 BRS [i 1] Config>circuit 17
  BRS [i 1] [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17 using defaults.
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 60%
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible
```

```
  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>add-class    7
  This circuit is currently using circuit defaults...
  Are you sure you want to override the defaults ?(Yes or [No]):
yes
  Class name [DEFAULT]? CIRC171
  Percent bandwidth to reserve [10]? 5
  BRS[i 1] [dlci 17] Config>assign vines
  Class name [DEFAULT]? CIRC171
  Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
  Frame Relay Discard Eligible <NO/YES>[NO]?


 BRS [i 1] [dlci 17]
Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 65%
  total classes defined (counting one local and one default) 5


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible


  class DEF1 has 5% bandwidth allocated
    the following protocols and filters assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible


  class CIRC171 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol VINES with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>show

  BANDWIDTH RESERVATION currently in RAM
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  5 current defined classes:
    class LOCAL has 10% bandwidth allocated
    class DEFAULT has 40% bandwidth allocated
    class DEF1 has 5% bandwidth allocated
    class DEF2 has 5% bandwidth allocated
    class CIRC171 has 5% bandwidth allocated



  protocol and filter assignments:

  Protocol/Filter      Class              Priority    Discard Eligible
```

```
---------------      -----              --------    ----------------
IP                   DEF1                 NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                CIRC171              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEF2                 NORMAL            NO

BRS [i 1] [dlci 17] Config>exit
BRS [i 1] Config>set-circuit-defaults
BRS [i 1] [circuit defaults] Config>change DEF1     8
Percent bandwidth to reserve [ 5]? 10
BRS [i 1] [circuit defaults] Config>change DEF2
Percent bandwidth to reserve [5]? 10
BRS [i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [circuit defaults] Config>exit


BRS [i 1] Config>circuit 16
  BRS [i 1] [dlci 16] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 16 using defaults.
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 70%
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 10% bandwidth allocated
    the following protocols and filters are assigned:
```

```
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 16] Config>exit


BRS [i 1] Config>circuit 17
  BRS [i 1[ [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 65%
  total classes defined (counting one local and one default) 5


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible


  class DEF1 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible


  class CIRC171 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol VINES with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>use-circuit-defaults     9
  This circuit is currently NOT using circuit defaults...
  Are you sure you want to delete current definitions and use defaults ? (Yes or
  [No]): yes
  Defaults are in effect for this circuit.
  Please reload router for this command to take effect.
  BRS [i 1] [dlci 17] Config>
  *restart
  Are you sure you want to reload the gateway? (Yes or [No] ):yes


  *t 6
  Gateway user configuration
  Config>feature brs
  Bandwidth Reservation User Configuration
  BRS Config>interface 1
  BRS [i 1] Config>circuit 17
  BRS [i 1] [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17 using defaults.
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 70%
```

```
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


   class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL



  BRS [i 1] [dlci 17]
Config>show

  BANDWIDTH RESERVATION currently in RAM
  interface number 1, circuit number 17 using defaults.
  maximum queue length 10, minimum queue length 3
  4 current defined classes:
    class LOCAL has 10% bandwidth allocated
    class DEFAULT has 40% bandwidth allocated
    class DEF1 has 10% bandwidth allocated
    class DEF2 has 10% bandwidth allocated

  protocol and filter assignments:

  Protocol/Filter      Class              Priority    Discard Eligible
  ---------------      -----              --------    ----------------
  IP                   DEF1                 NORMAL            NO
  ARP                  DEFAULT              NORMAL            NO
  DNA                  DEFAULT              NORMAL            NO
  VINES                DEFAULT              NORMAL            NO
  IPX                  DEFAULT              NORMAL            NO
  OSI                  DEFAULT              NORMAL            NO
  AP2                  DEFAULT              NORMAL            NO
  ASRT                 DEF2                 NORMAL            NO

  BRS [i 1] [dlci 17] Config>exit
```

使用 BRS 和优先级排队

第2章 配置和监控保留带宽

本章描述保留带宽系统 (BRS) 的配置和操作命令。

本章包括以下几个部分:

- 『保留带宽配置概述』
- 第20页的『保留带宽配置命令』
- 第37页的『进入保留带宽监控提示状态』
- 第38页的『保留带宽监控命令』

保留带宽配置概述

要使用保留带宽配置命令并在路由器上配置保留带宽，请:

1. 在 OPCON (*) 提示符下，输入 **talk 6**。
2. 在 Config> 提示符下，输入 **feature brs**。
3. 在 BRS Config> 提示符下，输入 **interface #**。
4. 在 BRS [i 0] Config> 提示符下，输入 **enable**。

   这是接口提示层，本例中的接口号为零。对每个正在配置的接口重复步骤 3 和步骤 4。

   如果在帧中继接口上配置 BRS，则继续步骤 4a:

   如果在其他接口上配置 BRS，直接转向步骤 5。

   a. 在 BRS [i 0] Config> 提示符下，输入 **circuit** #，其中 # 是要配置的线路号。
   b. 在 BRS [i 0] [dlci 16] Config> 提示符下，输入 **enable**。这是线路提示级别，本例中的线路 (DLCI) 号是 16。
   c. 在 BRS [i 0] [dlci 16] Config> 提示符下，输入 **exit** 返回接口级提示状态。
   d. 对每个需定义 BRS t 类的线路重复步骤 4a 到 4c。
5. 重装 此路由器。
6. 重复步骤 1 到 3，为已启用的特定接口配置保留带宽。
7. 如果正在 PPP 接口上配置 BRS，则在 BRS[i 0]Config> 提示符下，使用第21页的表3 中所列的配置命令，配置通信量类别，将协议、过滤器和标签分配给通信量类别。如果正在 FR 接口上配置 BRS，执行步骤 8 到 10。
8. 如果正在 FR 接口上配置 BRS，可使用第21页的表2中所列的命令配置线路类别，并将线路分配给线路类别。
9. 如果使用缺省线路定义，则在 BRS[i 0]Config> 提示符下输入 **set-circuit-defaults** 命令。执行此操作即可到 BRS[i 0][circuit defaults] 提示符下，可使用第21页的表3 中相应命令配置通信量类别，为通信量类别分配协议、过滤器及标签。一旦完成为通信量类别处理定义缺省线路定义，则输入 “exit” 返回 BRS[i 0] Config> 提示符。
10. 如果您的 FR 线路不能使用缺省线路定义进行通信量类别处理，则输入 **circuit** *permanent-virtual-circuit circuit_number*。执行此操作即可进入线路提示状态，然后使用第21页的表3中列出的命令为通信量类别处理创建线路特定定义。

注: 无需重装此路由器使 t 类和 c 类配置更改生效。

输入 **talk 6 (t 6)** 命令可进入配置进程。

输入 **feature brs** 命令可进入 BRS 配置进程。在命令中输入功能名 (brs) 或号码 (1)。

命令 **interface #** 选取用户要为保留带宽配置的特定接口。配置 BRS 类别之前，必须使用命令 **enable** 启用接口上的 BRS。在第19页的4 中，提示表明选取的接口号为零。

circuit # 命令可用来选择要配置 BRS 通信量类的 FR 接口上的电路。为此线路配置 BRS t 类时，必须使用 **enable** 命令启用线路上的 BRS。在 第19页的4.b 中，提示表明已选取接口 0 上的线路 16。

配置线路类别(仅对帧中继)和通信量类别之前，必须启用选定接口和线路的预留带宽，然后重装此路由器。

若要随时返回到 `Config>` 提示符下，在不同的 BPS 提示层输入 **exit** 命令，直到退回 `Config>` 提示符下。

保留带宽配置命令

本节描述的是保留带宽配置命令。可以使用的命令将随显示 BRS 配置提示符不同 (`BRS Config>`、 `BRS [i x] Config>` 、 `BRS [i x] [dlci y] Config>` 或 `BRS [i x] [circuit defaults] Config>`) 而不同。

表 1. 保留带宽配置命令摘要 (BRS Config> 提示状态下的可用命令)

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Activate-IP-precedence-filtering	对通过安全 IP 信道发送的，或处于次级 TCP 或 UDP 分段中的 APPN 或 SNA 包，激活其 BRS IPv4 优先过滤。在配置 DLSw、HPR over IP 或 TN3270 时，还必须配置 IPv4 优先位设定。
Deactivate-IP-precedence-filtering	停止 IPv4 优先过滤处理。
Enable-hpr-over-ip-port-numbers	对 APPN-HPR over IP 通信量启用 BRS 过滤，允许配置用来识别 HPR over IP 包的 UDP 端口号。 **注:** 如果 APPN 存在于装入映像中，则不支持此命令，因为 BRS 从 APPN 获知是否已经配置 HPR over IP 。如果已配置，则从 APPN 支持获取那些将用于 HPR over IP 包的 UDP 端口号。
Disable-hpr-over-ip-port-numbers	禁用 APPN-HPR over IP 通信量的 BRS 过滤。 **注:** 如果 APPN 存在于装入映像中，则不支持此命令，因为 BRS 已从 APPN 获知是否已配置 HPR over IP。

表 1. 保留带宽配置命令摘要 (BRS Config> 提示状态下的可用命令) (续)

命令	功能
Interface	选择要配置保留带宽的接口。 **注:** 使用任何其它配置命令前必须输入此命令。请参阅表2和 表3。
List	列出可支持保留带宽的接口，并表明这些接口的保留带宽是启用的还是禁用的。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

表 2. 对于帧中继接口，BRS 接口配置命令可在 BRS [i #] Config> 提示符下使用

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add-circuit-class	设置 c 类带宽的名称及其带宽百分比。
Assign-circuit	分配一指定线路给特定 c 类带宽。
Change-circuit-class	更改为 c 类带宽配置的带宽量。
Circuit	进入 BRS 线路级提示状态 (BRS [i x][dlci y] Config>) ，在该提示符下可使用表3中所列命令，配置帧中继线路上的保留带宽。
Clear-block	从 SRAM 清除与当前接口有关的配置数据。线路类配置数据，和通信类处理的缺省线路定义被清除。
Deassign-circuit	将指定线路恢复为缺省的 c 类
Default-circuit-class	指定缺省 c 类带宽的名称及其在接口带宽中所占的百分比。
Del-circuit-class	删除指定 c 类带宽。
Disable	禁用接口上的保留带宽。
Enable	启用接口上的保留带宽。
List	显示 SRAM 中 c 类和分配的线路定义。
Queue-length	设置优先级队列中包数目的最大值和最小值。
Set-circuit-defaults	进入 BRS [i x] [circuit defaults] Config> 命令提示符状态，以便使用表3中适当的命令为通信类别处理创建缺省线路定义。
Show	显示 SRAM 中当前定义的 c 类别和指定的线路。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

下表列出可用的 BRS 线路命令，对于 PPP 接口，可在 BRS [i x] Config> 提示符下执行，对于帧中继线路，可在 BRS [i x] dlci [y] Config> 提示符下执行，也可在 BRS [i x] [circuit defaults] Config> 提示符下执行。

表 3. BRS 通信类处理命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add-class	分配一指定量的带宽给用户定义的通信量类。
Assign	分配协议或过滤器给配置的通信量类。
Change-class	更改为 t 类带宽配置的带宽量。
Clear-block	从 SRAM 清除 PPP 接口上或帧中继线路上通信量类、协议、过滤器、标识符分配配置数据。 **注:** 此命令不能在 BRS [i x] [circuit defaults]Config> 提示符下执行。
Deassign	将对指定包或过滤器的排队方法恢复为使用缺省 t 类和缺省优先级。
Default-class	按需要设置缺省的 t 类和优先级，并将所有未分配的协议指定给新的缺省 t 类。
Del-class	删除先前配置的 t 类带宽。

表 3. BRS 通信类处理命令 (续)

命令	功能
Disable	禁用在此 PPP 接口或帧中继线路上保留带宽。 **注:** BRS 无法在 BRS [i x] [circuit defaults] Config> 提示符下启用，或禁用。
Enable	启用在此 PPP 接口或帧中继线路上保留带宽。 **注:** BRS 在 BRS [i x] [circuit defaults] Config> 提示符下无法启用，或禁用。
List	列出 SRAM 中存储的已配置的 t 类和协议、过滤器和标签赋值。
Queue-length	设置优先级队列中的包的最大数目和最小数目。 **注:** 在 BRS [i x] [circuit defaults] Config> 提示符下不支持此命令。
Show	列出 RAM 中存储的当前定义的 t 类和协议、过滤器和标签赋值。 **注:** BRS [i x] [circuit defaults] Config> 提示符下不支持此命令。
Tag	为配置 MAC 过滤功能时标识的 MAC 过滤器分配一个 BRS 标签名 (TAG1 - TAG5)。
Untag	删除 BRS 标签名 (TAG1 - TAG5) 与配置 MAC 过滤功能时标识的 MAC 过滤器的相关关系。
Use-circuit-defaults	允许用户删除线路专用定义，使用线路缺省定义进行通信量类别处理。此命令对帧中继仅在 BRS [i x] dlci [y] Config> 提示符下有效。 **注:** 必须重装此路由器以使缺省值生效。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

使用相应的命令配置点对点协议 (PPP) 和帧中继保留带宽。对于帧中继，需配置线路和网络接口。对于 PPP，只需配置网络接口。

注:

1. 当从 BRS 接口菜单发出 **clear-block**、 **disable**、**enable**、 **list** 和 **show** 命令时，这些命令将影响或列出为选定接口配置的保留带宽信息。如果这些命令从 BRS 线路菜单上发出，则它们只影响或显示配置给永久虚拟线路 (PVC) 的帧中继保留带宽信息。
2. 使用保留带宽命令前，请记住:
   - 使用任何其它的配置命令前，必须先使用 **interface** 命令选择一接口。(BRS 配置强制要求这一操作。)
   - 参数 *Class-name (类名称)* 区分大小写。
   - 要查看当前的 *class-names*，使用 **list** 或 **show** 命令。
   - 在接口或线路上启用保留带宽后，可增加/删除/更改线路和通信量类别，动态分配线路或协议。enable、disable、use-circuit-defaults 和 clear-block 命令必须重装路由器才能生效。
3. t 类和 c 类配置的更改内容无需重装 此路由器即可生效。

Activate-IP-precedence-filtering

使用 **activate-ip-precedence-filtering** 命令，激活 APPN 和 SNA 包的 BRS IPv4 优先过滤系统，这些包是通过安全 IP 隧道发送的，或按次级的 TCP 或 UDP 分段发送

的 。配置 DLSw、HPR over IP 或 TN3270 时，还须配置 IPv4 优先位设置值。详情请参阅第8页的『将 IP 版本 4 优先位处理用于 IP 安全隧道和次级分段中的 SNA 通信』。

语法:

activate-ip-precedence-filtering

Add-circuit-class

注: 只在配置帧中继时使用。

在接口层使用 **add-circuit-class** 命令，分配指定数量的带宽，分配给用户定义的 c 类带宽的线路组使用。

语法:

add-circuit-class *class-name %*

Add-class

使用 **add-class** 命令分配一指定量的带宽给用户定义的 t 类带宽。

注: 如果此命令用于一个帧中继线路，且该线路当前使用缺省线路定义进行通信处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，则线路将改成通信类处理时使用的线路专用定义，此时允许命令运行。如果回答『No』，则放弃此命令，而继续使用缺省的线路定义。若要更改缺省线路定义，则应进到 BRS [ix][circuit defaults]Config> 命令提示符下。

语法:

add-class [*class-name* 或 *class#*] *%*

示例 1: **在帧中继线路上增加一个名为 CIRC17 的类**

```
BRS [i 1] [dlci 17] Config>add-class
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults ?(Yes or
[No]):y
Class name [DEFAULT]? CIRC17
Percent bandwidth to reserve [10]?5
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17
maximum queue length 10, minimum queue length 3
total bandwidth allocated 65%
total classes defined (counting one local and one default) 5


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible
```

```
 class DEF1 has 5% bandwidth allocated
   protocol IP with priority NORMAL is not discard eligible.


 class DEF2 has 5% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.


 class CIRC171 has 5% bandwidth allocated
   no protocols or filters are assigned to this class.

 assigned tags:

 default class is DEFAULT with priority NORMAL
```

示例 2: 在帧中继线路上增加一个名为 class1 的类

```
BRS [i 2] [dlci
128]>add
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults ?(Yes or [No]):
y
Class name [DEFAULT]?
Class is already allocated.
BRS [i 2] [dlci 128]>add class1
Percent bandwidth to reserve [10]?
BRS [i 2] [dlci 128]>

BRS [i 2] [dlci 128]>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible

class class1 has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] [dlci 128]>
```

Assign

使用 **assign** 命令分配指定标签、协议包或过滤器给一个给定 t 类，并分配此类范围的优先级。四个优先级类型是:

- Urgent
- High
- Normal (缺省优先级)
- Low。

语法:

assign [*protocol-class* or TAG or *filter-class*] [*class-name* or *class#*]

assign 命令还允许为帧中继的帧设置合理丢弃 (DE) 位。

注: 如果此命令用于帧中继线路，而线路当前使用缺省线路定义进行通信量类别处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，线路将被改成使用线路专用定义进行通信处理，此时允许命令运行。如果回答『No』，放弃此命令，缺省线路定义继续使用。要想更改缺省线路定义，应进入 BRS [i x][circuit defaults]Config> 命令提示状态。

实例 1:

```
assign IPX test
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? low
protocol IPX maps to class test with priority LOW Discard eligible <Yes/no> [N]?
```

实例 2: 分配一个 TOS 过滤器给 class1; 先前已使用 *add class* 命令将 class1 增加到配置中。

```
BRS [i 2] [dlci 128]>assign ?
IP
ARP
DNA
VINES
IPX
OSI
AP2
ASRT
TUNNELING-IP
SDLC/BSC-IP
RLOGIN-IP
TELNET-IP
NETBIOS
SNA/APPN-ISR
SNMP-IP
MULTICAST-IP
DLSW-IP
TAG1
TAG2
TAG3
TAG4
TAG5
APPN-HPR
NETWORK-HPR
HIGH-HPR
MEDIUM-HPR
LOW-HPR
XTP-IP
UDP_TCP1
UDP_TCP2
UDP_TCP3
UDP_TCP4
UDP_TCP5
TOS1
TOS2
TOS3
TOS4
TOS5
Protocol or filter name [IP]? TOS1  1
Class name [DEFAULT]? class1  2
Priority  [NORMAL]?
Frame Relay Discard Eligible  [NO]?
TOS Mask [1-FF] [FF]?
TOS Range (Low) [0-FF] [0]? 1
TOS Range (High) [1]? 3
BRS [i 2] [dlci 128]> list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
```

```
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible


class class1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    filter TOS1 with priority NORMAL is not discard eligible
       with TOS range x1 - x3 and TOS mask xFF

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] [dlci 128]>show

BANDWIDTH RESERVATION currently in RAM
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
3 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class class1 has 10% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEFAULT              NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEFAULT              NORMAL            NO
TOS1                 class1               NORMAL            NO
   TOS range x1 - x3
    TOS mask xFF

BRS [i 2] [dlci 128]>
```

1 使用 TOS 过滤器时，用户需输入三个参数：TOS mask、TOS range-low 和 TOS range- high。请参考*Protocol Configuration and Monitoring Reference Volume 1*中『配置和监控 IP』一章的 『Add』 命令，获得这些参数的详细说明。

Assign-circuit

注: 只在配置帧中继时使用。

在接口层使用命令 **assign-circuit**，分配指定线路给指定 c 类带宽。为线路类分配 PVC 时，使用 DLCI；为线路类分配 SVC 时，使用线路名。

注: 必须在虚拟线路上使用命令 **circuit** 启用 BRS，在使用此命令分配线路给线路类时，需重装此路由器。

语法:

assign-circuit *# class name*

Change-circuit-class

注: 只在配置帧中继时使用。

在接口层使用 **change-circuit-class** 命令，更改分配给指定 c 类的线路组所使用的带宽百分比。

语法:

change-circuit-class *class-name %*

Change-class

使用 **change-class** 命令更改为 t 类带宽配置的带宽量。

注: 如果此命令用于一个帧中继线路，且该线路当前使用缺省线路定义进行通信处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，线路将被改成使用线路专用定义进行通信处理，此时允许命令运行。回答『No』，则放弃此命令，缺省线路定义继续使用。要想更改缺省线路定义，应进入 BRS [i x][circuit defaults]Config> 命令提示状态。

语法:

change-class [*class-name* 或 *class#*] *%*

Circuit

注: 只在配置帧中继时使用。

使用 **circuit** 命令配置帧中继永久虚拟线路 (PVC) 或交换虚拟线路 (SVC)。此命令只能从 BRS 接口配置提示符下 (BRS [i #] Config>) 发出。

语法:

*ci***rcuit**

在命令 **add-class**、 **assign** 、**default-class**、 **del-class**、**deassign** 或 **change-class** 可执行前，必须启用线路上的 BRS ，并重装此路由器。

PVC 实例:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth:  [16]

BRS [i 1 ] [dlci 16] Config> enable
```

SVC 实例:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth:  [16]
svc01

BRS [i 1 ] [svc svc01] Config> enable
```

配置 BRS 和优先级排队

在帧中继线路上发出 **enable** 命令，且此路由器已重装后，在此线路上可以运行以下配置命令:

add-class	deassign	enable	tag
assign	default-class	exit	untag
change-class	del-class	list	clear-block
disable	show	use-circuit-defaults	

Clear-block

使用 **clear-block** 命令，从 SRAM 中清除当前保留带宽配置数据。

语法:

clear-block

- 对于 PPP 协议，如果从接口提示符下输入此命令，则清除此接口上所有 BRS 配置数据。
- 对于帧中继，如果在接口提示符下输入此命令，则在此接口或此接口的所有线路上不再启用 BRS，并将清除用于通信量类处理的所有线路类配置数据和缺省线路定义。但是，每一条线路上的通信量类配置数据并没有清除，如果在接口上重启 BRS，则这些数据可用。
- 要清除线路通信量类别配置数据，首先从接口层提示符下输入命令 **circuit**，然后从线路层提示符下输入命令 **clear-block**。当清除了每条线路上的通信量类别配置数据后，在接口层提示符下输入命令 **clear-block**，以清除线路类配置数据。所作更改在重装此路由器后生效。

实例:

```
clear-block
You are about to clear BRS configuration information for this interface
Are you sure you want to do this (Yes or No): y
BRS [i 1] Config>
```

Deactivate-IP-precedence-filtering

使用 **deactivate-ip-precedence-filtering** 命令取消 IPv4 优先过滤处理。

语法:

deactivate-ip-precedence-filtering

Deassign

使用 **deassign** 命令可将指定协议包或过滤器排队方法恢复为使用缺省 t 类和缺省优先级。

注: 如果此命令用于帧中继线路，而线路当前使用缺省线路定义进行通信量类别处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，则线路将改成通信类处理时使用的线路专用定义，此时允许命令运行。 回答『No』，则放弃此命令，继续使用缺省的线路定义。若要更改缺省线路定义，则应进到 `BRS [i x][circuit defaults]Config>` 命令提示符下。

语法:

deassign [*prot-class* or *filter-class*]

Deassign-circuit

注: 只在配置帧中继时使用。

在接口层使用命令 **deassign-circuit** 恢复指定线路排队方法为缺省的 c 类。

语法:

deassign-c #

Default-circuit-class

注: 只在配置帧中继时使用。

在接口层使用命令 **default-circuit-class** 设置缺省 c 类带宽的用户定义名，以及分配给此类线路的带宽的百分比，其中包括未分配给 c 类带宽的孤立线路。

语法:

default-circuit-class *class-name %*

Del-circuit-class

注: 只在配置帧中继时使用。

在接口层使用 **del-circuit-class** 命令，删除指定 c 类带宽。

语法:

del-circuit-class *class-name*

Default-class

使用 **default-class** 命令按需要设置缺省 t 类和优先级的值。如果先前未指定值，则使用系统缺省值。否则，使用最后一个先前指定值。

注: 如果此命令用于帧中继线路，而该线路当前正使用缺省线路定义进行通信处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，则线路将改成通信类处理时使用的线路专用定义，此时允许命令运行。 回答『No』，则放弃此命令，继续使用缺省的线路定义。若要更改缺省线路定义，则应进到 `BRS [i x][circuit defaults]Config>` 命令提示符下。

语法:

default-cl [*class-name* 或 *class#*] *priority*

Del-class

使用 **del-class** 命令从指定接口或线路上删除先前配置的 c 类带宽。

注: 如果此命令用于帧中继线路，而该线路当前正使用缺省线路定义进行通信类处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，则线路将改成通

信类处理时使用的线路专用定义，此时允许命令运行。回答『No』，则放弃此命令，继续使用缺省的线路定义。若要更改缺省线路定义，则应进到 BRS [ix][circuit defaults]Config> 命令提示符下。

语法:

del-class [*class-name* 或 *class#*]

Disable

使用 **disable** 命令禁用接口(如果在接口提示符下输入)或线路(如果在线路提示符下输入)上的保留带宽。所作更改在重装此路由器后生效。

要验证是否已禁用保留带宽，请输入命令 **list**。

语法:

disable

Disable-hpr-over-ip-port-numbers

使用命令 **disable-hpr-over-ip-port-numbers**，禁用 HPR over IP 通信的 BRS 过滤。

语法:

disable-hpr-over-ip-port-numbers

要验证是否禁用 HPR over IP 通信的 BRS 过滤，请输入命令 **list**。

注: 如果装入映像中包括 APPN，则可配置 HPR over IP 通信是否将在 APPN Config> 命令提示符下使用。

Enable

使用命令 **enable**，在接口上(如果在接口提示符下使用)，或在线路上(如果在线路提示符下使用)启用保留带宽。所作更改在重装此路由器后生效。

语法:

enable

注:

- 在 PPP 接口上配置 BRS 时，在接口提示符下发出命令 **enable**，并在配置通信类、分配协议和过滤器给通信量之前，重装 此路由器。
- 在帧中继线路上初始化启用 BRS 时，线路初始化为使用缺省线路定义执行通信量类处理。在接口提示符下，和需要定义通信量类的每条线路的提示符下，发出 **enable** 命令。然后在配置接口的线路类，和每条线路的通信量类之前，重装此路由器。例如:

```
t 6
Gateway user configuration
Config>f brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>enable
```

```
Please reload
router for this command to take effect
BRS [i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1


class DEFAULT has 10% bandwidth allocated
  no circuits are assigned to this class.

default class is DEFAULT

BRS [i 1] Config>circ 16
BRS [i 1] [dlci 16] Config>enable
Defaults are in effect for this circuit.
Please reload
router for this command to take effect.
BRS [i 1] [dlci 16] Config>ex
Please reload
router for this command to take effect.
BRS [i 1] [dlci 16] Config>
```

Enable-hpr-over-ip-port-numbers

使用命令 **enable-hpr-over-ip-port-numbers** 启用 APPN-HPR over IP 通信量的 BRS 过滤，配置用于识别 HPR over IP 包的 UDP 端口号。

注: 如果装入映像中包括 APPN，则在 APPN Config> 命令提示符下启用 HPR over IP，并指定用于 HPR over IP 通信量的 UDP 端口号。

语法:

enable-hpr-over-ip-port-numbers

实例:

```
BRS Config> enable-hpr-over-ip-port-numbers
XID exchange port number [12000]?
HPR net  trans prio port number [12001]?
HPR high trans prio port number [12002]?
HPR medium trans prio port number [12003]?
HPR low    trans prio port number [12004]?
```

XID exchange port number

此参数用来指定用于 XID 交换的 UDP 端口号。此端口号必须与在网络中其他设备上定义的端口号相同。

有效值: 1024 - 65535

缺省值: 12000

Network priority port number

此参数用来指定用于网络优先通信的 UDP 端口号。此端口号必须与在网络中其他设备上定义的端口号相同。

有效值: 1024 - 65535

缺省值: 12001

High exchange port number

此参数用来指定用于网络高优先级通信的 UDP 端口号。此端口号必须与在网络中其他设备上定义的端口号相同。

有效值: 1024 - 65535

缺省值: 12002

Medium exchange port number

此参数用来指定用于中优先级通信的 UDP 端口号。此端口号必须与在网络中其他设备上定义的端口号相同。

有效值: 1024 - 65535

缺省值: 12003

Low exchange port number

此参数用来指定用于低优先级通信的 UDP 端口号。此端口号必须与在网络中其他设备上定义的端口号相同。

有效值: 1024 - 65535

缺省值: 12004

Interface

使用 **interface** 命令，选择将应用保留带宽配置命令的串行接口。*运行 PPP (点对点协议)的路由器和帧中继接口支持保留带宽。*

语法:

interface *interface#*

注:

1. 为了在新的接口上输入保留带宽命令，使用其它任何保留带宽配置命令***之前***，必须输入此命令。如果已退出保留带宽提示，希望返回到先前配置的接口更改保留带宽，首先要再次输入此命令。
2. 如果使用 WAN 恢复，并在主接口上配置 BRS， 还必须在辅接口上配置 BRS。一般情况下，使用 WAN恢复时，辅接口可以替代主接口。但 BRS 却不能作相应转换；因此，BRS 需要在主接口和辅接口上同时配置。

要在特殊接口上启用保留带宽，在 `BRS Config>` 提示符下，输入支持特殊协议或功能的接口的号码。然后，您可以按本章中描述的那样，使用 BRS **enable** 配置命令。启用接口号后，在对接口进行任何其它配置更改前，必须重新加载 2212 使命令生效。

注:

1. 如果正在帧中继接口上配置 BRS，在重新加载此路由器前，可使用 **circuit** 命令选择线路，并在重新加载此路由器前启用这些线路上的保留带宽。

List

使用 **list** 命令显示当前定义的带宽类及其保证的百分比速率。

命令 **list** 和命令 **show** 类似。命令 **list** 显示当前 SRAM 定义，命令 **show** 显示当前 RAM 定义。

语法:

list *interface#*

在不同的提示符下发出 **list** 命令，其输出结果也将不同。可以在下列提示符下发出 **ist** 命令。

- BRS [i 1] [dlci 16] Config>
- BRS [i 1] Config>
- BRS Config>
- BRS [i 1] [circuit defaults] Config>

注: 如果在帧中继线路提示符下 (BRS [i x] [dlci y] Config>) 使用此命令，可显示线路在使用缺省线路定义，还是在使用线路专用定义进行通信量类处理。如果线路正在使用缺省线路定义，则显示当前缺省线路定义的通信量类、协议、过滤器和标签赋值。但是，如果想改变缺省线路定义，则需要进入 BRS[i x] [circuit defaults] Config> 提示符状态才能进行修改。

在 PPP 接口的 BRS 接口层提示符 (BRS [i 0]) 下和在帧中继接口的 BRS 线路层提示符 (BRS [i 0] [dlci 16] Config>) 下，命令 **list** 列出了通信量类、所配置的带宽百分比和分配的协议和过滤器。

在帧中继的 BRS 接口层提示符下，命令 **list** 列出线路类、所配置的带宽百分比和分配的线路。

实例 1

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is disabled

 BRS Config>interface 1
 BRS [i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
        17
        16  using defaults.
        18  using defaults.

 default class is DEFAULT

 BRS [i 2] Config>exit
 BRS Config>interface 2
 BRS [i 2] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 2
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 50%
 total classes defined (counting one local and one default) 2


 class LOCAL has 10% bandwidth allocated
```

```
  protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with default priority
     protocol ARP with default priority
     protocol DNA with default priority
     protocol VINES with default priority
     protocol IPX with default priority
     protocol OSI with default priority
     protocol AP2 with default priority
     protocol ASRT with default priority

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 2] Config>
```

实例 2

```
 BRS [i 1] [dlci 17]
Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
   protocol ASRT with priority NORMAL is not discard eligible
   filter NETBIOS with priority NORMAL is not discard eligible


class CLASS1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
   protocol IP with priority NORMAL is not discard eligible
   protocol ARP with priority NORMAL is not discard eligible
   protocol DNA with priority NORMAL is not discard eligible
   protocol VINES with priority NORMAL is not discard eligible
   protocol IPX with priority NORMAL is discard eligible
   protocol OSI with priority NORMAL is not discard eligible
   protocol AP2 with priority NORMAL is not discard eligible
```

实例 3

```
 BRS [i 1] [circuit defaults]
Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, default circuit
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 70%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.



 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible


 class DEF1 has 10% bandwidth allocated
   protocol IP with priority NORMAL is not discard eligible.


 class DEF2 has 10% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.
```

```
assigned tags:

default class is DEFAULT with priority NORMAL

 BRS [i 1] [circuit defaults] Config>
```

实例 4

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is enabled.

    Transmission Type   Port Number
    -----------------   -----------
        XID exchange        12000
        HPR network         12001
        HPR high            12002
        HPR medium          12003
        HPR low             12004
```

Queue-length

使用 **queue-length** 命令设置各个 BRS 优先级队列中可排队的包的数目。每个 BRS 类都有分配给其协议、过滤器和标签的优先级值，每个优先级队列内可存储此命令指定的包数。

语法:

queue-length *maximum-length minimum-length*

此命令设置可在每个 BRS 优先级队列中排列的缓冲区的最大数目，以及当此路由器输入缓冲区不足时，每个 BRS 优先级队列中可排列的缓冲区最大数目。

如果对 PPP 接口发出 **queue-length** 命令，则此命令设置定义给接口的 BRS t 类的每个优先级队列的队列长度值。

如果对帧中继接口发出 **queue-length** 命令 (在 `BRS [i 0] Config>` 提示符下)，则此命令为每个 BRS t 类优先级队列的长度设置缺省值，而 BRS t 类则为定义给接口的每一个永久虚拟线路。

对于帧中继 PVC，如果发出 **queue-length** 命令 (在类似下面的提示符下: `BRS [i 0] [dlci 16] Config>`)，则此命令将设置为 PVC 定义的 BRS t 类的各优先级队列的队列长度。这些值将替代为帧中继接口设置的缺省队列长度值。

警告: 如果不是特别需要，请不要使用此命令。队列长度的缺省值是推荐给大多数用户使用的值。如果设置的队列长度值太高，可能会严重降低路由器的性能。

Set-circuit-defaults

使用 **set-circuit-defaults** 命令可访问用来定义通信量类处理的缺省线路定义的命令。这样，接口上使用相同通信量类、协议、过滤器和标签赋值的帧中继线路，便可使用这些缺省线路定义。

语法:

set-circuit-defaults

Show

使用 **show** 命令显示 RAM 中当前定义的带宽类。

语法:

show *interface#*

在不同的提示符下发出 **show** 命令，其输出结果也将不同。可以在下列提示符下发出 **show** 命令。

- BRS [i *x*] Config> - 接口号 *x* 的接口层提示符。
- BRS [i *x*] [dlci *y*] Config> - 帧中继接口号 *x* 上的线路 *y* 的线路层提示符。以下实例显示的是在线路层提示符下 show 命令的输出。

```
BRS [i 1] [dlci 17]
Config>show

Protocol/Filter      Class             Priority    Discard Eligible
---------------      -----             --------    ----------------
IP                   CLASS1              NORMAL            NO
ARP                  CLASS1              NORMAL            NO
DNA                  CLASS1              NORMAL            NO
VINES                CLASS1              NORMAL            NO
IPX                  CLASS1              NORMAL            Yes
OSI                  CLASS1              NORMAL            NO
AP2                  CLASS1              NORMAL            NO
ASRT                 DEFAULT             NORMAL            NO
NETBIOS              DEFAULT             NORMAL            NO
```

在 PPP 的接口提示符和帧中继的线路提示符下，将显示通信量类信息。在帧中继的接口提示符下，将显示线路类信息。

注:

1. 在帧中继线路提示符下 (BRS [i x] [dlci y] Config>) 使用此命令，可指示线路是在使用缺省线路定义，还是在使用线路专用定义进行通信量类处理。如果线路正在使用缺省线路定义，则显示当前定义给缺省线路定义的通信量类、协议、过滤器和标标签赋值。但是，如果想改变缺省线路定义，则需要进到 BRS[i x] [circuit defaults] Config> 提示符下才能进行修改。
2. 此命令不能在 BRS [i x] [circuit defaults] Config> 提示符下执行。

Tag

使用 **tag** 命令可将一个 MAC 过滤器项分配给下一个可用的 BRS 标签名，该项已在配置 MAC 过滤功能时标记。BRS 标签名有 TAG1、TAG2、TAG3、TAG4 和 TAG5。在 assign 命令中使用 BRS 标签名，这样可将标签分配给 BRS 通信类。

语法:

tag *mac_filter_tag#*

使用 **list** 命令列出分配给 BRS 标签名的 MAC 过滤器标签，以及分配给带宽通信量类的 BRS 标签名。

注: 如果此命令用于一个帧中继线路，且该线路当前使用缺省线路定义进行通信处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，则线路将改成通

信类处理时使用的线路专用定义，此时允许命令运行。 回答『No』，放弃此命令，继续使用缺省的线路定义。若要更改缺省线路定义，则应进到 BRS [i x][circuit defaults]Config> 命令提示符下。

Untag

使用 **untag** 命令删除 MAC 过滤器标签号与 BRS 标签名的关系。只有当与标签对应的 BRS 标签名未分配给带宽通信量类时，才可删除此标签。

语法:

untag *mac_filter_tag#*

使用 **list** 命令，可显示哪些 MAC 过滤器标签分配给 BRS 标签名，哪些 BRS 标签名分配给通信量类。

注: 如果此命令用于一个帧中继线路，且该线路当前使用缺省线路定义进行通信处理，则要求用户选择是否替换缺省线路定义。如果回答『Yes』，则线路将改成通信类处理时使用的线路专用定义，此时允许命令运行。 回答『No』，则放弃此命令，继续使用缺省的线路定义。若要更改缺省线路定义，则应进到 BRS [i x][circuit defaults]Config> 命令提示符下。

Use-circuit-defaults

在线路层使用 **use-circuit-defaults** 命令，删除线路专用定义，使用线路缺省定义进行通信量类处理。系统将提示用户确认使用线路缺省值。

语法:

use-circuit-defaults

注:

1. 只在配置帧中继时使用此命令
2. 此路由器必须重装，以使缺省值生效。

实例:

```
BRS [i 1] [dlci 17]
Config>use-circuit-defaults
This circuit is currently NOT using circuit defaults...
 Are you sure you want to delete current definitions and use defaults ? (Yes or
 [No]): y
 Defaults are in effect for this circuit.
 Please reload
 router for this command to take effect.
 BRS [i 1] [dlci 17] Config>
```

进入保留带宽监控提示状态

要使用保留带宽监控命令并在路由器上监控保留带宽，请:

1. 在 OPCON 提示符 (*) 下，输入 **talk 5**。
2. 在 GWCON 提示符 (+) 下，输入 **feature brs**。
3. 在 BRS> 提示符下，键入 **interface#**，其中 # 是监控接口号。这样便可进入 BRS 接口层提示符，BRS [i x]>，其中 x 是接口号。

4. 在接口提示符下，键入 **circuit #** 以指定接口上待监控的线路，但此项操作仅限于帧中继。

   这样便可进入线路层提示符 BRS [i x] [dlci y]>，其中 x 是接口号，而 y 是线路号。

5. 在此提示符下，输入适当的监控命令。(请参考『保留带宽监控命令』。)

   talk 5 (t 5) 命令可使用户进入监控进程。

   feature brs 命令可使用户进入 BRS 监控进程。可使用功能名 (brs) 或号码 (1) 输入此命令。

   interface # 命令用于选择特定的、准备用于监控保留带宽的接口。

   circuit # 命令用于选择帧中继永久虚拟线路 (PVC) 的 DLCI。

   在 BRS> 提示符下输入 **exit** 命令，即可随时返回 GWCON 提示状态。

   只要进入保留带宽监控提示状态 (BRS>)，即可输入表4中描述的任何特定的监控命令。

保留带宽监控命令

本节总结并解释了保留带宽监控命令。表4列出了保留带宽监控命令。在不同的 BRS 监控提示符下 (BRS>, BRS [i x]> 或 BRS [i x] [dlci y]>)，所能使用的命令将有所不同。

表 4. 保留带宽监控命令摘要

命令	只能在 FR 上使用	功能
? (帮助)		显示此命令层下的全部可用命令，或者列出特定命令的选项(如果存在)。请参阅第xxvi页的『获得帮助』
Circuit	是	选择帧中继永久虚拟线路 (PVC) 的 DLCI。只有在线路提示层，才可监控帧中继保留带宽通信量。
Clear		清除当前 t 类计数器，将它们存储为**最终** t 类计数器。计数器按类列出。
Clear-circuit-class	是	清除当前 c 类计数器，将它们存储为**最终** c 类计数器。计数器按类列出。
Counters		显示当前 t 类计数器。
Counters-circuit-class	是	显示当前 c 类计数器。
Interface		选择要监控的接口。 **注:** 使用任何其它保留带宽监控命令前必须输入此命令。
Last		显示最后保存的 t 类计数器。
Last-circuit-class	是	显示最后保存的 c 类计数器。
Exit		返回前面的命令级。请参阅第xxvi页的『退出较低级别的环境』

Circuit

注: 仅在监控帧中继时使用。

使用 **circuit** 命令选择要进行监控的帧中继 PVC 的 DLCI。此命令只能从 BRS 接口监控提示符下 (BRS [i #]>) 发出。

语法:

circuit *permanent-virtual-circuit-#*

选择了帧中继线路后，下列命令可在线路提示符下使用:

```
   CLEAR
   COUNTERS
   LAST
EXIT
```

Clear

使用 **clear** 命令保存当前保留 t 类带宽计数器，这样，计数器便可通过 **last** 命令进行检索，并清除其中的值。计数器基于带宽通信类进行保留。

语法:

clear

Clear-Circuit-Class

注: 仅在监控帧中继时使用。

使用 **clear-circuit-class** 命令保存当前保留 c 类带宽计数器，这样，计数器便可通过 **last-circuit-class** 命令进行检索，并清除其中的值。这些计数器将基于线路类进行保留。

语法:

clear-circuit-class

Counters

使用 **counters** 命令显示统计信息，这些信息描述配置给 PPP 接口或帧中继线路的通信量类的保留带宽通信。

语法:

counters

实例: **counters**

```
Bandwidth Reservation Counters
Interface 1

Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
LOCAL                0              0              0
DEFAULT              1             30              0
CLASS 1              1             56              0
CLASS 2              0              0              0

TOTAL                2             86              0
```

注: Bytes Ovfl 列列出了无法传送的包的字节数。其原因可能是优先级队列的长度已达到最大，或包无法排队，而无法排队的原因则可能是优先级队列处于最小队列长度阈值，但发送包的接口的接收缓冲区又运行过慢。

Counters-Circuit-Class

注: 仅在监控帧中继时使用。

使用 **counters-circuit-class** 命令显示配置给帧中继线路的通信量类的统计信息。

语法:

counters-circuit-class

实例: **counters-circuit-class**

```
Bandwidth Reservation Circuit Class Counters
Interface 1


Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
DEFAULT             25           3402             26
CIRCLASS1            1             56              0
CIRCLASS2            0              0              0

TOTAL               26           3458             26
```

Interface

使用 **interface** 命令选择串行接口，以应用保留带宽监控命令。*运行 PPP (点对点协议)的路由器和帧中继接口支持保留带宽。*

语法:

interface *interface#*

注: 要在新接口上输入保留带宽命令，必须在使用任何其它保留带宽监控命令前，输入此命令。如果退出保留带宽监控提示符 (BRS>) 后又要返回监控保留带宽，则必须首先再次输入此命令。

要在特殊接口上监控保留带宽，在 BRS> 监控提示符下，输入接口号。然后，可使用本章描述的保留带宽监控命令。

Last

使用 **last** 命令显示最后保存的 t 类统计信息。t 类统计信息的显示格式与 **counters** 命令相同。

语法:

last

Last-Circuit-Class

注: 仅在监控帧中继时使用。

使用 **last-circuit-class** 命令显示最后保存的线路类统计信息。c 类统计信息的显示格式与 **counters-circuit-class** 命令相同。

语法:

last-circuit-class

第3章 使用 MAC 过滤

本章说明在信息包的处理中如何使用介质访问控制 (MAC) 以指定信息包的过滤器。该章节包括以下部分:

- 『MAC 过滤和 DLSw 通信』
- 第42页的『MAC 过滤参数』

过滤器是一系列应用于信息包以决定在桥接中如何处理信息包的规则。MAC 过滤仅作用于已桥接的通信量。

注: MAC 过滤可应用于隧道通信

在过滤进程中，对信息包进行处理、过滤或在桥接中对其加上并标记。具体操作为:

- **处理** - 允许信息包在通过桥接器时不受影响。
- **过滤** - 不允许信息包通过桥接器。
- **加标签** - 允许信息包通过桥接器，但是，要基于可配置的参数在 1 到 64 之间给信息包加上标号。

MAC 过滤器由下面的三个对象组成:

1. 过滤程器-项 - 应用于信息包内地址字段或任意窗口数据的一条规则。应用该规则的结果是判断真(成功匹配)或假(不匹配)。
2. 过滤器-列表 - 列出一个或多个过滤器-项。
3. 过滤器 - 包含一系列的过滤器-列表。

MAC 过滤和 DLSw 通信

您可通过 MAC 过滤来过滤 DLSw 网络的入网 LLC 通信。

为了设置 LLC 的过滤器，请将*桥接器网络*的编号用做过滤器的接口编号。在接口(为路由器而配置的)的编号加上 2，以确定桥接器网络的编号。如果要查看接口的列表，请在 `Config>` 提示符下输入 **list devices** 命令，或者在 `+` 提示符下输入 **configuration** 命令。

下例中，桥接器网络的编号是 7。

```
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
```

例如，在您设置桥接器网络的过滤器时，路由器并没有丢弃与排它过滤器相匹配的帧。相反，路由器将这些帧转发给桥接器。

MAC 过滤参数

您可指定下列所有参数或其中的一部分，以生成过滤器:

- 信源 MAC 地址或信宿 MAC 地址
- 信息包内要匹配的数据
- 应用于信息包字段(要进行过滤的)的掩码
- 接口号
- 输入输出指定
- 包含/排除/标记指定
- 标记值(如果指定了标记)

过滤器-项参数

下面的参数是用于创建一地址-过滤器-项:

- 地址类型: SOURCE 或 DESTINATION
- 标签: *tag-value*
- 地址掩码: *hex-mask*

各过滤器-项指定与信息包地址类型相匹配的地址类型 (SOURCE 或 DESTINATION)。

地址掩码是以十六进制输入的数字字符串，用于比较信息包的地址。在比较掩码与指定的 MAC 地址之前，将掩码应用到信息包的 SOURCE 或 DESTINATION MAC 地址中。

地址掩码的长度必须与 MAC 地址的长度相同，并且指定了将逻辑添加至 MAC 地址中的字节(在与指定的 MAC 地址作相等比较之前添加)。如果未指定掩码，则假设指定了所有的 1s。

过滤器-列表参数

下面的参数是用于创建过滤器-列表的:

- 名称: *ASCII-string*
- 过滤器-项列表: *filter-item 1 . . . filter-item n*
- 操作: INCLUDE、EXCLUDE、TAG(*n*)

为一个或多个过滤器-项建立过滤器-列表。为每个过滤器-列表都指定一个不同的名称。

将过滤器-列表应用到信息包，即指将各过滤器-项进行比较(按添加到列表的顺序作比较)。如果列表中的任何一过滤器-项返回了 TRUE 状态，那么过滤器-列表将返回到列表的指定操作下。

过滤器参数

下面的参数是用于创建过滤器的:

- 过滤器-列表名称: *ASCII-string 1 . . . ASCII-string n*

- 接口编号: *IFC-number*
- 端口方向: INPUT 或 OUTPUT
- 缺省操作: INCLUDE、EXCLUDE 或 TAG
- 缺省标记: *tag-value*

通过将一组滤器-列表名称与接口编号相关连，并分配 INPUT 或 OUTPUT 的指定，这样就创建了过滤器。把过滤器应用到信息包，是指将每个相关连的过滤器-列表都应用到指定接口上所正在接受 (INPUT) 或发送 (OUTPUT) 的信息包中。

当过滤器将信息包估计为 INCLUDE 的条件时，则转发信息包。当过滤器将信息包估计为 EXCLUDE 条件时，则丢弃信息包。当过滤器将信息包估计为 TAG 条件时，则认为可转发加有标记的信息包。

各过滤器的附加参数是缺省操作，这是由于所有的过滤器-列表不匹配而造成的结果。缺省操作是 INCLUDE。缺省操作可设置为 INCLUDE、EXCLUDE 或 TAG。另作说明的是: 如果缺省操作是 TAG，则也应指定标记值。

使用 MAC 过滤标记

下表列出了 MAC 过滤标记的一些用法

- 带宽保留和 MAC 过滤功能部件 (MCF) 使用标记，共同处理 MAC 地址过滤。使用带宽保留的用户可对桥接器通信量进行归类，例如，通过向通信量加标记来归类。
- 在 MAC 过滤配置主控制台中生成一过滤器-项，再指定一标记，就完成了标记进程。然后，用此标记为与此标记相关连的所有信息包建立一个带宽类。当前的标记数值必须是在 1 到 64 之间。
- 如果在 MAC 过滤配置进程中生成了加标记的过滤器，则可使用带宽保留 (BRS) **tag** 配置命令，给 MAC 过滤器标记编号指定一个 BRS 标记名 (TAG1、TAG2、TAG3、TAG4 或 TAG5)。然后，在 BRS **assign** 配置命令中使用 BRS 标记名，以向带宽保留通信类和优先级指定相应的 MAC 过滤器。
- 可从 1 到 5 的顺序设置 5 个加标记的 MAC 地址。首先搜索的 TAG1，然后搜索 TAG2 ，按此顺序一直搜索到 TAG5。

标记也可适用于 IP 隧道的『组』。在将信息包指定到特定的组的情况下(通过 MAC 地址过滤的加标记功能部件指定)，IP 通道端点可归属任何一组。

第4章 配置和监控 MAC 过滤

本章节说明如何进入 MAC 过滤配置提示符、监控提示符，及如何使用可操作的命令。包括以下部分:

- 第52页的『访问 MAC 过滤监控提示符』
- 第52页的『MAC 过滤监控命令』

进入 MAC 过滤配置提示符

使用 CONFIG 进程中的 **feature** 命令，访问 MAC 过滤配置命令。**feature** 命令允许您访问协议和网络接口配置进程之外的特定功能的配置命令。

在 **feature** 命令后输入一个问号，可获取您的软件发行版能用的功能列表。例如:

```
Config> feature ?
WRS
BRS
MCF
Feature name or number [MCF]?
```

如果要访问 MAC 过滤配置提示符，请输入 **feature** 命令，在其后加上*功能部件编号* (3) 或*缩略名称* (MCF)。例如:

```
Config> feature mcf
MAC Filtering user configuration
Filter config>
```

进入 MAC 过滤配置提示符后，您可以开始输入指定的配置命令。如果要在任意时间返回到 CONFIG 提示符下，则在 MAC 过滤配置提示符下输入 **exit** 命令。

MAC 过滤配置命令

本节概述 MAC 过滤配置命令。在 `Filter config>` 提示符下输入这些命令。

使用以下命令配置 MAC 过滤功能。

表 5. MAC 过滤配置命令概述

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Attach	向过滤器添加过滤器列表。
Create	生成过滤器列表或生成一个 INPUT 或 OUTPUT 过滤器。
Default	将指定过滤器的缺省操作设置为 EXCLUDE、INCLUDE 或 TAG。
Delete	删除与过滤器列表相关的全部信息。同时删除使用 create filter 命令所生成的过滤器。
Detach	从过滤器中删除一个过滤器列表。
Disable	禁用整个 MAC 过滤系统或禁用某个特定的过滤器。
Enable	全部启用 MAC 过滤系统或启用某个特定的过滤器。
List	列出关于所有的过滤器列表及过滤器(由用户配置)的摘要。同时，为此过滤器所附的过滤器列表及此过滤器的后续信息生成一个列表。
Move	指定过滤器所附的过滤器列表进行重新排序。

表 5. MAC 过滤配置命令概述 (续)

命令	功能
Reinit	以更新的配置重新初始化整个 MAC 过滤系统，而不影响路由器的其它部分。
Set-Cache	更改过滤器的高速缓冲存储区大小。
Update	添加或删除特定过滤器列表中的信息。并且，向您提供合适的子命令菜单。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Attach

使用 **attach** 命令，向过滤器添加过滤器-列表。

通过将一组过滤器-列表与接口编号相关联，从而建立起过滤器。一个或多个过滤器-项形成了过滤器-列表。

语法:

attach *filter-list-name filter-number*

Create

使用 **create** 命令,生成过滤器-列表或 INPUT 或 OUTPUT 过滤器。

语法:

create list *filter-list-name*

filter [input or output] *interface-number*

list *filter-list-name*
生成过滤器-列表。列表的名称是由用户选择的至多 16 个字符所组成的唯一字符串 (Filter-list-name)。此名字是用于标识正在建立中的过滤器-列表。它也可以同过滤器-列表相关的其它命令一起使用。

filter [input or output] *interface-number*
生成过滤器，并将其置入与接口上的输入或输出方向关联的网络中，输入或输出方向由接口编号指定。缺省情况下，生成的过滤器没有附加过滤器-列表，缺省操作是 INCLUDE，并且处于 ENABLED 状态。

Default

使用 **default** 命令，将指定了过滤器编号的过滤器的缺省操作设置为 exclude、include 或 tag。

语法:

default exclude *filter-number*

include *filter-number*

tag *tag-number filter-number*

exclude *filter-number*
将指定有过滤器编号的过滤器的缺省操作设置为 exclude。

include *filter-number*
将指定有过滤器编号的过滤器的缺省操作指定为 include。

tag *tag-number filter-number*
将指定有过滤器编号的过滤器的缺省操作指定为 TAG，并且，将相关连的标记值设置成标记编号。

Delete

使用 **delete** 命令，删除与过滤器-列表相关的所有信息，并且释放已分配的字符串作为新建过滤器-列表名称的字符串。如果过滤器-列表是附加到用户已创建的过滤器，则此命令将在控制台上显示出错消息，但不删除任何信息。此外，此命令还删除属于该列表的所有过滤器-项。

同时，此命令删除使用 **create filter** 命令生成的过滤器。

语法:

delete list *filter-list*
filter *filter-number*

list *filter-list*
删除与过滤器-列表相关的全部信息，并且，释放已分配的字符串作为新建过滤器-列表名称的字符串。此过滤器-列表必须是由先前的 **create list** 命令输入的一个字符串。

如果过滤器-列表是附加到用户已创建的过滤器上，则此命令在控制台上显示出错消息，而不将任何信息删除。使用此命令时，将删除属于该列表的所有过滤器-项。

filter *filter-number*
删除由 **create filter** 命令生成的过滤器。

Detach

使用 **detach** 命令，从过滤器(过滤器-编号参数)中删除过滤器-列表名称(过滤器-列表参数)。

语法:

detach *filter-list-name filter-number*

Disable

使用 **disable** 命令，禁用整个 MAC 过滤系统或禁用一特定的过滤器。

语法:

disable all
filter *filter-number*

all 禁用整个 MAC 过滤系统。然而，以前启用的过滤器则仍设置为 ENABLED。

filter *filter-number*
禁用一特定的过滤器。过滤器-编号参数与在 **list filters** 命令中显示的数值相对应。

Enable

使用 **enable** 命令启用整个 MAC 过滤系统或启用一特定的过滤器。

语法:

enable all

filter *filter-number*

all 启用整个 MAC 过滤系统，尽管过滤器本身可能仍被设置成 DISABLED。

filter *filter-number*
启用特定的过滤器。过滤器-编号参数与在 **list filters** 命令中显示的数值相对应。

List

使用 **list** 命令列出关于所有过滤器-列表和由用户配置的过滤器的摘要。但是附加到一个过滤器的所有过滤器-列表的列表并未给出。显示的其它信息包括:

- 含有过滤系统状态 (ENABLE、DISABLE) 信息的列表
- 一组已配置的过滤器-列表记录
- 每个已配置的过滤器记录

此外，还显示出每个过滤器的下列信息:

- 过滤器编号
- 接口编号
- 过滤器方向 (NPUT、OUTPUT)
- 过滤器状态 (ENABLE、DISABLE)
- 过滤器缺省操作 (TAG、INCLUDE、EXCLUDE)。

该命令还为此过滤器所附的过滤器-列表及该过滤器的全部后续信息生成一个列表。

语法:

list all

filter *filter-number*

all 显示出所有已配置的过滤器-列表和过滤器的摘要。

filter *filter-number*
为指定过滤器所附的过滤器-列表和该过滤器的全部后续信息生成一个列表。

Move

使用 **move** 命令，将附加到指定过滤器的过滤器-列表(由过滤器-编号参数指定)重新排序。 Filter-list-name1 指定的列表移到 Filter-list-name2 指定的列表的紧前面。

语法:

move *filter-list-name1 filter-list-name2 filter-number*

Reinit

使用 **reinit** 命令，以更新的配置为基础重新初始化整个 MAC 过滤系统，而不影响路由器的其它部分。

语法:

reinit

Set-Cache

使用 **set-cache** 命令，将缺省高速缓冲存储区的大小 (16) 改为 4 到 32768 之间的数目。

语法:

set-cache *cache-size filter-number*

Update

使用 **update** 命令，向特定的过滤器-列表添加信息或从中删除信息。与所需的过滤器-列表-名称一起使用此命令，可使您进入特定过滤器-列表的 `Filter filter-list-name Config>` 提示符下。然后，您可在此新的提示符下更改指定列表中的信息。

新提示符级用来向过滤器-列表添加过滤器-项或从中删除过滤器-项。为给定过滤器-列表指定过滤器-项的顺序是很重要的，因为它决定了将过滤器-项应用到信息包的顺序。

语法:

update *filter-list-name*

更新子命令

本节概述 MAC 过滤的配置子命令。在 `Filter filter-list-name config>` 提示符下输入这些子命令。

表 6. 更新子命令概述

子命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	添加源或目标 MAC 地址过滤器或窗口过滤器。向过滤器-列表添加过滤器-项。
Delete	从过滤器-列表中删除过滤器-项。
List	列出所有过滤器-列表和由用户配置的过滤器的摘要。同时，对此过滤器所附的过滤器-列表及该过滤器的全部后续信息生成一个列表。
Move	将指定过滤器后所附的过滤器-列表重新排序。
Set-Action	设置过滤器-项以估计 INCLUDE、EXCLUDE 或 TAG (带有标记-编号选项)的状态。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

使用下列子命令以更新过滤器-列表。

Add

使用 **add** 子命令，向过滤器-列表添加过滤项。此子命令使您能添加十六进制的数值，以同源或目标 MAC 地址作比较，或添加带有掩码的窗口数据序列，以同信息包数据作比较。

向指定过滤器-列表添加过滤器-项的顺序是很重要的，因为它决定了将过滤器-项应用到信息包的顺序。

每次使用 **add** 子命令，都在过滤器-列表中生成一个过滤器-项。生成的第一个过滤器-项的过滤器项指定为第 1 号，将第二个指定为第 2 号，余下依次类推。您成功地输入 **add** 子命令之后，设备显示出刚刚添加的过滤器-项的编号。

首次发生的匹配终止过滤器-项的应用，并且，根据过滤器-列表的指定操作，过滤器-列表将估计 INCLUDE、EXCLUDE 或 TAG。如果过滤器-列表的过滤器-项都不产生匹配，则返回过滤器的缺省操作 (INCLUDE、EXCLUDE 或 TAG)。

语法: **add** source *hex-MAC-addr hex-Mask*

destination *hex-MAC-addr hex-Mask*

window MAC *offset-value hex-data hex-mask*

window INFO *offset-value hex-data hex-mask*

source *hex-MAC-addr hex-Mask*

添加十六进制的数值，以同源 MAC 地址作比较。 ***hex-MAC-addr*** 必须是十六进制偶数位的数，最多由 16 位数组成，前面不应加上 0x。

hex-mask 参数长度必须与 hex-MAC-address 长度相等，并且，同信息包中的指定 MAC 地址进行逻辑“与”。缺省的 hex-mask 自变量全为二进制 1。

hex-MAC-addr 参数可按规范的或非规范的位次序指定。规范位的次序可指定为十六进制的数值(例如，000003001234)。也可由在每两位数之间加有连字符 (-) 的一系列十六进制数来表示 (例如，00-00-03-00-12-34)。

非规范的位次序可指定为每两位之间有冒号 (:) 的一系列十六进制数(例如 00:00:C9:09:66:49)。过滤器项的 MAC 地址总是使用连字符 (-) 或冒号 (:) 来显示，以区分其是规范的还是非规范表示法。

destination *hex-MAC-addr hex-Mask*

与 add source 子命令作用相同，所不同的只是同信息包中的目标 MAC 地址作进行匹配，而不是同源 MAC 地址进行匹配。

window MAC *offset-value hex-data hex-mask*

使用指定偏移量(从帧的开始部分计算)得到添加滑动窗口过滤器项，它将带有掩码的十六进制数据与信息包数据相匹配。

window INFO *offset-value hex-data hex-mask*

类似于 **add window mac** 命令，所不同的是偏移量是按信息字段的开始部分计算的。

Delete

使用 **delete** 子命令可从过滤器-列表中删除过滤器-项。通过将过滤器-项-编号指定为添加该项时所分配的编号，即可删除过滤器-项。

当使用 **delete** 子命令时，编号序列中生成的任何间隔都被填充。例如，如果将过滤器-项 1、2、3、4 中的 3 删除，则过滤器-项 4 自动重新编号为 3。

语法:

delete *filter-item-number*

List

使用 **list** 子命令可列出所有过滤器-项记录的列表。以下有关每个 MAC 地址过滤器-项的信息将显示出来:

- 规范或非规范形式的 MAC 地址和地址掩码。
- 过滤器-项编号
- 地址类型(源或目标)
- 过滤器-列表操作

语法:

list canonical

noncanonical

mac-address canonical

mac-address noncanonical

window

canonical

列出过滤器-列表内的所有过滤器-项记录的清单，清单中给出项的编号、地址类型 (SRC、DST)、规范形式的 MAC 地址及规范形式的地址掩码。同时给出过滤器-列表的操作。

mac-address canonical

列出过滤器-列表内的过滤器-项记录的清单，清单中给出项的编号、地址类型 (SRC、DST) 和规范形式的 MAC 地址及规范形式的地址掩码。此外，还给出过滤器-列表的操作。

noncanonical

列出过滤器-列表内的过滤器-项记录的清单，清单中给出项的编号、地址类型 (SRC、DST)、非规范形式的 MAC 地址及非规范形式的地址掩码。同时指定过滤器-列表的操作。

mac-address noncanonical

列出过滤器-列表内的过滤器-项记录的清单，清单中给出项的编号、地址类型 (SRC、DST)、非规范形式的 MAC 地址及非规范形式的地址掩码。同时给出过滤器-列表的操作。

window

列出过滤器-列表内所有滑动窗口过滤器-项记录的清单，清单中给出项的编号、基数、偏移量、数据和掩码。同时给出过滤器-列表的操作。

Move

move 子命令将过滤器-列表内的过滤器-项重新排序。编号指定为 *filter-item-name1* 的过滤器-项将被重新编号并移动到 *filter-item-name2* 的紧前面。

语法:

move *filter-item-name1 filter-item-name2*

Set-Action

set-action 子命令允许您设置过滤器-项以估计 INCLUDE、EXCLUDE 或 TAG (带有 tag-number 选项)状态。如果过滤器-列表内有一过滤器-项与要过滤的信息包中的内容相匹配，则过滤器-列表将估计到指定的条件。缺省设置是 INCLUDE。

语法:

set-action [INCLUDE or EXCLUDE or TAG] *tag-number*

访问 MAC 过滤监控提示符

自 GWCON 进程使用 **feature** 命令，存取 MAC 过滤监控命令。**feature** 命令允许您在协议和网络接口的监控进程之外，存取特定设备功能的监控命令。

在 **feature** 命令后输入一个问号，获取一个您的软件发行版可用的功能列表。例如:

```
+ feature ?
WRS
BRS
MCF
```

为进入 MAC 过滤监控提示符，输入 **feature** 命令，在命令后加上功能部件编号 (3) 或名称缩写 (MCF)。例如:

```
+ feature mcf
MAC Filtering user monitoring
Filter>
```

进入 MAC 过滤监控提示符后，您可以开始输入特定的监控命令。如果要在任何时侯返回到 GWCON 提示符下，请在 MAC 过滤监控提示符下输入 **exit** 命令。

MAC 过滤监控命令

本节概述 MAC 过滤监控命令。请在 `Filter>` 提示符下输入这些命令。

表 7. MAC 过滤监控命令概述

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Clear	清除在 list filter 命令下列出的"按每个过滤器"的统计信息。
Disable	全局禁用 MAC 过滤或"按每个过滤器" 禁用 MAC 过滤。
Enable	全局启用或"按每个过滤器"启用 MAC 过滤。
List	列出当前在路由器中运行的各过滤器统计信息及设置情况的概要。
Reinit	按更新配置重新初始化整个 MAC 过滤系统，而不影响路由器的其它部分。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

使用以下命令以监控 MAC 过滤功能。

Clear

使用 **clear** 命令，清除过滤器的统计信息。

语法:

clear all

filter *filter-number*

all 清除由 **list all** 命令列出的统计信息。

filter *filter-number*
清除由 **list filter** 命令列出的统计信息。

Disable

使用 **disable** 命令，全局禁用 MAC 过滤系统。此命令并不单独禁用某个过滤器。

此命令也能禁用由过滤器-编号所指定的过滤器。禁用此过滤器并不修改配置记录。如果没有指定自变量，则全局禁用 MAC 过滤。

语法:

disable all

filter *filter-number*

all 全局禁用 MAC 过滤。此命令并不单独禁用某个过滤器。

filter ***filter-number***
禁用由过滤器编号指定的过滤器。禁用此过滤器并不修改配置记录。如果没有指定过滤器编号，则全局禁用 MAC 过滤。

Enable

使用 **enable** 命令，全局启用 MAC 过滤。此命令并不单独启用某个过滤器。

此命令同时启用由过滤器-编号所指定的过滤器。启用此过滤器并不修改配置记录。如果没有指定自变量，则全局启用 MAC 过滤。

语法:

enable all

filter *filter-number*

all 全局启用 MAC 过滤。此命令并不单独启用某个过滤器。

filter *filter-number*
启用由过滤器编号指定的过滤器。启用此过滤器并不修改配置记录。如果没有指定过滤器编号，则全局启用 MAC 过滤。

List

使用 **list** 命令，列出当前设备中运行的各过滤器统计信息及设置情况，使用**list all** 命令时显示的每个过滤器的以下信息:

- 缺省操作
- 高速缓冲存储区的大小
- 缺省标签
- 状态(启用/禁用)
- 作为 INCLUDE、EXCLUDE 或 TAG 而过滤的信息包数目。

此外，**list filter** 命令还对指定过滤器显示出下列信息:

- list all 命令显示出的全部信息
- 当前在此过滤器中运行的全部过滤器-列表，包括:
  - 列表名称
  - 列表操作
  - 列表标签
  - 已由各过滤器-列表过滤的信息包数目

语法:

list all

filter *filter-number*

all 列出当前在路由器中运行的各过滤器统计信息和设置情况。

filter *filter-number*
生成各过滤器的统计信息和设置情况，及当前在该过滤器中运行的过滤器-列表。

Reinit

使用 **reinit** 命令，按更新配置重新初始化整个 MAC 过滤系统，而不影响路由器的其它部分。

语法:

reinit

第5章 使用 WAN 恢复

本章节包括以下部分:

WAN 恢复、WAN 重新路由和拨号溢出

WAN 恢复、WAN 重新路由和拨号溢出功能部件具有类似的功能，彼此之间可能会引起混淆。本概述旨在帮助您确定哪些功能是对您有用的，并帮助您查找配置这些功能所需的信息。

有关这三个功能部件的配置命令，请参阅“配置 WAN 恢复”一章。有关 WAN 重新路由和拨号溢出的详细信息，请参阅第75页的『第7章 WAN 重新路由功能』。

WAN 恢复

WAN 恢复是最基本的功能。当使用 WAN 恢复时，您已配置一条主链路和一条辅助链路。如果主链路失效，则接通辅助链路，此辅助链路具备主链路的所有特性。因为辅助链路使用了主链路的协议定义，所以您不必在辅助链路上配置任何协议定义。

对于 WAN 恢复:

- 主链路和辅助链路之间是配对的。
- 对于一条主链路，您仅可配置使用一条特定的辅助链路。
- 您不必在辅助链路上配置协议定义(例如: 协议地址)。
- 主链路可能是 PPP 串行接口或多链路的 PPP 接口。但不可能是 PPP 拨号线路接口。
- 辅助链路必须是 PPP 拨号线路或多链路的 PPP 接口。
- 必须使用 **enable wrs** 命令启用 WRS 功能。
- 必须使用 **enable secondary-circuit** 命令启用主/辅链路对。

注: 当在主链路上配置了 BRS，且主链路是 WAN 恢复的主/辅链路对的一部分时，您必须在辅助链路上配置 BRS。典型情况下，在配置了 WAN 恢复后，辅助链路即获得主链路的标识。但对于 BRS 则并非如此；因此，在主辅链路上都需要配置 BRS。

WAN 重新路由

WAN 重新路由是更高级的功能。当您使用 WAN 重新路由时，您需配置一条主链路和一条备用链路。如果主链路失效，则可接通备用链路。路由选择协议(例如 RIP 或 OSPF)检测新的可用的链路，并调整用于转发信息包的路由。

对于 WAN 重新路由:

- 主链路和备用链路之间是配对的。
- 您可配置多条主链路使用相同的备用链路。
- 在备用链路上，您必须配置协议定义。
- 主链路可以是可在该链路上配置路由选择协议(例如 IP 或 IPX) 的链路。例如，主链路可以是 LAN 接口、或 PPP、或帧中继、或 X.25 串行接口，或者是 PPP 或帧中继拨号线路。下面实例中的接口类型不能是主链路：SDLC 串行接口、SRLY 串行接口和类似 V.25bis 及 ISDN 的基网络。
- 备用链路可以是可在该链路上配置路由选择协议(例如 IP 或 IPX)的任何链路，并且，备用链路的数据链路类型不必与主链路的数据链路类型相匹配。例如，备用链路可以是 LAN 接口、PPP、帧中继或 X.25 串行接口，或者是 PPP 或帧中继拨号线路。下面实例中的接口类型不能是备用链路：SDLC 串行接口、SRLY 串行接口及类似 V.25bis 和 ISDN 的基网络。
- 如果主链路是拨号线路，则其不可能是按需拨入拨号线路(您必须在拨号线路上配置 'set idle 0')。由于 I.430、I.431 和信道化的 T1/E1 拨号线路是隐式安装的，因此可将其用做 WRS 主链路。

  注: 无须任何明确配置，即可将 I.430/I.431 和已信道化的 T1/E1 拨号线路用作 WRS 主链路。
- 备用链路可能不是按需拨入拨号线路(您必须在拨号线路上配置 'set idle 0')。
- 您必须使用 **enable wrs** 命令，以启用 WRS 功能。
- 您必须使用 **enable alternate-circuit** 命令，以启用主/备用链路对。
- 您可有选择地配置稳定化次数和 start-and stop-time-of-day-revert-back 次数，以控制向主链路的转换。
- 如果备用链路是 X.25，则当配置路由器(启用了 WAN 重新路由)的 X.25 接口时，请使用 **national-personality set disconnect-procedure active** 命令，并且，当在另一个路由器上配置 X.25 接口时，请使用 **national-personality set disconnect-procedure passive** 命令。

拨号溢出

拨号溢出类似于 WAN 重新路由，但不是必须在主链路失效时才能接通备用链路。相反，它对主链路的使用率进行监控，如果超过了阈值，就接通备用链路。此外，不同的是，不是在备用链路上应用所有的协议，而仅应用 IP 协议，其它的协议继续使用主链路，除非将主链路断开。

如果断开了主链路，则启动 WAN 重新路由，并且在备用接口上配置的任何协议都可开始检测和使用备用接口上的路由。

对于拨号溢出:

- 拨号溢出使用 WAN 重新路由配对的主/备用链路对。
- 您必须配置 WAN 重新路由配对以使用拨号溢出，所有 WAN 重新路由配置的限制都适用。
- 将为拨号溢出而使用的 WAN 重新路由配对的主链路，必须是帧中继。
- 您必须使用 OSPF 路由选择协议以使用拨号溢出。
- 您必须使用 **enable dial-on-overflow** 命令，以配置添加阈值、丢弃阈值、带宽监控间隔及备用链路最低连通时间。

- 稳定时间和 start-time-of-day-revert-back 及 stop-time-of-day-revert-back 的次数并不影响拨号溢出的操作。

有关 WAN 重新路由的信息，请参阅 第75页的『第7章 WAN 重新路由功能』。

开始配置前

在开始配置 WAN 恢复之前，您必须做以下准备:

1. 为 PPP 而配置的主串行接口(租用线路)。在路由器上，您可使用任何串行接口。
2. 在路由器上配置的与相关拨号线路相连的接口。您可将 ISDN 接口或 V.25bis 接口用做基网络。
3. 当主接口断开时可以拨入的已配置辅助拨号线路。为配置拨入的拨号线路，将空闲定时器设置为 0，并可在拨号 Circuit Config> 提示符下，使用 **set idle** 命令。
4. 为仅发送呼叫而配置的链路的一端上的辅助拨号线路。请在 Circuit Config> 提示符下，使用 **set calls outbound** 命令。

   注: 请不要在辅助接口上配置任何协议地址。辅助链路(拨号线路)在处于活动状态时，在辅助链路上使用主接口的协议赋值。
5. 为仅接受呼叫而配置的链路的另一端上的辅助拨号线路。请在 Circuit Config> 提示符下使用 **set calls inbound** 命令。

WAN 恢复的配置过程

本节说明配置 WAN 恢复所需的步骤。在您开始配置之前，请在 Config> 提示符下，使用 **list device** 命令，以列出不同设备的接口号。

按以下步骤，在路由器上配置 WAN 恢复:

1. 在 Config> 提示符下，输入 **feature wrs** 命令，以显示 WRS Config> 提示符。例如:

```
Config>feature wrs
WAN Restoral user configuration
WRS Config>
```

2. 向主接口指定辅助拨号线路。此拨号线路将备份主接口。例如:

```
     WRS
Config>add secondary-circuit
     Secondary interface number  [0]? 3
     Primary interface number  [0]? 1
```

3. 在您添加的辅助拨号线路上启用 WAN 恢复。例如:

```
WRS Config>enable secondary-circuit
Secondary interface number  [0]? 3
```

4. 在路由器上全局启用 WAN 恢复。例如:

```
WRS Config>enable wrs
```

5. 重启路由器以使更改的配置生效。

辅助拨号线路配置

为配置拨号线路:

1. 确定拨号线路接口编号，为此，请输入:

   ```
   Config> list device
   ```

   如果没有列出 PPP 拨号线路接口，则添加拨号线路接口，请输入:

   ```
   Config> add device dial-circuit

   Adding device as interface 3
   Defaulting Data-link protocol to PPP
   Use "net 3" command to configure circuit parameters
   ```

2. 在 Config> 提示符下配置辅助电路(拨号线路)，使其拥有与主接口 (PPP) 相同的数据链路类型，如下所示:

   ```
   Config> set data PPP
   Interface Number [0]? 3
   ```

3. 请输入 **network** *interface#*，存取拨号线路配置提示符 (Circuit Config>)。

   ```
   Config> network 3
   ```

4. 为拨号线路选择基网络接口。基网络可以是 V.25bis、或 ISDN.

   ```
   Circuit Config> set net 2
   ```

5. 将拨号线路空闲定时器设置为 0 (0=固定)，如下所示:

   ```
   Circuit Config> set idle 0
   ```

6. 将备份连接的一端(如路由器 A) 设置为接收呼叫，如下所示:

   ```
   Circuit Config> set calls inbound
   ```

7. 将备份连接的另一端设置为启动呼叫(例如，路由器 B)，如下所示:

   ```
   Circuit Config> set calls outbound
   ```

注:

1. 请不要使用 **set calls both** 命令。逐一设置这些呼叫，可有助于防止入网和出网连接冲突。
2. 请不要在拨号线路上配置转发器(例如 IP 或 IPX 等)地址。当辅助接口(拨号线路)处于活动状态时，在辅助接口上使用主接口的协议赋值。
3. 有关 ISDN 配置说明，请参阅*Access Integration Services 软件用户指南*中的‘使用 ISDN 接口’。
4. 有关 V.25bis 配置说明，请参阅*Access Integration Services 软件用户指南*中的 ‘使用 V.25bis 接口’。

第6章 配置和监控 WAN 恢复

本章说明 WAN 恢复配置和可操作的命令。包括以下部分:

WAN 恢复、WAN 重新路由和拨号溢出配置命令

WAN 恢复配置命令允许您创建或修改 WAN 恢复的接口配置。本节概述和说明了 WAN 恢复配置命令。

表8列出了 WAN 恢复配置命令和这些命令的功能。在 WRS Config> 提示符下输入这些命令。要进入 WRS Config>, 请在 Config> 提示符下输入 **feature wrs**。

表 8. WAN 恢复配置命令概述

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	添加主-到-辅的映射(对于 WAN 恢复) 或主-到-备用的映射(对于 WAN 重新路由)。
Disable	禁用 WRS、禁用个别的辅助链路映射或备用链路映射。
Enable	启用 WRS、启用个别的辅助链路映射或备用链路映射。
List	显示当前恢复配置。
Remove	删除由添加命令生成的主链路到辅链路或主链路到备用链路的映射。
Set	设置稳定数值和设置 time-of-day-revert-back 计数器。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add

使用 **add** 命令，为主串行链路标识辅助拨号线路、备用拨号线路或租借链路的接口。

语法:

add alternate-circuit

secondary-circuit

alternate-circuit

add alternate-circuit 命令将备用接口连接到主接口以用于 WAN 重新路由。对于一个备用接口，您可指定多个主接口。备用链接类型不必与主链接类型相同(例如，备用链接类型可以是 PPP 拨号线路，而主链接类型则可以是帧中继租借线路)。

例如:

```
WRS
Config>add alt
Alternate interface number  [0]? 6
Primary interface number  [0]? 1
```

Alternate interface number

这是预先指定到备用接口的接口编号。任何 LAN 接口、PPP 接口、帧中继接口或 X.25 串行接口，或者任何 PPP 或帧中继拨号线路都是合法的备用接口。缺省值是 0。

Primary interface number

这是主接口的接口编号，是在添加设备时预先指定的。主接口可以是任何预先定义的 LAN 接口、PPP 帧中继或 X.25 串行接口，或者是任何预先定义的 PPP 或帧中继拨号线路。缺省值是 0。

secondary-circuit

add secondary-circuit 命令将辅助接口连接到主接口以用于 WAN 恢复。这两个接口必须是预先配置的。您仅可向主接口指定一个辅助接口，而对于一辅助接口，您也仅可指定一主接口。

例如:

```
WRS Config>add secondary-circuit
Secondary interface number  [0]? 4
Primary interface number  [0]? 1
```

Secondary interface number

这是在添加设备时预先指定到辅助接口上的拨号线路接口号。任何 PPP 拨号线路或多链路 PPP 接口都可以是辅助接口。缺省值是 0。

Primary interface number

这是一个主接口的接口编号，是在添加设备时预先指定的。主接口可以是任何预先定义的运行 PPP 的租借线路。缺省值是 0。

Disable

使用 **disable** 命令，禁用 WAN 恢复功能，或者禁用 WAN 恢复的主/备用链路对，或者禁用 WAN 重新路由的主/备用链路对，或者禁用主/备用链路对的拨号溢出。

语法:

disable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit *interface#*

禁用 WAN 重新路由的主/备用链路对。

例如:

```
WRS Config> disable alternate-circuit
Alternate interface number  [0]? 6
```

Alternate interface number

这是备用接口的编号，该接口是使用 **add alternate-circuit** 命令预先配置的。缺省值是 0。

dial-on-overflow *alt-intfc#*

禁用用于所有主/备用链路对(使用一指定的备用接口)的拨号溢出。

例如:

```
WRS Config>
disable dial-on-overflow
alternate interface number  [0]? 6
```

Alternate interface number

这是备用接口的编号，该接口是使用 **add alternate-circuit** 命令预先配置的。缺省值是 0。

secondary-circuit*interface#*

通过相关的备用接口禁用特定主接口的恢复，直到在 WRS 控制台上使用了下一条 **enable secondary-circuit** 命令时为止。在 WRS 配置中，这两个接口必须是预先配置且是绑定在一起的。

例如:

```
WRS Config> disable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

这是辅助接口的编号，该接口是使用 **add secondary-circuit** 命令预先配置的辅助接口的编号。缺省值是 0。

wrs 全局禁用路由器上的 WAN 恢复功能。这表示同时禁用了 WAN 重新路由和拨号溢出。

Enable

使用 **enable** 命令，启用 WAN 恢复功能，启用 WAN 恢复的主/辅链路对，启用 WAN 重新路由的主/备用链路对，或者，启用主/备用链路对的拨号溢出。

语法:

enable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit*interface#*

启用备用链路

例如:

```
WRS Config>enable alternate-circuit
Alternate interface number  [0]? 6
```

Alternate interface number

这是备用接口的编号，该接口是使用 **add alternate-circuit** 命令预先配置的。缺省值是 0。

dial-on-overflow

启用拨号溢出，并允许您设置可控制拨号溢出操作的参数。

例如:

```
WRS>enable dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate
interface.
Primary interface number  ]0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!
```

Primary interface number

这是一个主接口的接口编号，对于此主接口，您正在启用 dial-on-overflow。缺省值是 0。

add-threshold

确定何时为附加带宽接通备用接口。此数值必须是以主接口的已配置线路速度的百分比来表示。缺省值是 90%。

drop-threshold

确定何时附加带宽不再需要备用接口。此数值必须是以主接口的已配置线路速度的百分比来表示。缺省值是 60%。

bandwidth monitoring interval

为使用参数 *add-threshold* 和 *drop-threshold*，确定主接口的带宽的监控频率。缺省值是 15 秒。

Minimum time to keep alternate up

当本地路由器上的 IP 通信重新路由到备用接口时，能够允许路由器建立新路由的时间周期。缺省值是 5 分钟。

secondary-circuit*interface#*

通过所指示的辅助链路，启用主链路的恢复。

例如:

```
WRS Config>enable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

这是辅助接口的编号，该接口是使用 **add secondary-circuit** 命令预先配置的。缺省值是 0。

wrs 启用路由器上的 WAN 恢复功能部件的功能。这表示如果配置了 WAN 重新路由和拨号溢出，则它们也同时启用。

List

使用 **list** 命令，显示功能部件的全局配置信息，并且显示 WAN 恢复的主-辅配对和 WAN 重新路由的主-备用配对及拨号溢出。

语法:

list

例如:

```
WRS Config>list
WAN Restoral is enabled.
Default Stabilization Time:       0 seconds
Default First Stabilization Time: 0 seconds

                                                 Secondary
   Primary Interface       Secondary Interface   Enabled
----------------------  ----------------------  --------
 4 - WAN PPP             7 - PPP Dial Circuit       No
                                        Alt.     1st  Subseq TOD Revert Back
Primary Interface  Alternate Interface     Enabled  Stab  Stab  Start    Stop
-----------------  ----------------------  -------  ----  ----  -------  -------

 1 - WAN Frame Re   2 - WAN Frame Relay      Yes    dflt  dflt  Not Set  Not Set


Dial-on-overflow is enabled.
Primary    add-       drop-      test       minimum
Interface  threshold  threshold  interval   alt up time
---------  ---------  ---------  ---------  -----------
     1         29%        20%      15 sec.   300 sec.
```

Remove

使用 **remove** 命令，删除映射到主接口的备用接口或辅助(备份)接口的映射。

语法:

remove alternate-circuit

secondary-circuit

alternate-circuit*alternate-interface# primary-interface#*

将备用(备份)接口到 WAN 重新路由主接口的映射删除。两个接口必须进行了预先指定，且是使用了 **add alternate-circuit** 命令绑定的。

Alternate-interface#

这是备用接口的编号，该接口是使用 **add alternate-circuit** 命令预先配置的。缺省值是 0。

Primary-interface#

这是预先绑定到备用接口(正被删除)的主接口的接口编号。缺省值是 0。

例如:

```
WRS Config>
remove alternate-circuit
Alternate interface number  [0]? 3
Primary interface number  [0]? 1
```

secondary-circuit*secondary-interface# primary-interface#*

将到 WAN 重新路由主接口的辅助(备份)接口映射删除。必须对两个接口进行了预先指定，并且是使用了 **add secondary-circuit** 命令将二者绑定起来的。

Secondary-interface#

这是辅助接口的编号，该接口是使用 **add secondary-circuit** 命令预先配置的。缺省值是 0。

Primary-interface#

这是预先绑定到辅助接口(正被删除)的主接口的接口编号。缺省值是 0。

例如:

```
WRS Config>
remove secondary-circuit
Secondary interface number  [0]? 3
Primary interface number  [0]? 1
```

Set

使用 **set** 命令，设置 WAN 重新路由的参数。

语法:

set ? default

first-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

default

使用 **set default** 命令，设置缺省值，该缺省值为未配置有稳定和首次-稳定时间的链路所使用。

first-stabilization

设置缺省的首次-稳定数值，以用于未配置有首次-稳定时间的链路。

```
WRS
Config>set default first
Default first primary stabilization time (0 - 3600 seconds)  [0]?
20
```

stabilization

设置缺省的稳定数值，以用于未配置有稳定时间的链路。

```
WRS
Config>set default stab
 Default primary stabilization time (0 - 3600 seconds)  [0]?
30
```

first-stabilization

设置主链路路由切换到备用链路(如果主链路没能连通)前，路由器初始化所需的秒数。

例如:

```
WRS
Config>set first
Primary interface number  [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

这是主接口的主接口编号，您正在对此主接口设置首次-稳定。缺省值是 0。

First primary stabilization time

此主接口的稳定时间。缺省值是 1。

stabilization

设置在主链路首次检测为连通后，路由选择切换到主链路之前，系统所要求的等待秒数。如果主链路在规定秒数后仍然保持连通，则停止在备用链路上继续进行路由选择。

例如:

```
WRS
Config>set first
Primary interface number  [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

这是主接口的主接口编号，您正在对此主接口设置稳定参数。缺省值是 0。

Primary stabilization time

主接口的稳定时间。缺省值是 1。

start-time-of-day-revert-back

一天内路由器能转换到主路由的最早时间。路由器可在 start-time-of-day-revert-back 与 stop-time-of-day-revert-back 之间的任何时间内返回到主接口。仅当主接口接通且满足稳定参数时，才还原到主接口。缺省值是 0。

例如:

```
WRS Config>set start
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]
3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

这是主接口的主接口编号，您正在对此主接口设置首次-稳定。缺省值是 0。

Time-of-day-revert-back-window start

该时间标出返回窗口的起始时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时间返回主接口。仅当主接口连通且满足稳定参数时，才可返回到主接口。缺省值是 1。

stop-time-of-day-revert-back

该时间标出返回窗口的结束时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时间返回主接口。仅当主接口接通且满足稳定参数时，才可返回主接口。缺省值是 1。

例如:

```
WRS Config>set stop
Primary interface number  [0]? 1
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured)
[0]?5
```

Primary interface number

这是主接口的主接口编号，您正在对此主接口设置首次-稳定。缺省值是 0。

Time-of-day-revert-back-window stop

该时间标出返回窗口的结束时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时间返回主接口。仅当主接口连通且满足稳定参数时，才可返回到主接口。缺省值是 1。

访问 WAN 恢复接口监控进程

如果要访问 WAN 恢复接口监控进程，请在 GWCON (+) 提示符下输入下列命令:

```
   +
feature wrs
```

WAN 恢复监控命令

WAN 恢复 (WRS) 监控命令允许您监控 WAN 恢复主-辅链路对、WAN 重新路由主-备用链路对及拨号溢出的状态。任何通过监控接口而对 WAN 恢复、WAN 重新路由、拨号溢出可操作状态所做的修改，将不在路由器重启时得到维护。

在 GWCON (+) 提示符下，输入 **feature wrs** 命令，进入 WRS 提示符。第66页的表9 中列出了 WRS 命令及其功能，下列各节对这些命令做出了说明。

表 9. WAN 恢复监控命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Clear	清除使用 **list** 命令所显示的监控统计信息。
Disable	禁用 WRS、单独的辅助接口或备用接口，或者禁用拨号溢出。
Enable	启用 WRS、单独的辅助接口或备用接口，或者启用拨号溢出。
List	显示一条或所有的备用或辅助链路上的监控信息。
Set	设置稳定数值和时间-天-返回定时器。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Clear

使用 **clear** 命令，清除使用 **list** 命令所显示的 WAN 恢复、WAN 重新路由及拨号溢出的统计信息。

语法:

clear

注: 该命令清除*最长的恢复周期*，但是并不清除*最近的恢复周期*。关于屏幕所显示信息，请参阅 **list** 命令中的实例。

Disable

使用 **disable** 命令，完全禁用 WAN 恢复功能部件、通过相关的辅助接口禁用特定的主接口、禁用备用接口或禁用拨号溢出。

语法:

disable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit

禁用 WAN 重新路由的主/备用链路。可能有使用相同备用链路的多个链路对。此命令禁用使用指定备用链路的所有链路对。

例如:

```
WRS>disable alternate-circuit
Alternate circuit number  [0]? 6
```

Alternate circuit number

这是备用电路的编号。缺省值是 0。

dial-on-overflow

禁用指定主/备用链路对的拨号溢出，而无须更改配对的 WAN 重新路由的启用/禁用状态。如果 dial-on-overflow 是处于活动的路由选择状态，则在下一个监控间隔的截止期限内终止。

secondary-circuit

通过相关的辅助接口，禁用特定主接口的恢复，直到使用了下一条 **restart**、

reload 或 **enable secondary-circuit** 命令时为止。在 WRS 配置中，这两个接口必须是预先配置且是绑定在一起的。

正常情况下，在 **talk 5** (GWCON) 中，**disable** 命令使接口进入非活动状态并保持在非活动状态下。然而，对于 WAN 恢复辅助接口，情形并非如此。适用于辅助链路的 **disable** 命令并不禁用接口本身。该命令仅仅禁用当前的呼叫(即，中断任何活动的呼叫)。为了禁用辅助链路的使用，您需要在 WAN 恢复监控提示符下输入 **disable secondary-circuit** 命令，并且，禁用在顶层 GWCON 提示符下的辅助接口。**例如:**

```
WRS>disable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

这是辅助接口的编号，该接口是使用 **add secondary-circuit** 命令预先配置的。缺省值是 0。

wrs 通过禁用 WRS 可禁用路由器上的 WAN 恢复、WAN 重新路由及拨号溢出，直到使用了下一条 **restart**、**reload** 或 **enable WRS** 命令时为止。

Enable

使用 **enable** 命令，启用 WAN 恢复接口，通过辅助链路启用主链路恢复，启用备用链路或启用拨号溢出。

语法:

enable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit

对于所有使用指定备用接口的配对，启用 WAN 重新路由的主/备用链路对。

例如:

```
WRS>
enable alternate-circuit
Alternate circuit number  [0]? 3
```

Alternate circuit number

这是备用电路的接口编号。缺省值是 0。

dial-on-overflow

启用拨号溢出并允许您设置可控制拨号溢出的参数。您可以有选择地使 IP 协议立即切换到备用接口上，从而，好像是忽略了添加阈值。

例如:

```
WRS> dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate interface.
Primary interface number  [0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!

Do you want to switch IP traffic to the alternate now?(Yes or [No]):
WRS>
```

secondary-circuit

通过所指示的辅助链路，启用主链路。

例如:

```
WRS> enable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

这是使用 **add secondary-circuit** 命令预先配置的辅助接口的编号。缺省值是 0。

wrs 启用路由器上的 WAN 恢复功能部件的功能。需启用此功能部件，以进行 WAN 恢复、WAN 重新路由或拨号溢出。

Set

使用 **set** 命令，设置 WAN 重新路由的参数。

语法:

set ?

default

first-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

default

使用 **set default** 命令，设置未配置有稳定和首次-稳定时间的链路所要使用的缺省值。

例如:

```
WRS Config>set default ?
FIRST-STABILIZATION
STABILIZATION
```

first-stabilization

设置缺省的首次-稳定值，以用于未配置有首次-稳定时间的链路。

```
WRS
Config>set default first

Default first primary stabilization time (0 - 3600 seconds)  [0]?
20
```

stabilization

设置缺省的稳定数值，以用于未配置有稳定时间的链路。

```
WRS
Config>set default stab
Default primary stabilization time (0 - 3600 seconds)  [0]?
30
```

first-stabilization

设置路由器初始化所需的秒数，这一设置应在主链路的路由选择切换到备用链路(如果主链路尚未连通)之前进行。

例如:

```
WRS
Config>set first
Primary interface number  [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

这是主接口的主接口编号，您正在对此主接口设置 first-stabilization。缺省值是 0。

First primary stabilization time

主接口的稳定时间。缺省值是 1。

stabilization

设置在主链路首次检测为即将连通之后，但路由选择切换到主链路之前需要等待的秒数。如果主链路在这一秒数后仍保持连通，则系统停止在备用链路上继续进行路由选择。

例如:

```
WRS
Config>set first
Primary interface number  [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

这是主接口的主接口编号，您正在对此主接口设置 stabilization。缺省值是 0。

Primary stabilization time

主接口的稳定时间。缺省值是 1。

start-time-of-day-revert-back

一天内路由器能转换到主路由的最早时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时刻返回主接口。仅当主接口接通且满足 stabilization 参数时，才返回到主接口。缺省值是 0。

例如:

```
WRS Config>set start
Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]
3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

这是主接口的编号，您正在对此主接口设置 first-stabilization。缺省值是 0。

Time-of-day-revert-back-window start

该时间标出还原窗口的起始时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时间返回主接口。仅当主接口接通且满足 stabilization 参数时，才返回到主接口。缺省值是 1。

stop-time-of-day-revert-back

该时间标出返回窗口的结束时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时间返回主接口。仅当主接口接通且满足 stabilization 参数时，才返回到主接口。缺省值是 1。

例如:

```
WRS Config>set stop
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
5
```

Primary interface number

这是主接口的编号，您正在对此主接口设置 first-stabilization。缺省值是 0。

Time-of-day-revert-back-window stop

该时间标出返回窗口的结束时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任意时间返回主接口。仅当主接口接通且满足 stabilization 参数时，才返回到主接口。缺省值是 1。

List

使用 **list** 命令，显示有关一个或所有的 WAN 恢复主-辅配对的监控信息，或者，显示一个或所有的 WAN 重新路由主/备用链路对的监控信息。

语法:

list all

alternate-circuit

secondary-circuit

summary

all 提供摘要信息，此摘要信息之后是各辅助接口的特定信息。

例如:

```
list all
WAN Restoral/Re-route is enabled with 2 circuits configured
    Total restoral attempts =          7 completions   =          7
    Total packets forwarded =         39
    Longest completed restoral period in hrs:min:sec     0:03:27

    Total overflow attempts =         20 completions   =         19
    Longest completed overflow period in hrs:min:sec     0:05:00

   Primary       Secondary    Restoral  Restoral   Current/Longest
Net Interface  Net Interface  Enabled    Active       Duration
-------------  -------------  --------  --------   --------------------
  4  PPP/0       7  PPP/1       No         No       00:03:27/ 00.06.00

                               Re-route/ Re-route/         Recent
   Primary       Alternate    Overflow  Overflow     Reroute/Overflow
Net Interface  Net Interface  Enabled    Active          Duration
-------------  -------------  --------  --------   --------------------
  1   FR/0       2   FR/1     Yes/Yes    No /No     00:00:56/
00:05:00
```

Total restoral attempts

主链路失效时，路由器尝试接通辅助链路的次数。

Completions

当辅助链路活动并接通时成功进行恢复的尝试次数。

Total packets forwarded

通过辅助接口转发的信息包总数。这是在两个方向上转发的信息包总和，是在发出 restart 或 restoral-statistics 命令之前、对所有成功恢复所积累的信息包数量。

Longest Completed Restoral Period

此字段以小时、分钟、秒的格式，显示恢复操作的最长时间，不包括当前所占用的时间。

Total Overflow Attempts
溢出引起的尝试次数。

Completions
当辅助链路活动并接通时成功进行溢出尝试的次数。

Longest Completed Overflow Period
以小时、分钟、秒的格式，显示溢出操作的最长的时间，不包括当前所占用的时间。

Primary Net Interface
通过相关的辅助接口，进行备份的接口。

Secondary Net Interface
用于备份相关主接口的拨号线路。

Restoral Enabled
指示当前在启用此主接口的恢复。

Restoral Active
指示恢复是否是活动的 (Yes 或 No)。

Current/Longest Duration
以小时、分钟、秒的格式，指示辅助网络接口处于接通状态的当前和最长持续时间。

Primary Net Interface
通过相关的备用接口，进行备份的接口。

Alternate Net Interface
正被用作相关主接口的备用备份的接口。

Re-route/Overflow Enabled
指示是否启用重新路由和溢出 (Yes 或 No)。

Re-route/Overflow Active
指示重新路由和溢出是否是活动的 (Yes 或 No)。

Recent Re-route Overflow Duration
以小时、分钟、秒的格式，指示备用网络接口的最近重新路由和溢出的持续时间。

Alternate-circuit
提供备用链路总数。允许监控操作员检索各备用链路接口和相关主映射的 WAN 重新路由状态及相关的统计信息。

例如:

```
WRS>li alt 7
Primary    1:FR/0 Frame Relay V.35/V.36
Alternate  7:PPP/1 Point to Point V.25bis Dial Circuit
reroute Enabled, currently inactive
overflow Enabled, currently inactive
Primary first stabilization time: default (0 seconds)
Primary stabilization time: default (0 seconds)
Time-of-day revert back not configured: start = 0, stop = 0
Restored 0 times (0 attempts)
Overflow 0 times (0 attempts)
```

Primary Interface
正通过相关的备用接口备份的接口。

Alternate Interface

用于备份相关主接口的拨号电路。

Reroute Enabled

指示当前是否启用此主接口的重新路由。

Overflow Enabled

指示当前是否启用此主接口的溢出。

Primary first stabilization

在主链路的路由选择切换到备用链路(如果主链路尚未连通)前，路由器初始化所需的秒数。

First stabilization

主链路首次检测为即将连通之后，路由选择切换回主链路之前系统需要等待的秒数。继续在备用链路上进行路由选择，直到主链路在该秒数之后仍处于连通状态。

Time-of-day revert back

一天内路由器能转换到主路由的时间。路由器可在 start-time-of-day-revert-back 和 stop-time-of-day-revert-back 之间的任何时间返回主接口。仅当主接口接通且满足 stabilization 参数时，才返回到主接口。缺省值是 0。

Restored times

重新路由主接口的尝试次数。

Overflow times

dial-on-overflow 的尝试次数。

secondary-circuit

提供各辅助链路的总体信息。允许监控操作员检索各辅助链路和相关主映射的 WAN 恢复状态及相关的统计信息。

例如:

```
list secondary-circuit
Secondary interface number  [0]? 1

                                                    Secondary
Primary Interface          Secondary Interface      Enabled
-------------------        --------------------     ---------
1  PPP/0  Point to Poi     3  PPP/1  Point to Poi     Yes

Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:

  Primary restoral attempts =       6   completions =    5
  Restoral packets forwarded =    346
    Most recent restoral period in hrs:min:sec          00:08:20
```

Primary Interface

正在通过相关的辅助接口备份的接口。

Secondary Interface

用于备份相关主接口的拨号线路。

Secondary Enabled

指示当前是否在启用此主接口的恢复。

Router Primary Interface State

指示主接口的状态为下列选项之一:

接通 - 指示链路是接通的。

断开 - 指示链路是断开的。

禁用 - 指示操作员已禁用链路。

不存在 - 指示虽已配置了链路，但存在硬件问题。

Router Secondary Interface State

指示相关的辅助接口状态为下列选项之一:

接通 - 指示链路是接通的。

断开 - 指示链路是断开的。在 Config> 提示符下，或者在操作员控制台上，禁用辅助链路的基网络时也会发生这种情况。

可用 - 指示链路处于等待模式下。

测试 - 指示链路是在建立连接的进程中。

Restoral Statistics:

Primary Restoral Attempts

主链路失效时，接通辅助链路的尝试次数。

Restoral Packets forwarded

此字段指示所转发的信息包总数。

Most Recent Restoral Period

指示辅助链路处于接通的时间、最后一次使用的时间或在当前恢复中使用的时间。

summary

提供各辅助链路的总体信息。

例如:

```
list summary
WAN Restoral is enabled with 3 circuit(s) configured

  Total restoral attempts =      3 completions =      2
  Total packets forwarded =    346
  Longest restoral period in hrs:min:sec   00:08:20

Primary Interface and State      Secondary Interface and State
---------------------------   ----------------------------------
 1  PPP/0  - Up                 3  PPP/1  - Available
```

Total restoral attempts

主链路失效时，路由器接通辅助链路的尝试次数。

Completions

当辅助链路活动并接通时成功进行恢复的尝试次数。

Total packets forwarded

通过辅助接口转发的信息包总量。这是在两个方向上转发的信息包总数，是在使用 restart 和 clear restoral-statistics 命令之前，在所有的恢复周期内所积累的信息包数量。

Longest restoral period

此字段以小时、分钟、秒的格式，显示操作的最长时间，不包括当前所占用的时间。

Primary Interface and State

通过相关的辅助接口进行备份的接口。有效状态是:

接通 - 指示链路是接通的。

断开 - 指示链路是断开的。

禁用 - 指示操作员已禁用链路。

不存在 - 指示虽已配置了链路，但存在硬件问题。

Secondary Interface and State

用于备份相关主接口的拨号电路。有效状态是:

接通 - 指示链路是接通的。

断开 - 指示链路是断开的。在 Config> 提示符下，或者在操作员控制台上，禁用辅助链路的基网络时也会发生这种情况。

测试 - 指示链路是在建立连接的进程中。

可用 - 指示链路处于等待模式下。

第7章 WAN 重新路由功能

本章说明 WAN 重新路由功能。包括以下部分:

- 『WAN 重新路由概述』
- 第77页的『配置 WAN 重新路由』

WAN 重新路由概述

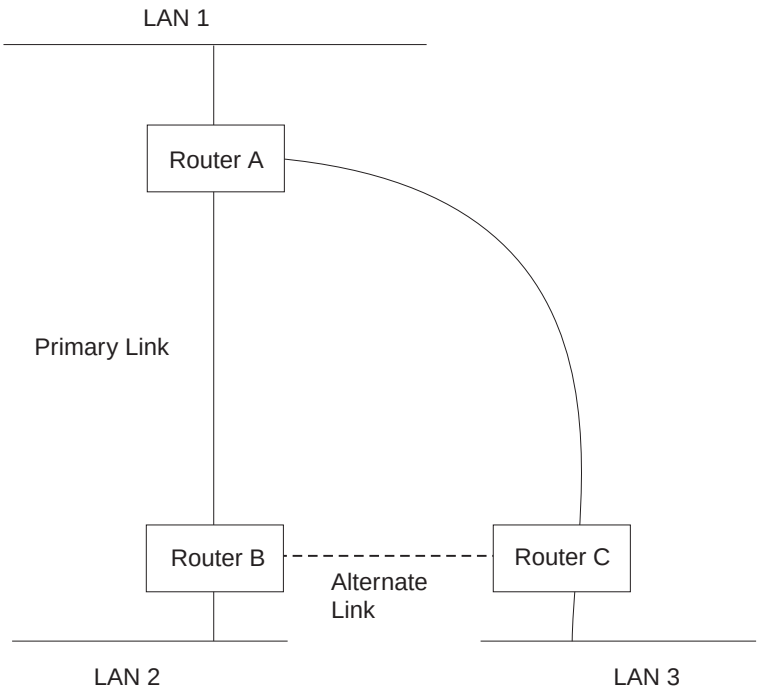
WAN 路由可使您设置备用路由，当主链路失效时，路由器便可通过备用路由自动启动对信宿的新连接。有关 WAN 恢复的说明及有关 WAN 重新路由和拨号溢出是如何一起运行的说明，请参阅第55页的『WAN 恢复、WAN 重新路由和拨号溢出』。

WAN 重新路由进程涉及到:

1. 检测失效的主链路
2. 转换到备用链路
3. 检测主链路恢复
4. 转换到主链路

备用链路可以是可在该链路上配置路由选择协议(例如 IP 或 IPX) 的任何链路，并且，备用链路的数据链路类型不必与主链路的数据链路类型相匹配。例如，备用链路可以是 LAN 接口、PPP、帧中继或 X.25 串行接口，或者是 PPP 或中继拨号电路。下面是不能成为备用链路的接口类型实例: SDLC 串行接口、SRLY 串行接口及类似 V.25bis 和 ISDN 的基网络。

注: 如果主链路或备用链路是拨号电路，则不能将拨号电路配置成按需拨入。



如果路由器 A 和 B 之间的主链路失效，则 WAN 在路由器 B 和 C 之间建立起备用链路。从而，路由器 A 和 B 就可通过路由器 C 进行通信。

图 3. WAN 重新路由. 正常情况下，在路由器 A 和 B 及路由器 A 和 C 之间有连接。

拨号溢出

对于 IP 通信量，当主链路上的通信量速率达到指定的阈值时，拨号溢出允许您使用备用的接口。这表明在接通备用链路之前，不必断开主接口。当主接口的通信量达到指定的阈值时，路由器接通备用电路。为使用拨号溢出，必须配置 WAN 重新路由，且主接口必须是帧中继。 IP 是仅能通过拨号溢出而转换到备用接口的协议。此外，当使用拨号溢出时，应将 OSPF 用做 IP 路由选择协议，以取代 RIP。

有关配置拨号溢出的信息，请参阅第59页的『WAN 恢复、WAN 重新路由和拨号溢出配置命令』。

带宽监控

在 WAN 重新路由配置期间，可对拨号溢出指定带宽监控的间隔。对主接口的接收和传输带宽使用率进行监控。当主接口带宽达到*添加*阈值时，生成 WAN 重新路由请求，以接通备用接口。如果 WAN 重新路由成功接通了备用接口，则 IP 停止在主接口上的路由选择并开始在备用接口上进行路由选择。

如果 WAN 重新路由没有成功地接通备用路由，则其定期进行接通备用接口的尝试，直到主接口的带宽使用率降至*放弃*阈值以下。

当主接口的接收和传输带宽使用率达到*放弃*阈值，并且已超过最小配置时间时，放弃使用备用接口。这使 IP 终止备用接口上的路由选择，而开始使用主接口。

添加阈值和分接阈值指定成主链路的线路速度百分比(已配置)。配置的线路速度不是总与链路的实际速度相匹配。向各个方向的链路上的通信量是分开计算的。如果在任何方向上的通信量大于指定的百分比，则超越阈值。

配置 WAN 重新路由

以下是配置 WAN 重新路由时所需的步骤。下一节是有关如何执行这些任务的示例。

为配置 WAN 重新路由，您需要:

1. 配置主链路
2. 配置备用电路
3. 向主链路指配备用电路。您也可为主链路指定稳定周期。

   您可向主链路指定在超越稳定周期(如果已经配置)之后所发生的 time-of-day revert-back。这就使辅助链路仍保持接通状态，直到用户所期望的时间结束和在非高峰期还原到主链路时止。

   注: 主链路和备用链路可以是不同的数据链路类型。它们可以是:

   - LAN 接口。
   - PPP 串行接口。li>
   - 帧中继串行接口。
   - X.25 串行接口。
   - PPP 拨号电路。
   - 帧中继拨号电路。

WAN 重新路由配置样本

第78页的图4说明了在 ISDN 上将帧中继拨号电路用做备用链路的 WAN 重新路由。如果路由器 A 和路由器 C 之间的帧中继 DLCI 失效，则 WAN 重新路由使用拨号电路建立起通过路由器 D 的备用连接。如果主链路之一不能连接到总部的一条支线上，则 WAN 重新路由通过另外一条支线建立起连接到总部的备用路由。

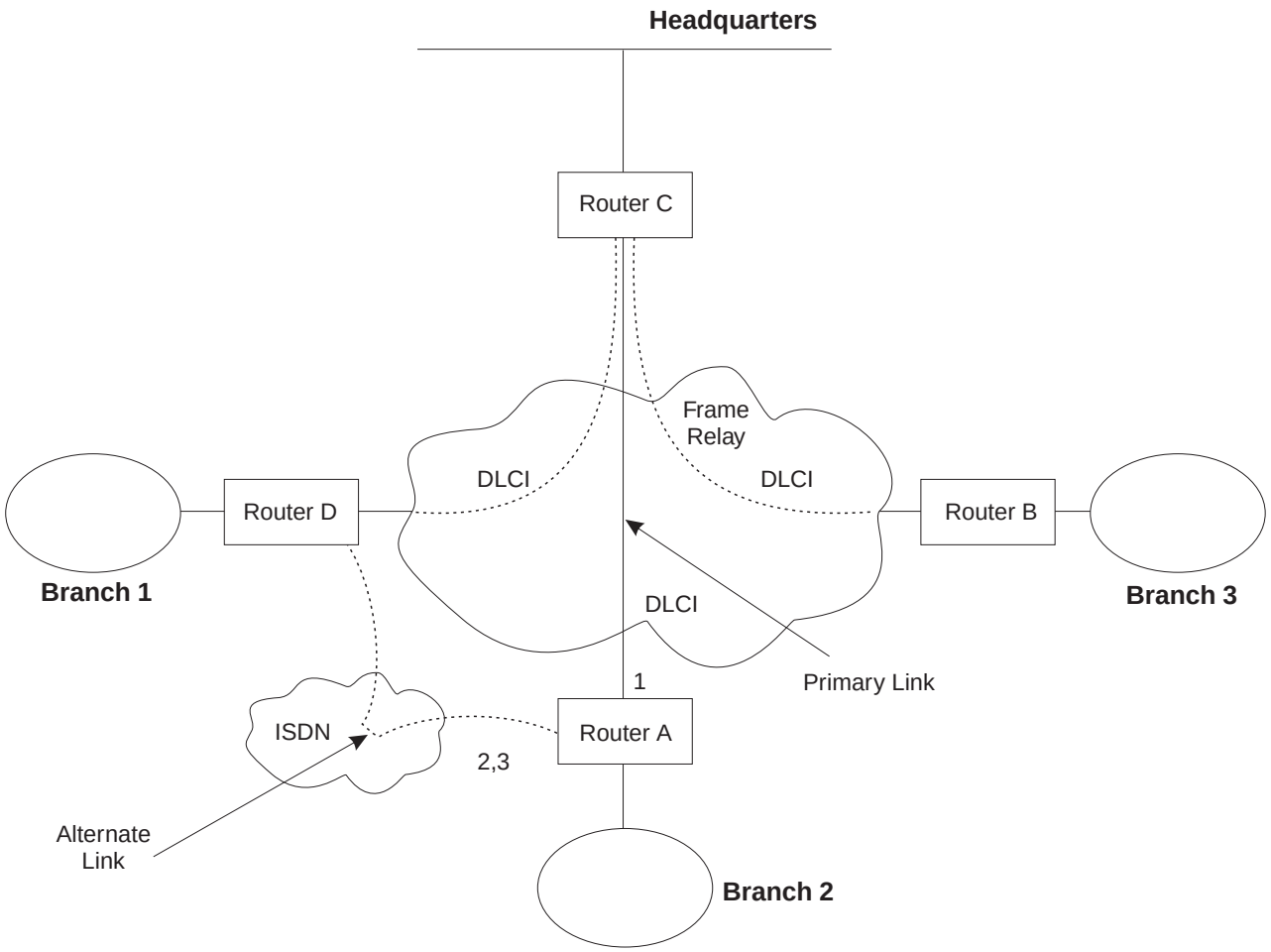


图 4. WAN 重新路由配置样本. 分部使用帧中继以连接到总部。

以下部分是说明如何在图4中的路由器 A 上设置 WAN 重新路由。您需要:

- 配置主帧中继接口 (1), 使其有所需的 PVC 或 PVC 组, 或者, 在帧中继接口上启用 No-PVC 功能。
- 配置 ISDN 接口 (2) 及其帧中继拨号电路 (3)。
- 将拨号电路指定为主链路帧中继接口的备用链路, 并且, 在拨号电路配置提示符下发出 'set idle 0' 命令。
  - 您可有选择性地指定:
  - 主链路的稳定周期,
  - 主链路的time-of-day revert-back 窗口。

下面对这些任务进行了详细的说明。

配置帧中继接口

为对 WAN 重新路由配置帧中继接口, 在路由器 A 上, 在主帧中继接口上的路由器 A 和 C 之间添加 PVC。

当对其它路由器的连接断开时, 为使主 FR 接口显示断开, 您需三个选项:

1. 启用 No-PVC 功能。启用了此功能后, 如果没有活动的 PVC, 则 FR 接口断开。

2. 按要求配置 PVC，但不要配置要求的 PVC 组中的 PVC。在这种情况下，FR 接口在 PVC 不活动的状态下断开。
3. 按要求配置 PVC 集，并将其作为必需的 PVC 组的一部分。在这种情况下，FR 接口在必需的 PVC 组中的所有 PVC 不活动的状态下断开。

按照这些步骤，配置主帧中继接口:

1. 如果您没有这样配置，将接口上的数据链路设置为帧中继。

```
Config>set data-link frame relay
Interface Number [0]? 2
```

2. 进入帧中继配置进程。

```
Config>network
What is the network number [0]?2
Frame Relay user configuration
FR Config>
```

注: 仅完成配置主帧中继接口的两个剩余步骤中的一个。

3. 使用 **add permanent-virtual-circuit** 命令，添加 PVC。

   按照要求，配置 PVC:

   对于问题 『Is circuit required for interface operation ?』， 请输入 **y**。

   为将 PVC 配置成必需的 PVC 组成员:

   a. 对于问题 『Does circuit belong to a Required PVC group ?』，请输入 **y**。

   b. 请输入组名，以回答问题 『What is the group name ?』。

   如果您已添加了 PVC，请使用 **change permanent-virtual-circuit** 命令，按照需要配置 PVC，并将其恰当地指定到必需的 PVC 组。详细信息，请参阅*Access Integration Services 软件用户指南*中的使用帧中继接口。

```
FR Config>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]?y
Does the circuit belong to a required PVC group [N]? y
What is the group name []?group1
```

4. 如果需要，请启用 No-PVC 功能。

   注: 仅当您没有进行上一步时，完成这一步。

```
FR Config>enable no-pvc
```

您还可对帧中继设置其它参数。详细信息，请参阅*Access Integration Services 软件用户指南*中的'使用帧中继'。

配置 ISDN 接口和拨号电路

配置路由器 A 和 D 之间的 ISDN 接口和拨号电路。有关如何配置 ISDN 接口和拨号电路，请参阅*Access Integration Services 软件用户指南*中的'使用 ISDN 接口'。

与 WAN 恢复所不同的是，您必须在将用做备用链路的拨号链路上配置可路由协议。如果不能阻止可路由协议发送维护信息包，则即使无须路由选择，备用链路都将建立连接。在这种情况下，如果您仅为了重新路由选择而使用备用链路，则禁用拨号电路。为禁用拨号电路，请在 Config> 提示符下，输入 **disable interface** 命令。

如果您向 ISDN 接口指定了多条拨号电路，则您可对拨号电路设置优先级。如果所有的 B 信道在物理接口上有活动的拨号电路，并且具有较高优先级的电路接收了信息包，则最低的优先级连接终止，而较高的优先级电路建立起连接。

您可将优先级设置在 0 和 15 之间，其中 15 表示最高优先级的电路，0 表示最低优先级的电路。新建拨号电路的缺省优先级是 8。请在 `Circuit Config>` 提示符下输入 **set priority** 以更改优先级。

指定和配置备用链路

进入 WAN 重新路由配置进程，以将拨号电路指定为 LAN 接口、PPP、帧中继或 X.25 串行接口的备用电路，或将拨号电路指定为 PPP 或帧中继拨号电路，并且，在需要的情况下，可指定稳定周期或/和 time-of-day revert-back 窗口。

有两种类型的稳定周期:

- *首次稳定周期*，是当路由器首次尝试接通主接口时，在主接口进入活动状态之前路由器所等待的时间。如果在首次稳定周期结束之后，主链路未进入活动状态，则 WAN 重新路由接通备用链路。
- *稳定周期*，是在路由器从备用链路转换到主链路之前，路由器为确定主链路是可靠的而所等待的时间。

time-of-day revert-back 窗口是在接通主链路及任何已配置的稳定时间结束后，用户期望转换到主链路的特定时间。

通过使用 24 小时时钟，用户指定还原窗口开始和结束时的小时时间。辅助链路处于接通状态，直到到达开始时间时才断开。如果主链路刚开通时的时间是处于开始和结束小时(位于窗口中)之间，则启动稳定时间之后立即转换到主链路。

按这些步骤指定和配置备用链路:

1. 进入 WAN 恢复配置进程。

   ```
   Config>feature wrs
   WAN Restoral user configuration
   ```

2. 将拨号电路指定为主帧中继接口的备用电路。

   ```
   WRS Config>add alternate-circuit
   Alternate interface number  [0]? 4
   Primary interface number  [0]? 1
   ```

3. 启用备用电路。

   ```
   WRS Config>enable alternate-circuit
   Alternate interface number  [0]? 4
   ```

4. 可选择性地指定首次稳定周期。

   如果要设置特定主接口的首次稳定周期，请使用 **set first-stabilization-period** 命令。对于未设置特定周期的所有接口，如果要设置缺省的首次稳定周期，请使用 **set default first-stabilization-period** 命令。

   ```
   WRS Config>set first-stabilization-period
   Primary interface number [0]?
   First primary stabilization time (0 - 3600 seconds -1=default) [-1]?

   WRS Config>set default first-stabilization-period
   Default first primary stabilization time (0 - 3600 seconds) [0]?
   ```

5. 可选择性地指定稳定周期。如果要为指定地接口设置稳定周期，请使用 **set stabilization-period** 命令。对于未设置特定周期的所有接口，如果要设置缺省的稳定周期，请使用 **set default stabilization-period** 命令。

```
WRS Config>set stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
WRS Config>set default stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

6. 可选择性地指定 time-of-day revert-back 窗口。

   如果要设置指定接口窗口的开始和结束时间，请使用 set start-time-of-day-revert-back 和 stop-time-of-day-revert-back 命令。缺省值 0 表示未配置任何窗口。24 小时时钟起始于 1 a.m.，结束于午夜 24 点。如果开始时间和结束时间相同(但不是 0)，则还原将准确地在这一时间同时发生。

   以下是设置返回窗口的两个实例:

   a. 如果开始时间是 23，结束时间是 3，则还原窗口显示为从 11 p.m. 到 3 a.m.。

   b. 如果开始时间是 1，结束时间是 5，则还原窗口显示为从 1 a.m. 到 5 a.m.。

```
WRS Config> set start-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
WRS Config> set stop-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?
```

配置 WAN 重新路由

第8章 使用网络调度程序功能

本章介绍如何使用网络调度程序功能，包括以下几个部分:

- 『网络调度程序概述』
- 第84页的『使用网络调度程序均衡 TCP 和 UDP 通信量』
- 第84页的『网络调度程序的高可用性』
- 第86页的『配置网络调度程序』
- 第92页的『通过 TN3270 服务器使用网络调度程序』

网络调度程序使用 IBM 研究的负载均衡技术，确定用来接收每一个新连接的最佳服务器。这项技术同样用在 Solaris、Windows NT 和 AIX 的 IBM 网络调度程序产品中。

网络调度程序概述

网络调度程序是提高服务器性能的一种功能，它通过在一组服务器内将 TCP/IP 会话请求转发到不同的服务器，实现所有服务器中的请求负载均衡。对于用户和应用程序来说，这种转发操作是透明的。网络调度程序广泛应用于一些服务器应用程序，如 E-mail、World Wide Web 服务、分布式并行数据库查询和其它 TCP/IP 应用程序。

通过网络调度程序也可将一组服务器的无状态 UDP 应用程序通信量负载均衡。

网络调度程序可提供解决锋值需求问题的功能强大、灵活和可变规模的方案，有助于最大限度地增加用户现场的潜能。在峰值需求期间，网络调度程序可自动查找用来处理入网请求的最佳服务器。

网络调度程序功能的负载均衡操作不使用域名服务器。而是通过一种独特的负载均衡及管理软件的组合，实现多个用户服务器当中通信量的均衡。网络调度程序还能检测失效服务器，并可将其通信量向其它可用服务器转发。

所有发向网络调度程序计算机的客户机请求都被转发到特定服务器，该服务器是由网络调度程序根据特定动态设置权重选定的最佳服务器。用户可使用这些权重的缺省值，或在配置操作期间加以更改。

服务器向客户机返回响应时无需网络调度程序的任何参与。无需附加的软件，就可在用户服务器上实现与网络调度程序的通信。

对于大型、可变规模的服务器网络来说，网络调度程序功能是其稳定、有效管理的关键。通过网络调度程序，可将许多独立的服务器链接成一个单一的虚拟服务器。这样用户现场对外就表现为一个单一的 IP 地址。网络调度程序独立地执行域名服务器的功能；所有请求都被发送到网络调度程序计算机的 IP 地址。

网络调度程序允许基于 SNMP 的管理应用程序通过接收基础统计信息和潜在警告，实现对网络调度程序状态的监控。有关的详细信息，请参阅 *Protocol Configuration and Monitoring Reference Volume 1* 中的『SNMP 管理』。

网络调度程序能有效地进行群集服务器的通信量负载均衡，实现用户现场的稳定、有效管理。

使用网络调度程序均衡 TCP 和 UDP 通信量

负载均衡有许多不同的方法。其中有些方法允许用户在第一个服务器速度缓慢或没有响应时，随机地选择其它的服务器。另一种方法是循环法，通过该方法域名服务器可选择一个用来处理请求的服务器。这种方法较好，但仍未考虑目标服务器上的当前负载或目标服务器是否可用。

以请求类型、服务器负载分析或用户指定的可配置权重集为基础，网络调度程序可以将对不同服务器的请求负载均衡。为管理各种不同类型的均衡操作，网络调度程序由以下部件组成:

执行器 对各连接的负载均衡是以接收到的请求类型为基准的。典型的请求类型是 HTTP、FTP 和 Telnet。此部件始终运行。

通告器 查询服务器并通过每个服务器的协议分析结果。通告器将结果信息传送到***管理器***以设置合适的权重。通告器是一个可选部件。

网络调度程序支持 FTP、HTTP、SMTP、NNTP、POP3 和 Telnet 类型的通告器，以及 TN3270 通告器，该通告器同 TN3270 服务器一同使用于 IBM 2210s、IBM 2212s 和 IBM 2216s 中，此外网络调度程序还支持与 Workload Manager (WLM) 一同在 MVS 系统上使用的 MVS 通告器。WLM 依据各自的 MVS ID 来管理一定数量的工作负荷。网络调度程序可以使用 WLM 协助对运行 OS/390 V1R3 或之后版本的 MVS 服务器的请求进行负载均衡。

对 UDP 协议来说，没有专门的协议通告器。如果您有 MVS 服务器，则可以使用 MVS 系统通告器来提供服务器负载信息。另外，如果端口正在处理 TCP 和 UDP 通信流，则可使用合适的 TCP 协议通告器为端口提供通告器输入。网络调度程序将使用该输入对端口上的 TCP 和 UDP 通信量进行负载均衡。

管理器 服务器权重的设置是基于:

- 执行器中的内部计数器
- 由协议通告器提供的来自服务器的反馈。
- 来自系统监控程序 (MVS 通告器) 的反馈。

管理器是一个可选部件。但是，如果不使用管理器，则网络调度程序将采用基于当前服务器权重的循环调度法来均衡负载。

当使用网络调度程序对无状态 UDP 通信量进行负载均衡时，用户只能使用那些以源自请求的目的地 IP 地址响应客户机的服务器。有关的完整解释，请参阅第90页的『配置网络调度程序服务器』。

网络调度程序的高可用性

基本网络调度程序功能有以下特性，从许多不同的角度看，正是这些特性保证网络调度程序出故障的概率很小:

- 该程序检查所有输入路径的通信量。如果现有连接上的一些信息包是通过网络调度程序以不同的路径到达服务器，则服务器会立即复位该连接。
- 该程序保持对所有已建立连接的跟踪，虽然该程序并不终止这些连接，但如果网络调度程序连接表的记录丢失，将导致连接复位。
- 对于当作上一中继和连接终止的任何先前的中继路由器，这种情况都会出现。

由于具有这些特性，所以对于整个群集器来说，下列故障是很严重的:

- 如果网络调度程序由于某种原因出现故障，丢失了所有连接表，则将失去客户机到服务器的所有现有连接。假设存在使某客户机直接到达服务器的第二个网络调度程序，则只有经过通常为几分钟的路由协议延迟之后，新的连接才能接通。
- 如果先前 IP 路由器与配置后的网络调度程序之间的接口失效，则将丢失所有连接，或一定存在另一个到达相同网络调度程序的接口，IP 路由器在这样的接口中执行事例恢复 (以延迟几分钟的顺序使用 ARP 老化机构)。
- 如果网络调度程序和服务器间的接口失效，且先前的中继路由器假设网络调度程序是上一个中继，则不会对新的连接进行重新路由。将丢失现有连接且无法建立新连接。

所有这些故障中，不仅有网络调度程序故障，也有网络调度程序邻居故障，都将导致丢失所有现有连接。即使使用运行标准 IP 恢复机构的备份网络调度程序，最理想的恢复操作也是很慢的，且只适应于新的连接。最坏的情况是这些连接无法恢复。

为改进网络调度程序的可用性，网络调度程序高可用性功能使用下列机构:

- 两个网络调度程序，它们具备与相同的客户机、相同的服务器群集器之间的连通性，同时两个网络调度程序间也具备连通性。
- 两个网络调度程序间的『脉动』机构，用于检测网络调度程序故障。
- 一种可达性标准，用来标识从每个网络调度程序能和不能到达的 IP 主机。
- 网络调度程序数据库的同步信息 (即连接表、可达性表和其它数据库)。
- 选择活动网络调度程序的逻辑，用于管理服务器的给定群集器和备份网络调度程序，它们之间保持同步。
- 执行快速 IP 替换的机构，在逻辑或操作员决定转换活动和备份状态时使用。

故障检测

除了基本的故障检测标准 (通过脉动消息检测活动和备份网络调度程序之间是否丢失连通性) 外，还有另一个名为『可达性标准』的故障检测机构。当配置网络调度程序时，用户提供主机列表，网络调度程序应能准确到达这些主机并正确工作。主机可以是路由器、IP 服务器或其它类型的主机。主机可达性通过检测主机网络连接获得。

如果脉动消息无法流过，或活动网络调度程序不再满足可到达性标准且备份网络调度程序可到达时，则发生转换。为了在所有可用信息基础上作决策，活动网络调度程序有规律地向备份网络调度程序发送其可达性能力。然后，备份网络调度程序将该能力与自己的比较，并决定是否转换。

数据库同步

主要网络调度程序和备份网络调度程序通过“脉动”机构保持它们的数据库同步。网络调度程序数据库包括连接表、可达性表和其它信息。网络调度程序高可用性功能使用数据库同步协议，以保证两个网络调度程序包含相同的连接表项。该同步考虑了引起传输延迟的一个已知错误容限。由协议执行数据库的初始同步，然后通过周期性的更新保持数据库同步。

恢复策略

出现网络调度程序故障时，IP 替换机构将立刻把所有通信量导向备份网络调度程序。数据库同步机构保证备份网络调度程序与活动网络调度程序具有相同的项。当网络 (任何客户机和后端服务器之间的硬件或软件媒介) 中出现故障，且存在通向备份网络调度程序的备用路径，则在备用路径上执行转换。

IP 替换

注: 假定群集器 IP 地址作为先前中继路由器 (IP 路由器)，位于同一逻辑子网上。

IP 路由器将通过 ARP 协议分解群集器地址。为执行 IP 替换，网络调度程序 (备份的变为活动的) 将向自身发出 ARP 请求，该请求被广播到所有直接相连且属于该群集器逻辑子网的网络。先前中继的 IP 路由器将更新其 ARP 表 (依据 RFC826)，以便将该群集器的所有通信量发送到新的活动 (先前备份的) 网络调度程序。

配置网络调度程序

为支持用户现场，用户可使用多种方法配置网络调度程序。如果客户连接的用户现场只有一个主机名，则可以定义一个单一群集器和用户准备接收连接的任意端口。该配置如图5中所示。

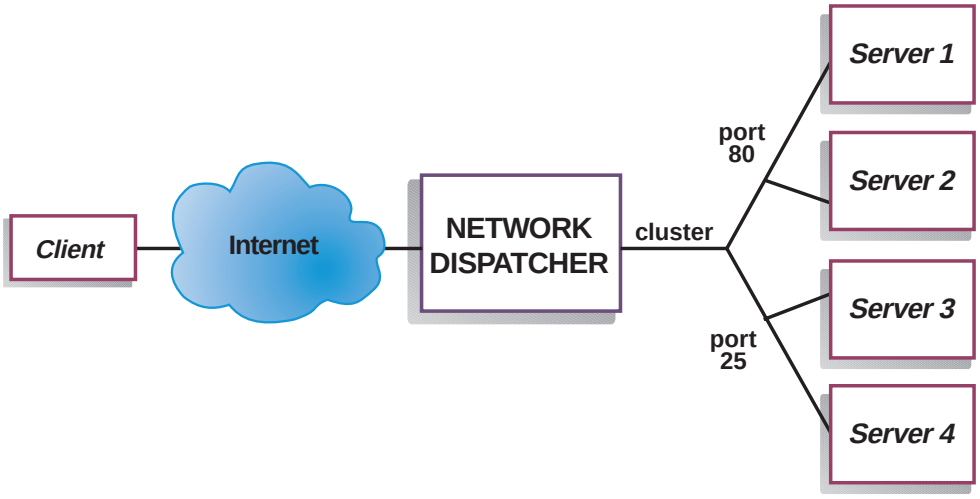


图 5. 下面是配置为 1 个单一的群集器和 2 个端口的网络调度程序的实例。

如果用户现场包括对许多公司或部门的主机操作，每一个公司或部门以不同的 URL 的加入用户现场，则有必要使用另一种配置网络调度程序的方法。在以上的情况中，用户或许希望为每个公司或部门定义一个群集器，并希望定义在如第87页的图6所示的 URL 上接收连接的任意端口。

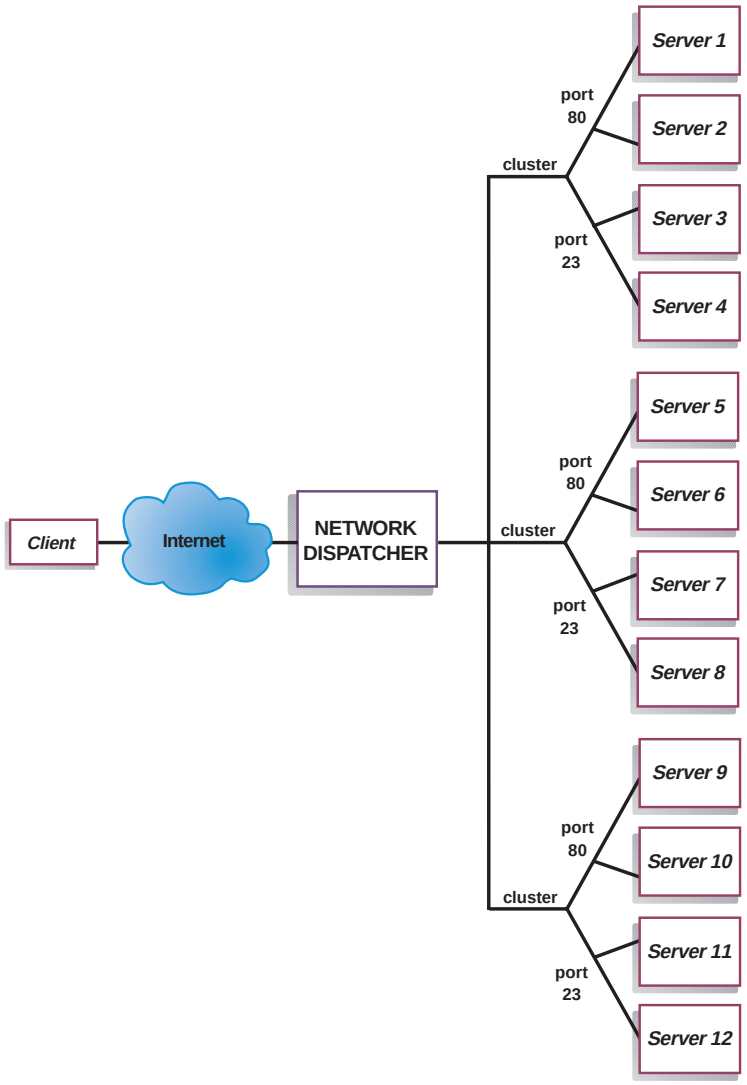


图 6. 下面是配置为 3 个群集器和 3 个 URL 的网络调度程序的实例。

如果您有非常大的现场，现场中每个协议支持多个服务器，则最好使用第三种配置网络调度程序的方法。例如，用户为下载大型文件，会选择带直接 T3 线路的分离 FTP 服务器。在以上情况中，用户或许希望为每个带单一端口，但带多个如第88页的图7所示服务器的协议定义一个群集器。

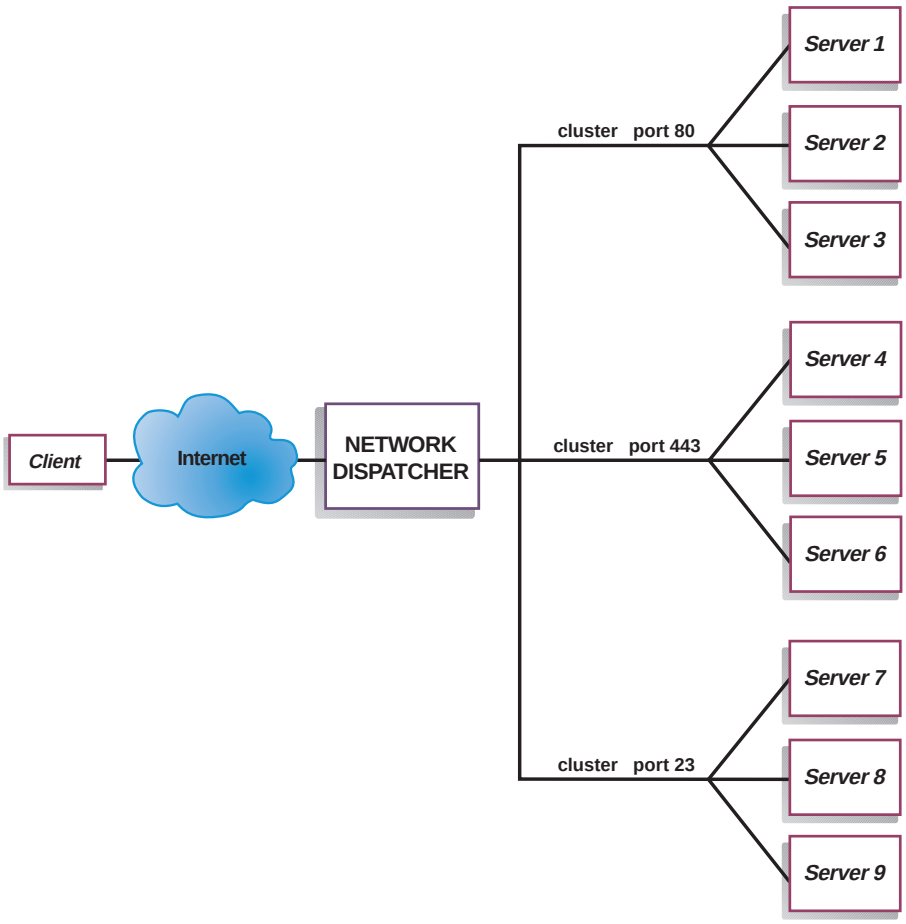


图 7. 下面是配置为 3 个群集器和 3 个 端口的网络调度程序的实例。

配置步骤

在配置网络调度程序之前，需要:

1. 保证网络调度程序具有与服务器的直接接口。服务器可具有同企业路由器或 Internet 的独立连接，这样从服务器到客户机的出网通信量可以旁路网络调度程序；但用户不必配置独立的连接。

   如果高可用性对您的网络十分重要，则可以从第89页的图8中看到典型的高可用性配置。

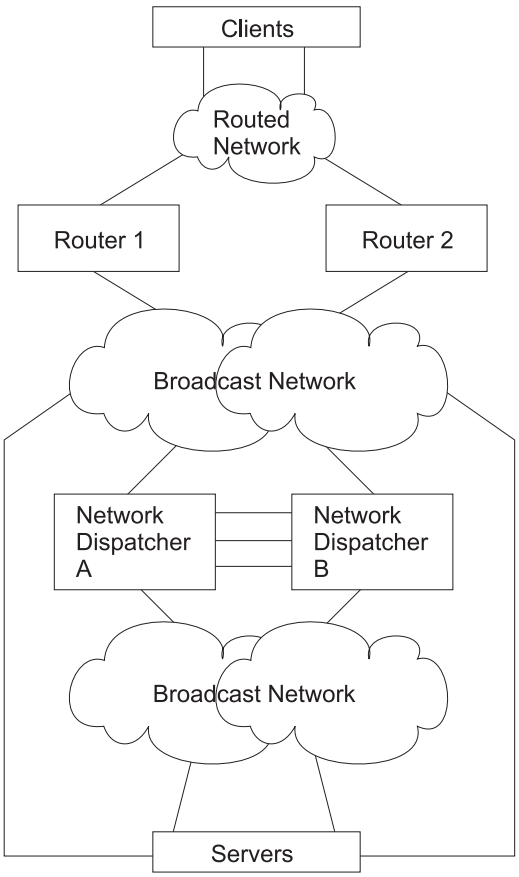


图 8. 高可用性网络调度程序配置

2. 配置设备接口。包括配置所有接口、所有接口上的 IP 地址和所有适用的路由协议。同时必须使用 **set internal-ip-address** 命令配置内部 IP 地址。请参阅*Protocol Configuration and Monitoring Reference Volume 1*，获取有关 **set internal-ip-address** 的详细信息。
3. 启动或重新启动设备。

在 IBM 2212 上配置网络调度程序

要在 IBM 2212 上配置网络调度程序，需要:

1. 使用 **feature ndr** 命令访问网络调度程序功能。
2. 使用 **enable executor** 和 **enable manager** 命令启用执行器和管理器。
3. 使用 **add cluster** 命令配置群集器。
4. 对于提供相应协议的服务器的每个群集器，使用 **add port** 命令配置 TCP 和 UDP 目的地端口。端口实例如: 用于 HTTP 的 80、用于 FTP 的 20 和 21 及用于 Telnet 的 23。
5. 使用 **add server** 命令配置服务器。服务器始终与端口和群集器相关。如果服务器的操作系统支持多别名设置，则一个服务器可服务多个端口，一个端口可应用到多个服务器，且一个服务器可属于多个群集器。
6. 使用 **add advisor** 命令配置任意通告器。

注:

a. 对于 MVS 通告器，不要在任何群集器下定义端口号码值 (缺省值是 10007)。该端口号码只由 MVS 通告器用于在 MVS 系统中与 WLM 通信。

b. 对于 TN3270 通告器，输入两个端口值。用于客户机/服务器通信的端口号码值 (缺省值是 23) 必须在合适的群集器下进行定义。不要在任意群集器下定义通信端口值 (缺省值是 10008)。通信端口值只由 TN3270 通告器用来从 TN3270 服务器收集负载信息。

7. 使用 **enable advisor** 命令启用用户配置后的通告器。

如果您要配置高可用性的网络调度程序，请按以下步骤操作。如果不需配置高可用性，则可结束配置。

注: 先在主要网络调度程序上执行这些步骤，然后在备份网络调度程序上执行。为保证数据库正确同步，主要网络调度程序中的执行器必须先于备份中的启用。

8. 网络调度程序是配置成主要的还是备份的，转换是配置成手动还是自动，可使用 **add backup** 命令进行设置。
9. 要配置主要和备份网络调度程序之间所有脉动路径，可使用 **add heartbeat** 命令。路径由源和目的 IP 地址指定。特别推荐在主要和备份网络调度程序之间配置多个脉动路径，以确保一个端口故障不会破坏主要和备份计算机之间的脉动通信。
10. 对于为确保完整服务，而要求网络调度程序必须能够到达的主机 IP 地址列表的配置，可使用 **add reach** 命令。一般来说，主要是服务器子网、企业路由器和主管部门工作站。

用户要更改配置，可使用 **set**、 **remove** 和 **disable** 命令。有关这些命令的详细信息，请参阅第95页的『第9章 配置和监控网络调度程序功能部件』。

配置网络调度程序服务器

要在服务器上配置网络调度程序，需要:

1. 反馈设备别名设置。

   对于 TCP 和 UDP 服务器，用户必须将反馈设备 (通常称为 ***lo0***) 设置 (或宁可别名设置) 为群集器地址。网络调度程序在将 IP 包转发到服务器计算机之前，不会更改该包中的目的地 IP 地址。当用户将反馈设备设置为或别名设置为群集器地址时，服务器计算机将接受被定位到群集器地址的信息包。

   对于服务器来说，使用群集器地址，而不是其自身的 IP 地址来响应客户机是十分重要的。以上所说不涉及 TCP 服务器，只涉及一些 UDP 服务器，当响应发送到群集器地址的请求时，这些服务器使用其自身的 IP 地址。当服务器使用其自身的 IP 地址时，有些客户机会因为服务器的响应不是来自它期望的源 IP 地址而废除该响应。用户应只使用那些响应客户机时使用来自请求的目的地 IP 地址的 UDP 服务器。在这种情况下，来自请求的目的地 IP 地址是群集器地址。

   如果您的操作系统是支持网络接口别名设置的操作系统，如 AIX、Solaris 或 Windows NT，则您应将反馈设备别名设置为群集器地址。使用支持别名设置的操作系统的好处是，用户可以将服务器计算机配置为服务多群集器地址。

   如果您的操作系统是不支持别名设置的操作系统，如 HP-UX 和 OS/2，则您必须将 ***lo0*** 设置为群集器地址。

   如果您的服务器是运行 TCP/IP V3R2 的 MVS 系统，则您必须将 VIPA 地址设置为群集器地址。它将作为反馈地址使用。VIPA 地址不一定要属于直接连接到 MVS

节点的子网。如果您的 MVS 系统正在运行 TCP/IP V3R3，则您必须将反馈设备设置为群集器地址。如果您正在使用高可用性，则必须在 MVS 系统中启用 RouteD，以便高可用性替换机构正常工作。

注： 本章列出的命令在以下的操作系统和版本中进行了测试：AIX 4.1.5 和 4.2、HP-UX 10.2.0、Linux、OS/2 Warp Connect Version 3.0、OS/2 Warp Version 4.0、Solaris 2.5 (Sun OS 5.5) 及 Windows NT 3.51 和 4.0。

可使用如表10中所示的用户操作系统命设置或别名设置反馈设备。

表 10. 对调度程序的反馈设备 (lo0) 进行别名设置的命令

系统	命令
AIX	**ifconfig lo0 alias** *cluster_address*
HP-UX	**ifconfig lo0** *cluster_address*
Linux	**ifconfig lo:1 cluster_address netmask up**
OS/2	**ifconfig lo cluster_address**
Solaris	**ifconfig lo0:1 cluster_address 127.0.0.1 up**
Windows NT	a. 单击开始，再单击设置。 b. 单击控制面板，再双击网络。 c. 如果您还没有如此操作，则添加 MS 反馈适配器驱动程序。 1) 在网络窗口中，单击适配器。 2) 选择 MS 反馈适配器，再单击确定。 3) 出现提示后，插入安装用 CD 或磁盘。 4) 在网络窗口中，单击协议。 5) 选择 TCP/IP 协议，再单击属性。 6) 选择 MS 反馈适配器，再单击确定。 d. 将反馈地址设置为您的群集器地址。接受缺省的子网掩码 (255.0.0.0)，不要输入网关地址。 **注：** 您必须先退出，然后在 TCP/IP 配置下的 MS 反馈驱动程序显示出来之前重新进入网络设置。

2. 查找附加路由。

   有些操作系统已创建了缺省路由，且需要删除该路由。

   a. 在 Windows NT 系统中查找附加路由可使用如下命令： **route print**

   b. 在所有 UNIX 系统和 OS/2 系统中查找附加路由可使用如下命令： **netstat -nr**

   c. Windows NT 系统实例：输入 route print 后，将显示与以下类似的表格。 (本例展示查找和删除通往网络掩码为 255.0.0.0 的群集器 9.67.133.158 的附加路由的操作过程。)

   活动路由:

网络地址	网络掩码	网关地址	接口	标准
0.0.0.0	0.0.0.0	9.67.128.1	9.67.133.67	1
9.0.0.0	255.0.0.0	9.67.133.158	9.67.133.158	1
9.67.128.0	255.255.248.0	9.67.133.67	9.67.133.67	1
9.67.133.67	255.255.255.255	127.0.0.1	127.0.0.1	1
9.67.133.158	255.255.255.255	127.0.0.1	127.0.0.1	1
9.255.255.255	255.255.255.255	9.67.133.67	9.67.133.67	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	224.0.0.0	9.67.133.158	9.67.133.158	1
224.0.0.0	224.0.0.0	9.67.133.67	9.67.133.67	1
255.255.255.255	255.255.255.255	9.67.133.67	9.67.133.67	1

d. 在“网关地址”一列下可查找群集器地址。如果存在附加路由，则群集器地址将出现两次。在给出的实例中，群集器地址 (9.67.133.158) 出现在第 2 行和第 8 行。

e. 网络地址可在群集器地址出现的每一行中查找。用户只需要这些路由中的一个路由，需删除其它无关的路由。删除的附加路由应是一个网络地址，以群集器地址的第一个数位开头，后跟三个零。在实例中，附加路由在第 2 行中，其网络地址为 9.0.0.0:

```
9.0.0.0         255.0.0.0      9.67.133.158      9.67.133.158      1
```

3. 删除所有附加路由。

使用用户操作系统命令 表11 来删除所有附加路由。

表 11. 不同操作系统的删除路由的命令

操作系统	命令
AIX	**route delete -net** *network_address cluster_address*
HP-Unix	**route delete** *cluster_address cluster_address*
Solaris	无需删除路由。
OS/2	无需删除路由。
Windows NT	**route delete** *network_address cluster_address* **注:** 该命令应在 MS-DOS 提示符下输入。

通过 TN3270 服务器使用网络调度程序

网络调度程序可通过群集器 2210s、2212s、网络公用程序使用，或通过运行 TN3270 服务器功能 (该功能为 TN3270e 服务器提供了大型 3270 环境的支持) 的 2216s 使用。TN3270 通告器允许网络调度程序从每个 TN3270e 服务器实时地收集有关负载的统计信息，以便在 TN3270 服务器中实现负载的最佳分布。除了那些网络调度程序路由器外部的 TN3270 服务器外，群集器中的 TN3270 服务器中可以有一个是内部的 - 它可作为网络调度程序在同一路由器运行。

配置过程的关键

TN3270e 服务器的配置与在这些服务器之前是否有网络调度程序同样重要。事实上，TN3270e 服务器无法知道来自客户机的通信量正通过另外的计算机进行调度。但是，当设置通过网络调度程序使用的外部 TN3270 服务器时，有一些要点应牢记:

- 由于网络调度程序不更改其转发给服务器的信息包中的目的地 IP 地址 (如群集器地址)，所以每个服务器中的 TN3270 服务器 IP 地址必须设置成与群集器 IP 地址相等。
- 为了将信息包传送给服务器功能，运行 TN3270 服务器功能的路由器必须知道路由器中运行的 TN3270 功能的 IP 地址。因此，TN3270 服务器 IP 地址 (如群集器地址) 也必须在每个 TN3270 服务器路由器上，作为路由器的内部 IP 地址或作为路由器接口之一上的辅助地址进行定义。
- 用户必须确保 TN3270e 服务器 (如 OSPF 或 RIP)上使用的所有路由协议都不发布群集器地址。网络调度程序路由器必须“拥有”涉及到客户机网络的群集器地址，这样网络调度程序路由器必须是唯一发布群集器地址的路由器。

- 在同一 LAN 上，如果客户机到网络调度程序的通信量与网络调度程序到服务器的通信相同，则用户必须确保不响应群集器地址的 ARP，因此群集器地址不能在服务器同该 LAN 的接口上定义。网络调度程序必须是在接收客户机通信量的 LAN 上唯一响应 ARP 的程序。

当 TN3270 服务器与网络调度程序处在同一路由器中时，TN3270 服务器 IP 地址被设置为群集器地址，但该地址必须未被当作内部 IP 地址或接口地址在路由器上定义。

明示 LU 和网络调度程序

在网络调度程序环境中，需要特别注意明示 LU 定义。对默示或明示 LU 的会话请求可被调度到任何服务器。这意味着必须在每个服务器中定义明示 LU，因为每个服务器不知道会话在哪个服务器之前进行调度。

第9章 配置和监控网络调度程序功能部件

本章介绍网络调度程序功能部件配置和操作命令。包括以下内容:

- 『访问网络调度程序配置命令』
- 『网络调度程序配置命令』
- 第112页的『访问网络调度程序监控命令』
- 第112页的『网络调度程序监控命令』

访问网络调度程序配置命令

要访问网络调度程序配置环境，需要:

1. 在 OPCON 提示符 (*) 下输入 **talk 6**。
2. 在 Config > 提示符下输入 **feature ndr**。

网络调度程序配置命令

表12对网络调度程序配置命令进行概述，其它章节对这些命令进行解释。这些命令在 NDR Config > 提示符下输入。

表 12. 网络调度程序配置命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	配置网络调度程序的各种部件，包括通告器、群集器、端口和服务器。
Clear	清除全部网络调度程序配置。
Disable	禁用备份、执行器和管理器等网络调度程序部件。同时也禁用特定的通告器。
Enable	启用备份、执行器和管理器等网络调度程序部件。同时也启用特定的通告器。
List	显示全部网络调度程序配置或配置的特定部分。
Remove	删除网络调度程序配置的特定部分。
Set	更改通告器、群集器、端口、服务器或网络调度程序管理器的配置参数。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add

使用 **add** 命令可配置通告器、群集器、端口、服务器和到达地址。 为达高可用性，用户也可将该网络调度程序配置为主要的或备份的，并配置用于脉动和数据库同步的 IP 地址。

语法:

add advisor . . .
backup . . .
cluster . . .

heartbeat . . .

port . . .

reach . . .

server . . .

Advisor*name port# interval timeout comm-port*

指定通告器的名称和端口。该参数也指定通告器以特殊协议收集信息的频率，和通告器认为协议不可用之后的时间周期。

name 指定通告器类型。

表 13. 通告器名称和端口号码

通告器号	通告器名称	缺省端口号
0	FTP	21
1	HTTP	80
2	MVS	10007
3	TN3270	23
4	SMTP	25
5	NNTP	119
6	POPS	110
7	TELNET	23

有效值: 0 - 7

缺省值: 1

port# 指定该通告器的端口号码。

有效值: 1 到 65535

缺省值: 请参阅表13。

interval

指定通告器查询每个服务器协议的频率，以秒为单位。如果经过该时间值的一半后仍没有收到服务器响应，则通告器认为该协议不可用。

有效值: 0 到 65535

缺省值: 5

timeout

指定通告器认为协议不可用之前的时间间隔，以秒为单位。

为保证管理器在其负载均衡决策中不使用数据溢出的信息，管理器不使用来自时间标记比该参数设置值晚的通告器信息。通告器超时时间应大于通告器轮询时间间隔。如果超时时间较短，管理器可能会忽略本应使用的报告。缺省情况下，通告器报告不会超时。

该超时值一般应用于用户禁用通告器的情况。请不要将该参数同先前介绍的一半时间间隔的超时混淆，该一半时间间隔的超时与无响应的服务器有关。

有效值: 0 到 65535

缺省值: 0，表示认为协议始终是可用的。

Comm-port

指定 TN3270 通告器用来与 TN3270 服务器通信的端口号码。该参数只用作 TN3270 通告器输入。

有效值: 1 到 65535

缺省值: 10008

例 1:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet) [1]?
1
Port number [80]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
```

例 2:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet) [1]?
3
Port number [23]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
Communication Port number [10008]?
```

backup*role strategy*

指定该网络调度程序是备份的还是主要的。

role 定义是主要的还是备份的网络调度程序。只有当用户准备进行冗余配置，并运行高可用性功能时，才能使用该命令。在这种情况下，用户还必须配置脉动 (**add heartbeat**) 和可达性 (**add reach**)功能。

有效值: 0 或 1

0 表示主要

1 表示备份

缺省值: 0

strategy

指定网络调度程序是否自动或手动地转换回主要模式。如果策略被设置为*自动*，则无论何时主要网络调度程序失效并变为备份 (即备份网络调度程序执行了 IP 替换功能)，一旦数据库同步，它将自动成为活动的网络调度程序。如果策略被设置为*手动*，则旧的主要网络调度程序将变为备份模式，且操作员必须使用 talk 5 中的 **switchover** 命令才能再次使其变为活动态。请参阅第118页的『 Switchover 』。

有效值: 0 或 1

0 = 自动

1 = 手动

缺省值: 0

实例:

```
add backup
Role (0=Primary, 1=Backup) [0]?
Switch back strategy (0=Auto, 1=Manual) [0]?
```

cluster *address FIN-count FIN-timeout Stale-timer*

指定群集器的 IP 地址和执行器执行网络调度程序数据库无用单元收集的频率。

address

指定群集器的 IP 地址。

有效值: 任意有效的 IP 地址

缺省值: 0.0.0.0

FIN-count

指定 *FIN 超时*或 *Stale 定时器* 时间到后，执行器尝试从网络调度程序数据库删除无用连接信息之前，必须处于 FIN 状态的连接数量。

有效值: 0 到 65535

缺省值: 4000

FIN-timeout

指定执行器尝试从网络调度程序数据删除无用连接信息前，一个连接在 FIN 状态下所经过的秒数。

有效值: 0 到 65535

缺省值: 30

Stale-timer

指定执行器尝试从网络调度程序数据删除无用连接信息前，连接已处于非活动态所经过的秒数。

有效值: 0 到 65535

缺省值: 1500

实例:

```
NDR
Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.12
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.12
Fintimeout has been set to 30 for cluster 113.3.1.12
Staletimer has been set to 1500 for cluster 113.3.1.12
NDR Config>
```

heartbeat *address1 address2*

指定用于脉动消息的一条路径。为保证可靠，建议用户配置多个项。脉动消息将从属于该网络调度程序的 *address1* 流向属于对等网络调度程序的 *address2*。

address1

指定该流出脉动消息的网络调度程序的接口 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

address2

指定脉动消息流向的对等网络调度程序的接口 IP 地址。它必须是从 *address1* 中指定的接口可到达的地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

实例:

```
add heartbeat
Source Heartbeat address [0.0.0.0]? 131.2.25.90
Target Heartbeat Address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port# port-type max-weight port-mode*

指定端口和端口属性。

cluster-address

指定群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

port# 指定该群集器所用协议的端口号。

有效值: 1 到 65535

缺省值: 80

port-type

指定可在该端口上进行负载均衡的 IP 通信量的类型。支持的类型有:

- 1 = TCP
- 2 = UDP
- 3 = 两者

有效值: 1, 2, 3

缺省值: 3

max-weight

指定该端口上服务器的最大权重。它影响执行器向每个服务器发出请求的数量之差。

有效值: 0 到 100

缺省值: 20

port-mode

指定端口是否从单一的客户机向单一的服务器 (已知是 sticky) 传送所有请求，是否使用被动 FTP (pftp) 和或在该群集器上不使用特定协议 (无)。

有效值: 0 - 2, 其中:

- 0 = 无
- 1 = sticky
- 2 = pftp

缺省值: 0

实例:

```
Config>feature ndr
NDR>add cluster 1.2.3.4 4000 30 1500
NDR>add port
Cluster address [0.0.0.0]? 1.2.3.4
Port number [80]? 80
Port type [3]?
Maximum weight [20]?
Port mode [0=none, 1=sticky, 2=pftp ]? 0
```

指定 URL 掩码时可以使用的通配符。当配置 Web 服务器高速缓存的网络调度程序，或在 f webc 提示符下使用 **add** 或 **modify url** 命令时，可以使用通配符。作为通配符使用的字符是 * (星号) 或 # (数字符号)。通配符可作为 URL 的一部分用在任何位置。

符号 * 代表无字符或作为该 URL 一部分的所有字符:

实例: *abc.html 将滤除以下 URL 掩码。

```
abc.html
finabc.html
defchtjqsprabc.html
```

符号 # 代表任意单个字符。

实例: ab#.html 将滤除以下 URL 掩码。

```
abc.html
abf.html
abo.html
```

当选择了端口模式 3（高速缓存=3）且未添加新的高速缓存分区时，以下实例是适用的。

```
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.11
Port number [80]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3) 0? 3
Do you want a new cache partition? Yes: n
Enter cache partition [0]? 0
Maximum TCP segment size  (Range 512-32768 bytes) 4096?
Default server TCP connection timeout (Range 5-240 seconds) 120?
Default client TCP connection timeout (Range 5-240 seconds) 120?
Do you want to modify cache partition [0]? No:
Requested port has been added to cluster 113.3.1.11
Maxweight has been set to 20 for port 80 in cluster 113.3.1.11
```

reach *address*

指定网络调度程序必须能够到达并正确运行的所有主机地址。它可以是服务器地址、路由器地址、主管部门工作站或其它 IP 主机。

address

指定目标 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

实例:

```
add reach
Address to reach [0.0.0.0]?
```

server *cluster-address port# server-address server-weight server-state*

指定群集器中服务器的属性。

cluster-address

指定拥有该服务器的群集器 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

port# 指定运行于该服务器连接上的协议。

有效值: 1 到 65535

缺省值: 80

server-address

指定服务器 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

server-weight

指定执行器的服务器权重。它影响网络调度程序向该特定服务器发送请求的频率。

有效值: 0 到*最大权重*，由 add port 命令指定。

缺省值: 最大权重，由端口命令指定

server-state

在执行器工作时，指定它是否将服务器当作可用的或不可用的。

有效值: 0 (下) 或 1 (上)

缺省值: 1

实例:

```
add server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [35]?
Server state (down=0 up=1) [1]?
```

参数配置限制

表14下面列出了不同项目的限制，用户可以据此配置网络调度程序。

表 14. 参数配置限制

参数	限制
Advisors	每个 2212 8 个
Clusters	每个 2212 32 个
Heartbeats	每个 2212 8 个
Ports	每个群集器 8 个
Reachs	每个 2212 8 个
Servers	在所有配置的群集器下，每个端口号是 128，每个配置后的端口 32 个。
Unique server IP address	每个端口 32 个

Clear

使用 **clear** 命令可以清除全部网络调度程序配置。

语法:

clear

Disable

使用 **disable** 命令可以禁用网络调度程序的功能部件。

语法:

disable advisor . . .
backup
executor
manager

advisor *name port#*

禁用网络调度程序的通告器。

name 指定通告器类型。

其它信息请参阅第96页的表13。

有效值: 0 - 7

缺省值: 0

port# 指定该通告器的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

实例:

```
disable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet) [1]?
1
Port number [0]? 80
```

backup

禁用网络调度程序的备份功能。

实例:

```
disable backup
Backup is now disabled.
```

executor

禁用网络调度程序执行器。禁用了执行等于禁用网络调度程序功能。

实例:

```
disable executor
Executor is now disabled.
```

注: 禁用执行器操作将停止当前正在运行的管理器、通告器和高可用性功能。

manager

禁用网络调度程序管理器。管理器是一个可选项。但是，如果用户不使用管理器，则网络调度程序将基于当前服务器权重使用循环调度法来均衡负载。

实例:

```
disable manager
Manager is now disabled.
```

注: 由于管理器部件对于通告器来说是先决条件，所以禁用管理器操作将停止所有通告器的运行。

Enable

使用 **enable** 命令可以启用网络调度程序功能部件。

语法:

enable advisor . . .
backup
executor
manager

advisor *name port#*

启用网络调度程序的通告器。

name 指定通告器类型。

其它信息请参阅第96页的表13。

有效值: 0 - 7

缺省值: 0

port# 指定该通告器的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

实例:

```
enable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet) [1]?
1
Port number [0]? 80
```

注: 由于管理器部件是通告器的先决条件，所以用户必须在启用任何通告器之前启用管理器。为保证通告器正确运行，用户还必须用 **set internal-ip-address** 命令来设置内部 IP 地址。请参阅*Protocol Configuration and Monitoring Reference Volume 1*，可获得有关 **set internal-ip-address** 命令的详细信息。

backup

启用网络调度程序的备份功能。

实例: **enable backup**

注: 在启用备份前，用户必须增加至少一个脉动

executor

启用网络调度程序执行器。

实例:

```
enable executor
Executor is now enabled.
```

manager

启用网络调度程序管理器。

实例:

```
enable manager
Manager interval was set to 2.
Manager proportions were set to 50 50 0 0
Manager refresh cycle was set to 2
Manager sensitivity was set to 5.
Manager smoothing factor was set to 1.50.
```

当第一次启用管理器时，管理器记录按如下的值创建:

时间间隔: 2 秒

刷新周期: 2

灵敏度: 5 %

平滑: 1.5

容量:

活动的: 50%

新的: 50%

通告器: 0

系统: 0

有关以上参数的介绍，请参阅第107页的『Set』。

List

使用 **list** 命令可以显示网络调度程序的有关信息。

语法:

list all

advisor

backup

cluster

manager

port

server

all 显示网络调度程序的全部配置信息。包括显示通告器、备份、群集器、管理器、端口和服务器的全部信息。

实例:

```
NDR Config> list all

Executor: Enabled

Manager: Enabled

        Interval        Refresh-Cycle   Sensitivity     Smoothing
        2               2               5 %             1.50
        Proportions:    Active  New     Advisor         System
                        50 %    50 %    0 %             0 %

Advisor:
        Name    Port    Interval        TimeOut         State     CommPort
        http    80      5               0               Enabled
        MVS     10007   15              0               Enabled
        TN3270  23      5               0               Enabled   10008
```

```
Backup: Enabled
        Role            Strategy
        PRIMARY         AUTOMATIC

        Reachability:   Address         Mask            Type
                        131.2.25.93     255.255.255.255 HOST
                        131.2.25.94     255.255.255.255 HOST

        HeartBeat Configuration:
           Source Address:  131.2.25.90 Target Address:   131.2.25.92
           Source Address:  132.2.25.90 Target Address:   132.2.25.92

Clusters:
        Cluster-Addr    FIN-count       FIN-timeout     Stale-timer
        131.2.25.91     4000            30              1500

Ports:
  Cluster-Addr    Port#   Weight  Port-Mode  Port-Type
  131.2.25.91     23      20 %    none       TCP
  131.2.25.91     80      20 %    none       Both

Servers:
        Cluster-Addr    Port#   Server-Addr     Weight  State
        131.2.25.91     23      131.2.25.93     20 %    up
        131.2.25.91     23      131.2.25.94     20 %    up
        131.2.25.91     80      131.2.25.93     20 %    up
        131.2.25.91     80      131.2.25.94     20 %    up
```

advisor
显示网络调度程序通告器的配置。

backup
显示网络调度程序的备份设置。

cluster
显示网络调度程序群集器的配置。

manager
显示网络调度程序管理器的配置。

port 显示网络调度程序端口的配置。

server 显示与网络调度程序群集器相关的服务器的配置。

Remove

使用 **remove** 命令可以删除网络调度程序配置的部件。

语法:

remove advisor . . .
backup
cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

advisor *name port#*
从网络调度程序删除特定的通告器。

name 指定通告器类型。

其它信息请参阅第96页的表13。

有效值: 0 - 7

缺省值: 0

port# 指定该通告器的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

实例:

```
remove advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet) [0]?
Advisor port [0]? 80
```

backup

删除高可用性功能。

注: 由于备份是脉动和到达功能的先决条件，所以删除备份操作将停止脉动和到达功能的运行。

实例: **remove backup**

cluster *address*

从网络调度程序配置删除群集器。

address

指定群集器的 IP 地址。

有效值: 任意有效的 IP 地址

缺省值: 0.0.0.0

注: 删除群集器操作也将删除与该群集器相关的所有端口和服务器。

实例:

```
remove cluster
WARNING: Deleting a cluster will make any port or server
         associated with it to also be deleted.
Cluster address [0.0.0.0]? 131.2.25.91
```

heartbeat *address*

从网络调度程序配置删除脉动地址。

address

指定目标网络调度程序的 IP 地址。

有效值: 任意有效的 IP 地址

缺省值: 0.0.0.0

实例:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port#*

从网络调度程序中的特定群集器删除端口。

cluster-address

指定群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

port# 指定该群集器所用协议的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

注: 删除端口操作也将删除与该端口相关的所有服务器。

实例:

```
remove port
WARNING: Deleting a port will make any server
associated with it also be deleted.   [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Cluster address [0.0.0.0]? 20.21.22.15
```

reach *address*

从网络调度程序必须能够到达的主机的列表删除服务器。

address

指定群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

实例:

```
remove reach
Target address [0.0.0.0]? 9.82.142.15
```

server *cluster-address port# server-address*

从群集器和网络调度程序配置中的端口删除服务器。

cluster-address

指定群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

port# 指定该群集器所用协议的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

server-address

指定群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

实例:

```
remove server
Cluster address [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Server address [0.0.0.0]? 20.21.22.15
```

Set

使用 **set** 命令可以更改现有通告器、群集器、端口或服务器的属性。用户也可以定义网络调度程序管理器的属性。

配置网络调度程序

语法:

set advisor . . .
cluster . . .
manager . . .
port . . .
server . . .

advisor *name port# interval timeout comm-port*

更改通告器的端口号、时间间隔和超时。

name 指定通告器类型。

其它信息请参阅第96页的表13。

有效值: 0 - 7

缺省值: 0

port# 指定该通告器的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

interval

指定通告器查询每个服务器协议的频率，以秒为单位。如果经过该时间截止值的一半后仍没有收到服务器响应，则通告器认为协议不可用。

有效值: 0 到 65535

缺省值: 5

timeout

指定通告器认为协议不可用之前的时间间隔，以秒为单位。

为保证管理器在其负载均衡决策中不使用数据溢出的信息，管理器不使用来自时间标记比该参数设置值晚的通告器的信息。通告器超时时间应大于通告器轮询时间间隔。如果超时时间较短，管理器可能会忽略应当使用的通告。缺省情况下，通告器通告不会超时。

该超时值一般应用于用户禁用通告器的情况。请不要将该参数同先前介绍的一半时间间隔的超时混淆，该一半时间间隔的超时与无响应的服务器有关。

有效值: 0 到 65535

缺省值: 0，表示认为协议始终是可用的。

comm-port

指定 TN3270 通告器用来与 TN3270 服务器通信的端口号码。该参数只作为 TN3270 通告器输入。

有效值: 1 到 65535

缺省值: 10008

实例:

```
set advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

cluster *address FIN-count FIN-timeout Stale-timer*

更改网络调度程序配置中群集器的 FIN 计数、FIN 超时和 Stale 定时器。

address

指定群集器的 IP 地址。

有效值: 任意有效的 IP 地址

缺省值: 0.0.0.0

FIN-count

指定 *FIN 超时*或 *Stale 定时器* 时间到后，执行器尝试从网络调度程序数据库删除无用连接信息之前，必须处于 FIN 状态的连接数量。

有效值: 0 到 65535

缺省值: 4000

FIN-timeout

指定执行器尝试从网络调度程序数据库删除无用连接信息前所经过的秒数。

有效值: 0 到 65535

缺省值: 30

Stale-timer

指定执行器尝试从网络调度程序数据库删除无用连接信息前，连接已处于非活动态所经过的秒数。

有效值: 0 到 65535

缺省值: 1500

实例:

```
set cluster
Cluster address [0.0.0.0]? 131.2.25.91
FIN count [4000]? 4500
FIN timeout [30]? 40
Stale timer [1500]? 2000
```

manager *interval proportion refresh sensitivity smoothing*

设置管理器确定满足请求的最佳服务器所使用的值。

interval

指定管理器在对执行器连接负载均衡操作中使用的服务器权重进行更新之前的时间量，以秒为单位。

有效值: 0 到 65535

缺省值: 2

proportion

指定管理器决策中外部因子的相对重要性。容量总和必须等于 100。这些因子是:

active 由执行器跟踪的每个 TCP/IP 服务器上的活动连接的数量。

有效值: 0 到 100

缺省值: 50

new 由执行器跟踪的每个 TCP/IP 服务器上的新连接的数量。

有效值: 0 到 100

缺省值: 50

advisor

从定义给网络调度程序的协议通告器输入。

有效值: 0 到 100

缺省值: 0

system

从由 MVS WLM 系统监视工具提供的 MVS 系统通告器输入。

有效值: 0 到 100

缺省值: 0

refresh

指定管理器从执行器发出状态请求的频率。该参数被指定为*时间间隔*数值。

有效值: 0 到 100

缺省值: 2

sensitivity

指定管理器在对执行器连接负载均衡操作中使用的权重更新之前，端口上所有服务器的权重更改百分率。

有效值: 0 到 100

缺省值: 5

smoothing

指定可更改的服务器权重的数量限制。平滑操作最大限度地减小了发布请求期间的更改频率。平滑索引越高，权重更改越少。平滑索引越低，权重更改越多。

有效值: 1.0 和 42 949 673.00 之间的小数值。

缺省值: 1.5

注: 在小数点后，用户只能指定两个位数。

实例:

```
set manager
Interval (in seconds) [2]? 3
Active proportion [50]? 40
New proportion [50]? 38
Advisor proportion [0]? 20
System proportion [0]? 2
Refresh cycle [2]? 4
Sensitivity threshold [5]? 10
Smoothing index (>1.00) [1.50]? 200
```

port *cluster-address port# port-type max-weight port-mode*

更改端口类型、最大权重、特定群集器的端口模式和端口号。

cluster-address

指定群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

port# 指定该群集器所用协议的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

port-type

指定可在该端口上进行负载均衡的 IP 通信量的类型。

有效值:

tcp=1

upd=2

both=3

缺省值: 3

max-weight

指定该端口上服务器的权重。它影响执行器向每个服务器发出请求的数量之差。

有效值: 0 到 100

缺省值: 20

port-mode

指定端口是否从单一的客户机向单一的服务器 (known as sticky) 传送所有请求，是否使用被动 FTP (pftp) 和 或在该群集器上不使用特定协议 (无)。

有效值:

无=0

sticky=1

pftp=2

缺省值: 0 (无)

实例:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Port type (tcp=1, udp=2, both=3) [0]?
Max. weight (0-100) [20]? 30
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1, pftp=2) []?
```

server *cluster-address port# server-address weight state*

更改群集器中特定服务器的服务器状态和服务器权重。

cluster-address

指定拥有该服务器的群集器的 IP 地址。

有效值: 任意 IP 地址

缺省值: 0.0.0.0

port# 指定该群集器所用协议的端口号。

有效值: 1 到 65535

缺省值: 无。用户必须输入端口号。

server-address

指定服务器 IP 地址。

有效值: 任意有效的服务器地址

缺省值: 0.0.0.0

state 在执行器工作时，指定它是否将服务器当作可用的或不可用的。

有效值: 0 (下) 或 1 (上)

缺省值: 1

weight

指定执行器的服务器权重。它影响网络调度程序向该特定服务器发送请求的频率。

有效值: 0 到*最大权重*，由 add port 命令指定。

缺省值: 最大权重，由端口命令指定

实例:

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]?
Server address [0.0.0.0]?
Server weight [20]? 25
Server state (down=0, up=1) [1]? 1
```

访问网络调度程序监控命令

要访问网络调度程序监控环境，需要:

1. 在 OPCON 提示符 (*) 下输入 **talk 5**。
2. 在 GWCON 提示符 (+) 下输入 **feature ndr**。

也可以使用 SNMP 来监控网络调度程序。有关的详细信息，请参阅*Protocol Configuration and Monitoring Reference Volume 1*中的 『SNMP 管理』。

网络调度程序监控命令

表15对网络调度程序监控命令进行概述，其它章节对这些命令进行解释。这些命令在 NDR > 提示符下输入。

表 15. 网络调度程序监控命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
List	显示通告器、群集器、端口或服务器的当前配置属性。
Quiesce	指定不再向服务器发送连接请求。同时暂时停止脉动和到达功能。

表 15. 网络调度程序监控命令 (续)

命令	功能
Report	显示与通告器和管理器相关的信息报告。
Status	显示计数器、群集器、端口、服务器、通告器、管理器和备份的当前状态。
Switchover	将运行于备份模式的网络调度程序强制为活动的网络调度程序。如果用户将转换模式指定为手动，则有必要使用该命令。
Unquiesce	允许网络调度程序管理器在配置了服务器的每个端口上，给先前停止的服务器指定大于 0 的权重。该操作允许新的连接请求流向选定的服务器。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

List

使用 **list** 命令可以显示关于网络调度程序的信息。

语法:

list advisor
cluster
port
server

advisor

显示网络调度程序通告器的配置。

实例:

```
list advisor
Advisor list requested.

-------------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-------------------------------------------
|  ftp    |    21  |       5   |  ACTIVE  |
|  Http   |    80  | unlimited |  ACTIVE  |
|  MVS    | 10007  | unlimited |  ACTIVE  |
|  TN3270 |    23  | unlimited |  ACTIVE  |
-------------------------------------------
```

cluster

显示网络调度程序群集器的配置。

实例:

```
list cluster
EXECUTOR INFORMATION:
 ---------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
Number of defined clusters: 2

CLUSTER LIST:
-------------
  131.2.25.91
  10.11.12.2
```

port 显示网络调度程序端口的配置。

实例:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91

  ------------------------------------------------------
 nCLUSTER:       131.2.25.91
-------------------------------------------------------n
 n  PORT   n   MAXWEIGHT   n PORT MODE  n PORT TYPE
-------------------------------------------------------n
 n    23   n        30     n   none     n    TCP      n    80
```

```
n        20     n   none     n    both
 ------------------------------------------------------------
```

server 显示与网络调度程序群集器相关的服务器的配置。

实例:

```
list server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0 Active: 0 FIN 0 Complete 0 Status: up S
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0 Active: 0 FIN 0 Complete 0 Status: up S

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0 Active: 0 FIN 0 Complete 0 Status: up S
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0 Active: 0 FIN 0 Complete 0 Status: up S
```

Quiesce

使用 **quiesce** 命令可以临时停止脉动或到达功能，或指定不再向服务器发送连接请求。

语法:

quiesce heartbeat
manager
reach

heartbeat *address*

停止脉动功能选定的路径。*address*是远程网络调度程序的 IP 地址，网络调度程序向该地址发送脉动消息。

实例:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

manager *address*

指定不再向特定服务器发出连接请求。 *address*是服务器的 IP 地址。

实例:

```
quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
```

reach *address*

停止网络调度程序对具体地址的轮询操作，以确定该地址是否可到达，其中*address*是作为可达性标准一部分的 IP 地址。

实例:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

使用 **report** 命令可以显示通告器或管理器报告。

语法:

report advisor

manager

advisor *type port#*

显示有关特定通告器信息的报告。

类型 指通告器类型。有关通告器类型，请参阅第96页的表13。

port# 是端口号码。

实例:

```
report advisor
0=ftp, 1=http, 2=MVS, 3=TN3270, 4=smtp, 5=nntp, 6=pop3, 7=telnet
Advisor name [0]? 1
Port number [0]? 80

------------------------------
|      ADVISOR:     http      |
|      PORT:          80      |
------------------------------
| 131.2.25.93      |       0  |
| 131.2.25.94      |      16  |
------------------------------
```

manager

显示当前管理器信息的报告。

实例:

```
report manager

----------------------------------
|  HOST TABLE LIST  |   STATUS   |
----------------------------------
|  131.2.25.93      |    ACTIVE  |
|  131.2.25.94      |    ACTIVE  |
----------------------------------

-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------|
|PORT:   23     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
-------------------------------------------------------------------------------
|131.2.25.93    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
-------------------------------------------------------------------------------
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |     0|    |    -2|
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------|
|PORT:   80     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
-------------------------------------------------------------------------------
|131.2.25.93    | 10| 10|  10|        0|  10|        1|  16|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        1|   3|    16|-999|    -1|
-------------------------------------------------------------------------------
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |    16|    |    -2|
-------------------------------------------------------------------------------


-----------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-----------------------------------------
```

```
| http   |    80 | unlimited |   ACTIVE |
| MVS    | 10007 | unlimited |   ACTIVE |
-------------------------------------------
Manager report requested.
```

Status

使用 **status** 命令可以获得通告器、备份、计数器、群集器、管理器、端口和服务器的状态。

语法:

status advisor
backup
cluster
counter
manager
ports
servers

advisor *name port#*

获取特定通告器的状态。

name 指定通告器类型。有关通告器类型，请参阅第96页的表13。

port# 是端口号码。

实例:

```
status advisor
0=ftp, 1=http, 2=MVS, 3=TN3270, 4=SMTP, 5=NNTP, 6=POP3, 7=TELNET
Advisor name [0]?
Port number [0]? 21

Advisor ftp on port 21 status:
==============================
Interval.................. 10
```

backup

获取备份功能的状态。

实例:

```
status backup
 Dumping status ...
 Role : PRIMARY   Strategy : AUTOMATIC  State : ND_ACTIVE Sub-State : ND_SYNCHRONIZED
 <<Preferred Target : 132.2.25.92>>

 Dumping HeartBeat Status ...
 .....Heartbeat target : 131.2.25.92 Status : UNREACHABLE
 .....Heartbeat target : 132.2.25.92 Status : REACHABLE

 Dumping Reachability Status ...
 .....Host:131.2.25.93   Local:REACHABLE
 .....Host:131.2.25.94   Local:REACHABLE
```

cluster *address*

获取指定群集器的状态，其中*address*是群集器的 IP 地址。

实例:

```
status cluster
Cluster Address [0.0.0.0]? 131.2.25.91

EXECUTOR INFORMATION:
 ---------------------
```

```
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996

CLUSTER INFORMATION:
 --------------------
Address..................... 131.2.25.91
Number of target ports..... 2
FIN clean up count.............. 4000
Connection FIN timeout..... 30
Active connection stale timer... 1500

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port type....................... BOTH
Port mode....................... NONE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
```

counter

获取所有计数器的状态。

实例:

```
status counter
Internal counters from executor:
--------------------------------
Total number of packets into executor...... 2684
Total packets for cluster processing (C)... 2684
Packets not addressed to a cluster(port)... 0

Cluster processing results:
---------------------------
Errors...................................... 0
Discarded................................... 0
Forward requested........................... 2684
Forward requested........................... 0
Forward discarded with error................ 0

Other processing problems:
--------------------------
Total packets dropped (C).................. 0
```

manager

获取管理器的状态。

实例:

```
status manager
Number of defined hosts... 2
Sensitivity............... 0%
Smoothing factor.......... 2
Interval.................. 3
Weights refresh cycle..... 4

Active connections gauge proportion......... 40%
New connections counter(delta) proportion... 38%
Advisor gauge proportion.................... 20%
System Metric proportion....................  2%

Manager status requested.
```

port *cluster-address port#*

获取特定端口的状态，其中:

cluster-address

是群集器的 IP 地址。

port# 是群集器上的端口号。

实例:

```
status port
Cluster Address [0.0.0.0]? 131.2.25.91
Port number  [0]? 80

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP count 2345 Active: 3431 FIN 3780 Complete
Address: 131.2.25.94 Weight: 20 Count: 7890  Active: 2980 FIN 2390 Status: up Saved Weight: -1
```

server *address*

获取特定服务器的状态，其中*address*是拥有该服务器的群集器的 IP 地址。

实例:

```
status server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 140 TCP Count: 100 UDP Count: 40  Active: 50 FIN 45 Complete 50  Stat
Address: 131.2.25.94 Weight: 20 Count: 250 TCP Count: 100 UDP Count: 40  Active: 60 FIN 54 Complete 50  Stat

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP Count: 2345  Active: 3431 FIN 3780 Complet
Address: 131.2.25.94 Weight: 20 Count: 7890  TCP Count: 10000 UDP Count: 2345  Active: 2980 FIN 2390 Complet
```

Switchover

当转换策略为手动时，可以使用 **switchover** 命令将运行于备份模式的网络调度程序强制为活动的网络调度程序。该命令必须在运行备份模式的网络调度程序的主机上输入。

语法:

switchover

Unquiesce

使用 **unquiesce** 命令可以重新启动先前用 **quiesce** 命令停止的脉动、管理器或到达功能。

语法:

unquiesce heartbeat

manager

reach

heartbeat *address*

重新启动脉动消息路径，其中*地址*是该网络调度程序将脉动消息发送到的远程网络调度程序的 IP 地址。

实例:

```
unquiesce heartbeat
Remote Address [0.0.0.0]? 9.10.11.1
```

manager *address*

重新向指定服务器发送连接请求。 *address*是该服务器的 IP 地址。

实例:

```
unquiesce manager
Server Address [0.0.0.0]? 20.21.22.15
```

reach *address*

重新启动网络调度程序对具体地址的轮询，以确定该地址是否可到达，其中*address*是作为可达性标准一部分的 IP 地址。

实例:

```
unquiesce reach
Reach address [0.0.0.0]? 20.3.4.5
```

第10章 使用数据压缩子系统

本章讨论在 2212 上通过帧中继和 PPP 接口进行数据压缩。包括以下部分:

- 『数据压缩概述』
- 『数据压缩的概念』

帧中继和 PPP 接口支持数据压缩。

数据压缩概述

数据压缩系统提供一种增大设备网络接口有效带宽的方法。它主要用于速度较慢的 WAN 链路。

PPP 和帧中继接口支持在此设备上的数据压缩:

- 对于 PPP 接口，压缩是根据 Internet 工程任务部 RFC 1962 中定义的压缩控制协议 (CCP) 实施的。CCP 提供协商使用压缩的底层机制，并提供在多个可能压缩算法或协议中加以选择的方法。

  此设备提供两个压缩协议: RFC 1974 中定义的 Stac-LZS 协议; RFC 2118 中描述的 Microsoft 点到点压缩协议 (MPPC)。这两个协议均基于 Stac Electronics 提供的压缩算法。
- 对于帧中继接口，压缩是根据帧中继技术论坛委员会通过的 FRF.9, *帧中继数据压缩实施协议*实施的。FRF.9 描述数据压缩协议 (DCP), 它是参考 PPP 的 CCP 制定的，同样也提供了协商各种压缩算法和压缩选项的方法。此设备支持 DCP 『mode 1』 协商。FRF.9 还描述了一个更普遍的模式, 『mode 2』; 但在此不支持这一模式。使用与 PPP Stac-LZS 协议相同的压缩引擎可完成自压缩。

数据压缩的概念

设备上的数据压缩通过更有效地使用链路上的可用带宽，增大了网络链路的吞吐量。其基本原理十分简单: 在链路速度给定的情况下，如果以最大可能压缩通过链路的数据流，则数据流的传输时间便会降至最低。

数据压缩可以在网络模型的许多层上执行。在“频谱”的一端，是应用程序先压缩数据，然后再将它传给网络其它地方的对等应用程序，而在“频谱”的另一端，则是设备在数据链路层执行压缩，处理两节点间的纯位流传送。压缩如何完成、效率如何取决于各种因素，包括在哪一层网络层进行压缩，压缩器和解压缩器对正在压缩的数据有多少固有认识，选取的压缩算法以及实际压缩的数据。最好的压缩位置通常是在应用层: 例如，文件传输应用程序通常有这样的优势，即压缩数据前，可以先获得整个数据文件，然后可以对文件尝试不同的压缩算法，看哪一种方法更适合压缩此特殊文件的数据。尽管这可能为这种类型的应用文件会有极佳的压缩效果，但却不能解决在网络上压缩大量通信数据这一普遍问题。因为大多数联网的应用程序无法在生成数据的同时压缩数据。

设备压缩发生在更低的网络层，即数据链路层。对于此设备，压缩是针对通过链路传输的的单个包进行的。在包流经此设备时进行实时压缩：即发送方在传送包之前先压缩它，解压缩器一接到包便解压缩。此操作对高层联网协议是透明的。

数据压缩的基本内容

数据压缩器的工作原理是识别数据中的『冗余』信息，然后生成另一个包含最少冗余信息的数据集。『冗余』信息是基于当前可用数据衍生和重新生成的信息。例如，某个压缩器的工作原理可能是识别数据流中重复的字符模式，然后将这些重复的字符模式用较短的代码序列来代替。只要压缩器与解压缩器对这些代码序列表示的内容取得一致，解压缩器就总能从压缩数据中重建原始数据。

原始数据中的序列与压缩输出中相应序列的映射通常称为***数据词典***。这些词典可能是静态定义的 - 基于经验性的、可用于压缩和解压缩器的信息，或者也可能是通常根据正在压缩的信息动态生成的信息。当要处理的数据具有有限的周知属性，而普通压缩器处理这些数据又不十分有效时，静态词典最为适用。大多数的压缩系统，包括此设备使用的所有压缩器，使用的都是动态词典。在 2212 上，数据词典以当前正在处理的包和以先前看到过的包为基础，但是，对于执行压缩时在其它层上存在的数据流，它没有在数据流中『向前查看』的能力。对于数据词典动态生成并且只基于先前看到的数据的那些系统，此词典通常称作***历史***。 尽管在其它环境中历史只是数据词典的一种特定形式，但在本章中，这两个词汇可以互换使用。

设备使用动态词典，压缩器和解压缩器必须保持词典同步，这一事实表明数据压缩是在两个端点之间的数据流上工作的。因此，路由器上的压缩是一个面向连接的进程，连接的两端便是压缩器和解压缩器。开始对数据流进行压缩时，两端将数据词典重置为某个已知起始态，接收到数据后，再同时进行更新。

可以对每一个包实施压缩，处理每个包之前应重设历史。但是，通常在处理包的过程中不重置数据词典，这说明历史不仅基于当前包的内容，还基于前面看到的包的内容。这通常能够提高总的压缩率，因为它增加了压缩器搜索的可删除冗余数据的数据量。例如，一个主机通过 IP 『探测』另一个主机时，它将发送一系列的包，而每一个包又几乎都与最后发送的包相同。压缩器可能难于对第一个包实施压缩，但它可能识别出每一个序列包与刚发送的包非常相似，于是便可以生成这些包的高度压缩版本。

因为压缩器和解压缩器历史随接收到的包而更改，所以压缩机制对丢失、破坏或重排包很敏感。设备采用的压缩协议包括信号机制，使用该机制后，压缩器和解压缩器可以检测到同步丢失，并能相应地实现双方的再同步，例如，因传输失误而丢失包时便需要使用此信号机制进行再同步。典型作法是，可以在每一个包中包括一个序列号，解压缩器检查以确保它按顺序接收了所有的包。如果解压缩器检测到错误，它将复位到某个已知起始态，并发出信号通知压缩器作类似调整，废弃入网的压缩包，然后等待直至压缩器确认其已复位。

一般情况下，典型的链路上的压缩是对从链路两个方向进入的数据进行压缩。通常，连接的每一端都有一个压缩器运行和一个解压缩器在运行，它们分别与另一连接端的模拟部件进行通信，如第123页的图9所示。输出方(压缩)独立于输入方(解压缩)运行。在链路的每个方向上可以实施完全不同的压缩算法。建立链路连接后，链路的压缩控制协议将与对等方协商使用哪种压缩算法。如果连接的双方在使用压缩协议上未达成一致，则不实施压缩，链路正常操作- 包将以未压缩形式发送。

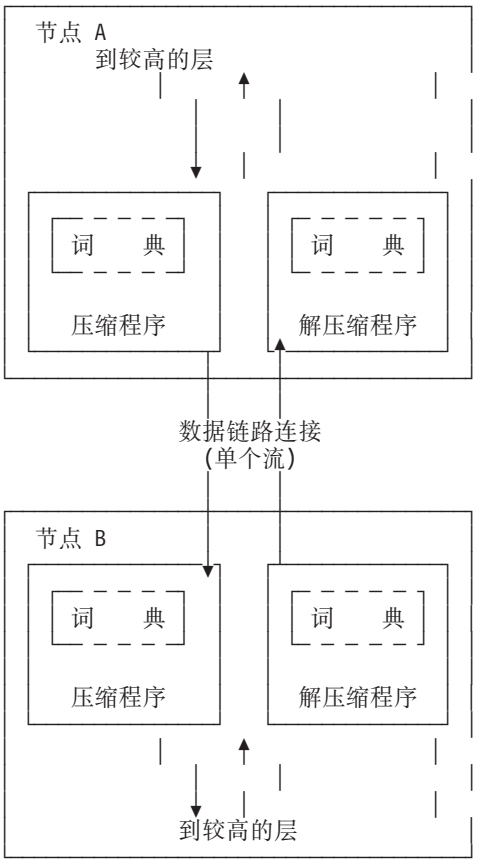


图 9. 使用数据词典进行双向数据压缩的实例

流实际代表链路一端的特定压缩进程与另一端相应的解压缩进程之间的连接，它比两个节点之间的『连接』更具体；复杂的压缩协议可以将两个主机之间的数据流分成多个流，并分别压缩这些流。例如，PPP 的 CCP 能够协商在单个 PPP 链路上使用多个历史，但此路由器对此并不支持。

注意事项

选择是否使用数据压缩不是一个简单的问题。对连接启用压缩之前，应考虑几个因素。

CPU 负荷

数据压缩是一个非常消耗计算能力的进程。随着要压缩的数据的增多(每单位时间)，加载到此设备处理器上的负荷也会相应加大。如果负荷增加过大，此设备的性能则会降低 - 体现在所有网络接口上，而不仅仅是执行压缩的设备。

此设备实际包含多个处理器，使用的是非对称多机处理 - 例如，链路 I/O 控制器，该控制器通过汇接方式与主处理器协调工作 - 因此，处理器负荷影响并非总能够方便地测量到。因为压缩进程可能是与包传输进程并行，因此负载实际上可能是完全透明的，不会带来任何问题。但是，不管如何，这可能会引起设备处理器超载或性能降低。

通常情况下，只在低速的 WAN 链路上才可启用压缩 - 可能只限于速度低于 64 千比/秒的链路(典型的 ISDN 拨号链路速度)。在所有链路上给予压缩数据的总带宽大致限制在几百千比特每秒左右。在 ISDN 主速率适配器所有信道上运行压缩不是一个明智之举。

使用某些设备配置参数可以限制能同时运行压缩的连接的数目。启用的接口可以比实际执行压缩的接口多。一旦达到活动压缩连接的数目限额，则其后的连接将协商不再使用压缩，这种情况至少要持续到有某些现存的压缩链接关闭为止。

内存占用

配置压缩时的另一个要注意的事项是所需的内存。压缩和解压缩历史占用一定的内存，内存是此设备的一个有限资源。例如，Stac-LZS 算法要求大约 16 千字节用于压缩历史，大约 8 千字节用于解压缩历史。由于每个建立的连接都必须存有这些历史，因此这一问题变得更为严重：在对等路由器中，压缩历史与相应的解压缩历史同步。对于 PPP 链接，指一个压缩历史和一个解压缩历史(假定数据压缩在链路上双向运行)。对于帧中继链接，可能需要更多这样的历史，其中每建立一个虚拟连接 (DLC1) 便需要一对历史。

此设备在引导时会分配一定数目的压缩和解压缩历史。并且总是成对分配，称作***压缩上下文*** - 上下文就是一个压缩历史配一个解压缩历史。从技术方面考虑，压缩和解压缩是独立的功能，其历史的指定也可分别执行。但实际上，压缩几乎总是双向运行，因此作为一种简化方式，用上下文替代个别的历史来管理和配置内存。给每一上下文分配 24 千字节，包括压缩和解压缩历史所需内存。

此设备试图在一个链路上建立压缩连接时，它总是首先从分配的上下文池中保留一个上下文。如果无上下文可用，则此连接不实施压缩。稍后，一旦上下文变为可用，路由器则尝试启动此连接上的压缩。

分配的压缩上下文数是一个可配置的参数。设置分配的上下文数目，以限制使用的内存量，和可同时执行压缩的连接数。限制同时操作的压缩连接数，可帮助控制 CPU 负载问题。

数据内容

应当在启用连接压缩前，考虑到连接中正在传输的数据的实质。对于某些类型的数据，其压缩效果要比其它类型更好。包含大量几乎相同信息的包 - 如 IP 『ping』 命令产生的一组包 - 其压缩效果通常极佳。在链路上传输的典型的随机文本和二进制数据，通常的压缩比大约是 1.5:1 到 3:1。某些数据根本无法实现良好压缩。特别是，数据经压缩后，很少能进一步压缩。实际上，先前压缩过的数据通过压缩引擎时还可能扩展。

如果预先能够知道连接上流通的大部分数据已经过压缩，则建议不要在此连接中使用压缩。可能发生的实例之一便是与主机的连接，此主机主要作为一个 FTP 文件归档站点，所有适合传输的文件以压缩形式存储在上面。

链路层压缩

最后一个要考虑的因素是两个主机之间网络链路的性质。压缩可以在更低层，甚至比设备硬件接口还低的层上执行。特别是，许多现代的调制解调器在其硬件和固件中装有数据压缩机制。如果正在一个低层(此设备外)的链路上实施压缩，建议最好不要在此

接口的设备上使用压缩。前面提到过，压缩一个已经过压缩的数据流通常是无效的，并且还可能略微降低设备性能。除非有理由相信此路由器执行压缩的效果比链路硬件更好，否则还是应使用链路硬件执行压缩。

在 PPP 链路上使用数据压缩

2212 使用 PPP 压缩控制协议 (CCP) 协商在链路上使用压缩。CCP 提供一个普遍性机制协商使用特定压缩协议，甚至可以在链路的各个方向使用不同的协议及协议专用的各种选项。此软件支持 Stac-LZS 和 MPPC 协议，因此对等实体也必须至少支持其中的一个算法，以成功协商两个节点之间的数据压缩。这两个节点还必须在算法专用选项上一致，以保证压缩执行。

在 PPP 链路上配置数据压缩

要在 PPP 链路上配置数据压缩:

1. 发出 **enable ccp** 命令，在链路上启用 CCP 协议。链路因此可与其它节点协商压缩。协商内容包括使用何种压缩协议，和所有的协议专用选项。
2. 发出 **set ccp protocols** 命令，选取要协商的压缩协议。
3. 发出 **set ccp options** 命令，为每个压缩协议设置可协商参数。

使用 **list ccp** 命令可显示当前压缩配置。

表16列出可用的命令，图10是在 PPP 链路上配置压缩的一个例子。有关这些命令的详细说明，请参阅‘点到点配置命令’(*Access Integration Services 软件用户指南* 中)。

表 16. PPP 数据压缩配置命令

数据压缩命令	操作
disable ccp	禁用数据压缩。
enable ccp	启用数据压缩。
set ccp options	设置压缩算法选项。
set ccp algorithms	指定一个压缩协议的优先级列表。
list ccp	显示压缩配置。

```
Config> network 1 1

Point-to-Point user configuration
PPP Config> enable ccp
PPP Config> set ccp options 2
STAC: # histories [1]? 1
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]? 3
PPP Config> list ccp
CCP Options
-----------

Data Compression enabled
Algorithm list: STAC-LZS
Stac:  histories 1
Stac:  check_mode SEQ
```

图 10. 在 PPP 链路上配置压缩实例

注:

1. 此网络命令选取 PPP 链路的网络接口。如果此链路是 PPP 拨号线路，还必须使用 **encapsulator** 命令，进入 PPP 配置菜单。
2. 如果启用 CCP，但没有给链路设置协议，则软件自动设置链路使用协议 STAC 和 MPPC，就好象已输入 **set ccp protocols stac mppc** 命令一样。

   如果设置了多个协议，则协议的顺序决定链路的协商喜好设置。
3. 如果输入命令 **set ccp protocols none**，此软件将自动禁用在链路上的进行压缩。

下列显示的是 talk 5 **list ccp** 命令的输出，且已配置 Microsoft 点到点加密 (MPPE)。配置 MPPE 则能启用 MPPC 压缩。有关配置 MPPE 的指导，请参阅*Access Integration Services 软件用户指南*中『配置和监控点到点协议接口』一章。

```
PPP> list ccp
CCP Options
-----------

Data Compression : Enabled
Algorithm list : MPPC
STAC histories : 1
STAC check_mode: SEQ

MPPE Options
------------

MPPE enabled
Mandatory encryption
Key generation : STATEFUL
```

监控 PPP 链路上的压缩

监控压缩的方法和监控其它 PPP 组件相同。*Access Integration Services 软件用户指南*中的 ‘访问接口监控进程’说明了如何进入 PPP 控制台环境和命令的详情。表17列出与压缩有关的命令。第127页的图11显示列出 PPP 接口上压缩的一个实例。

表 17. PPP 数据压缩监视命令

命令	功能
list control ccp	列出 CCP 状态和协商的选项。
list ccp	列出 CCP 包统计信息。
list cdp 或 **list compression**	列出压缩数据报的统计信息。

```
+ network 1
PPP > list control ccp

CCP State:                Open
Previous State:           Ack Sent
Time Since Change:        2 minutes and 52 seconds

Compressor:   STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ
MPPE:         Not negotiated

PPP > list ccp

CCP Statistic             In                        Out
-------------             --                        ---

Packets:                  2                         3
Octets:                   18                        27
Reset Reqs:               0                         0
Reset Acks:               0                         0
Prot Rejects:             1                         -

PPP > list cdp

Compression Statistic     In                        Out
---------------------     --                        ---

Packets:                  19541                     19542
Octets:                   2550673                   2740593
Compressed Octets:        821671                    899446
Incompressible Packets:   0                         0
Discarded Packets:        0                         -
Prot Rejects:             0                         -
Compression Ratios:       3.11                      3.24
```

图 11. 监控 PPP 接口上的压缩

在帧中继链路上使用数据压缩

配置全局压缩参数并在接口上启用压缩后，还必须为帧中继接口上的每一条线路 (PVC) 设置参数。定义给接口的每一个线路可能已启用压缩，每一个成功协商使用压缩的线路使用来自全局池中的一个压缩上下文。除此之外，还可以禁用接口上的压缩，这意味着接口上将没有一条线路适合运载经过压缩的数据通信。

在帧中继链路上配置数据压缩

要在 FR 链路上配置数据压缩:

1. 使用 **enable compression** 命令启用此接口上的压缩。链路因此可与其它节点协商压缩。
2. 使用 **add permanent-virtual-circuit** 命令，启用用来运载压缩数据的每一个新 PVC 上的压缩进程。通过 **change permanent-virtual-circuit** 命令可更改现有 PVC。

使用 **list lmi** 或 **list permanent-virtual-circuit** 命令可显示当前压缩配置。

第128页的表18列出帧中继链路上用来配置压缩的命令，第128页的图12 是一个配置帧中继链路的例子。请参阅*Access Integration Services 软件用户指南*中的‘帧中继配置命令’以获得详细说明。

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Maximum number of run-time compression PVCs (zero means no limit) [0]?
0
Do you want orphan PVCs to perform compression [Y]? n
The number of currently defined non-compression PVCs is 4
Would you like to change them all to compression PVCs [N]? y

FR Config> add perm

Circuit number [16]? 22
Committed Information Rate (CIR) in bps [65536]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? cir22
Is circuit required for interface operation [N]?
Do you want to have data compression performed [Y]?

FR Config>list lmi

                        Frame Relay Configuration


  LMI enabled            =      No  LMI DLCI                      =       0
  LMI type               =    ANSI  LMI Orphans OK                =     Yes
  CLLM enabled           =      No  Timer Ty seconds              =      11

  Protocol broadcast     =     Yes  Congestion monitoring         =     Yes
  Emulate multicast      =     Yes  CIR monitoring                =      No
  Notify FECN source     =      No  Throttle transmit on FECN     =      No

  Data compression       =     Yes  Orphan compression            =      No
  Compression PVC limit  =    None  Number of compression PVCs    =       2

  PVCs P1 allowed        =      64  Interface down if 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                =      12
  IR % Decrement         =      25  DECnet length field           =      No
  Default CIR            =   65536  Default Burst Size            =   64000
  Default Excess Burst   =       0

FR Config>list perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       2

             Circuit                Circuit   Circuit     CIR    Burst  Excess
              Name                  Number     Type      in bps  Size   Burst
---------------------------------- ------- ----------- ------- ------- -----
 circ16                              16    @ Permanent   65536   64000       0
 cir22                               22    @ Permanent   65536   64000       0

* = 线路是必需的
# = 线路是必需的, 并且属于必需的 PVC 组
@ = 可执行数据压缩的线路
```

图 12. 在帧中继链路上配置压缩实例

表 18. 数据压缩配置命令

命令	操作
add permanent-virtual-circuit #	用于启用接口上定义的特定 PVC 上的数据压缩
change permanent-virtual-circuit #	用于更改特定 PVC 是否将压缩数据。
disable compression	禁用数据压缩。
enable compression	启用数据压缩。
list lmi	显示接口的当前配置。
list permanent	列出线路的摘要信息。

注: 启用孤立线路上的压缩将减少此设备本地 PVC 的可用压缩上下文的数目。

如果启用帧中继接口上的压缩，而此接口早已启用压缩，则软件将询问用户，是否想更改接口上的压缩参数，具体如下面所示。您可以不通过禁用压缩而更改接口上的压缩状态。

更改帧中继接口上压缩的实例

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Data compression already enabled.
Do you wish to continue and change an interface parameter [Y]
Maximum number of run-time compression PVCs (zero means no limit) [0]?
32
Do you want orphan circuits to perform compression []?
Do you want to change the compression capability of all of your existing PVCs [N]?
```

在帧中继链路上监控数据压缩

监控压缩的方法与监控其它帧中继组件相同。*Access Integration Services 软件用户指南*中的帧中继监控命令描述了如何进入帧中继控制台环境，以及这些命令的详细说明。 表19列出与压缩相关的命令。 『监控帧中继接口或线路上压缩的实例』是在帧中继接口上列出压缩的一个实例。

表 19. 帧中继数据压缩监控命令

命令	显示
list lmi	列出接口的当前状态。
list permanent	列出线路的摘要信息。
list circuit	列出线路的当前状态。

监控帧中继接口或线路上压缩的实例

```
+ network 2
FR 2 > list lmi

Management Status:
  ------------------

    LMI enabled          =      No  LMI DLCI                   =       0
    LMI type             =    ANSI  LMI Orphans OK             =     Yes
    CLLM enabled         =      No

    Protocol broadcast   =     Yes  Congestion monitoring      =     Yes
    Emulate multicast    =     Yes  CIR monitoring             =      No
    Notify FECN source   =      No  Throttle transmit on FECN  =      No
    PVCs P1 allowed      =      64  Interface down if no PVCs  =      No
    Line speed (bps)     =   64000  Maximum frame size         =    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          =   65536  Default Burst Size         =   64000
    Default Excess Burst =       0

    Current receive sequence  =       0
    Current transmit sequence =       0
    Total status enquiries    =       0  Total status responses   =       0
    Total sequence requests   =       0  Total responses          =       0

    Data compression enabled  =     Yes  Orphan Compression       =      No

    Compression PVC limit     =    None  Active compression PVCs  =       1

  PVC Status:
  -----------
```

```
    Total allowed  =      64  Total configured  =       1
    Total active   =       1  Total congested   =       0
    Total left net =       0  Total join net    =       0


FR 2 > list permanent

 Circuit                                  Orphan  Type/   Frames      Frames
 Number            Circuit Name           Circuit State Transmitted  Received
 ------- -------------------------------- ------- ----- ----------- --------

     16  circ16                             No   @ P/A        58364      58355
     22  circ22                             No   & P/A        58364      58355

    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


FR 2 > list circuit 22

 Circuit name = circ22

     Circuit state        =    Active  Circuit is orphan   =           No
     Frames transmitted   =     58391  Bytes transmitted   =      2676894
     Frames received      =     58383  Bytes received      =      2671009
     Total FECNs          =         0  Total BECNs         =            0
     Times congested      =         0  Times Inactive      =            0
     CIR in bits/second   =     65536  Potential Info Rate =        64000
     Committed Burst (Bc) =     64000  Excess Burst (Be)   =            0
     Minimum Info Rate    =     16000  Maximum Info Rate   =        64000
     Required             =        No  PVC group name      =   Unassigned

     Compression capable  =       Yes  Operational         =          Yes
     R-R's received       =         0  R-R's transmitted   =            0
     R-A's received       =         0  R-A's transmitted   =            0
     R-R mode discards    =         0  Enlarged frames     =            0
     Decompress discards  =         0  Compression errors  =            0
     Rcv error discards   =         0

     Compression ratio    =  1.00 to 1  Decompression ratio =    1.00 to 1

     Current number of xmit frames queued                  =            0
     Xmit frames dropped due to queue overflow             =            0
```

第11章 配置并监视数据压缩

在 2212 上配置数据压缩的进程分为两步。核心压缩系统是软件的一个『功能部件』。用户可通过选择配置中的 CMPRS 功能部件并监视路由确定程序中的 GWCON 和 CONFIG 进程来设置并监视全局参数。除了配置全局参数，还必须为每个网络接口 (PPP 或帧中继)配置数据压缩，在这些网络接口上将传输压缩的数据通信。

本节说明了对压缩功能部件的配置和监视,以及在 PPP 和帧中继接口上对压缩的配置和监视。

配置压缩功能

压缩功能部件唯一可配置的参数是此设备引导时分配的压缩上下文数。可用的上下文数限定了可同时激活的连接数，同时也决定了为压缩历史记录保留的内存量。如将上下文数设置为 0，则将在所有接口上禁用压缩。

在配置过程中，在 Config > 提示处输入 **feature cmprs**，可执行压缩配置命令。要更改所分配的上下文数，可使用 **SET MAXCONTEXTS *n*** 命令，此处 ***n*** 是上下文数。要查看当前的配置，可使用 **list** 命令。在表20中汇总了所有配置命令设置，配置实例可参见图13。

```
Config> feature cmprs

Data Compression Global Configuration
CMPRS Config> ?
LIST
SET
EXIT

CMPRS Config> set ?
MAXCONTEXTS

CMPRS Config> set maxcontexts
Number of compression contexts to allocate? (0 - 1000) [0]?
10

CMPRS Config> list
Number of compression contexts to allocate: 10
```

图 13. 配置压缩功能

表 20. 压缩配置命令

命令	操作
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
List	显示 maxcontexts 的当前设置。
Set	设置所有接口可用的压缩上下文的最大数。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

List

使用 **list** 命令可显示 *maxcontext* 的当前设置。

语法:

list

Set

使用 **set** 命令可设置同时压缩数据的最多接口数。

语法:

set maxcontexts *n*

maxcontexts *n*

设置接口可用的最大压缩上下文数。该参数使此设备为压缩上下文分配一个内存池。如将 maxcontext 设置为 0，则即使在接口上启用压缩，也不会压缩数据。

注: 将该值设置过高，将占用过多的内存并会减少设备的通信量。

缺省值: 0

有效值: 0 到 1000

实例: **set maxcontexts**

```
Number of compression contexts to allocate? (0-1000)? [0]? 10
```

监视压缩功能

在监视过程中，在 + 提示处输入 **feature cmprs**，以执行压缩监视命令。 表21列出了可用的命令。

表 21. 压缩监视命令

命令	操作
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
List	列出正在使用的内存和上下文。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

List

使用 **list** 命令可列出正在使用的内存或上下文。

语法:

list all

contexts usage

memory usage

all 显示正在使用的上下文、使用上下文的接口以及内存使用统计数字。输出显示列出了上下文的使用和内存的使用情况。

实例: **全部列出**

context usage

显示接口当前分配的所有压缩上下文。可从显示中看出哪些接口当前正在压缩数据通信。

实例: 列出上下文的使用情况

```
Compression System Context (Data Dictionary) Usage
--------------------------------------------------

    CTX  Net Interface   Channel   Status
    ---  --- ----------  --------- --------------------
      0    2  FR/0              16 In use
      1    1  PPP/0              1 In use

Total: 10     Free: 8     In Use/Reserved: 2
```

CTX 上下文的编号，它是上下文的识别标签。此设备在引导时将创建一个上下文池，并为池中的每个上下文分配一个编号。设备上下文数也会在某些与压缩关联的 ELS 消息中显示。

Net 它表示分配给特定上下文的网络接口编号。

Interface

它表示网络接口的名称。

Channel

是区别分配到一个网络接口的多个上下文的标识符。网络编号和通道编号一起唯一标识出单一的压缩流。对于 PPP 链接，链路中只有一个压缩数据流，所以该数字将永远为 1。对于帧中继链接，该数字表示传送压缩通信的特定电路的虚拟电路编号 (DLCI)。

Status

该字节指明上下文的当前状态，通常为 『In use』。有时状态可为『Defunct』，表示链接压缩已结束，但上下文还未释放到池中，不能让其他压缩使用。

memory usage

显示压缩功能当前状态的基本统计信息。输出显示所分配的压缩上下文数，当前正在使用的上下文数，上下文必需的内存量和为压缩上下文保留的内存总量。

实例:

列出内存使用情况

```
Compression System Memory Usage Statistics
-------------------------------------------

Number of contexts allocated:            0 *        in use: 0
Size of compression context:             24624
   = Max compression history size:       16396
   + Max decompression history size:     8200
   + Overhead:                           28
Total memory allocated for contexts:     0

* Compression is disabled due to inability to allocate
  the requested number of contexts (500).
```

配置数据压缩

第12章 使用本地或远程认证

认证过程是确定用户(或实体)的过程。在 2212 上验证用户对 PPP 协议的访问可以增强用户概要文件管理的灵活性，这是由于用户概要文件与 PPP 认证协议 PAP、MSCHAP、CHAP 和 SPAP 关联。请参阅 *Access Integration Services 软件用户指南* 中的'PPP 认证协议'以获取有关配置 PAP、MSCHAP、CHAP 和 SPAP 的其他信息。

可以在本地配置认证，也可以使用网络中的认证服务器将其配置为合并用户配置，此认证服务器可用于为整个网络提供认证请求。 IBM 2212 在本地维护认证和以下认证服务器协议:

- Radius
- TACACS
- TACACS+

使用认证、授权和记帐 (AAA) 安全

认证、授权和记帐 (AAA) 安全是可配置协议,允许用户控制对服务的访问。可以将 AAA 配置为本地认证，也可以配置为远程认证。

可以为以下三种类型的功能配置安全协议。

- PPP 链接
- 注册用户 (Telnet /控制台注册)
- 隧道

可以通过设置主服务器和辅服务器来完成该项配置。服务器信息将在 AAA 配置之外单独进行配置和保存。使用的服务器概要文件名称在配置时提供。

在任何情况下都不能在本地记帐，记帐必须是 Radius 或 TACACS+。

只能在本地或是通过 Radius 或 TACACS+ 远程认证进行授权。

什么是 AAA 安全?

AAA 安全是此设备安全系统的名称。它包括:

认证 标识用户的过程。认证访问时使用的是名称和口令。

授权 确定用户可访问的服务的过程。授权处理时可能会发现用户未被授权，随后授权代理将提出问题，确定未授权的用户是否可以访问这些服务。

记帐 当用户开始或停止会话时的记录过程。支持两种帐户记录类型。

开始记录
表明即将开始一项服务。

停止记录
表明服务已终止。

使用 PPP

对于点对点协议 (PPP)，可以配置以下功能:

- 认证
- 授权
- 记帐

每一功能均都有各自独立配置的安全协议。

- 设置认证协议对授权或记帐均无影响。
- 设置授权协议对认证或记帐均无影响。
- 设置记帐协议将对认证和授权均无影响。
- 将 AAA 设置为远程，则会将认证设置为远程、授权设置为远程并将记帐设置为远程。
- 将 AAA 设置为本地，则会将认证设置为本地、将授权设置为本地并将记帐设置为忽略。不能禁用认证或授权。

有关在该环境中使用的 PPP 配置命令的详细信息。请参阅 *Access Integration Services 软件用户指南*中的 点到点配置命令。

有效的 PPP 安全协议

以下是有效的 PPP 安全协议:

认证方式
本地、RADIUS、TACACS+、TACACS

授权方式
本地、RADIUS、TACACS+

记帐方式
RADIUS、TACACS+

表 22. 设置 PPP 安全协议

操作	认证	授权	记帐
设置 AAA 为本地	本地	本地	忽略
设置 AAA 为远程	远程	远程	远程
设置 AUTHENT 为本地	本地	忽略	忽略
设置 AUTHOR 为本地	忽略	本地	忽略
设置 AUTHENT 为远程	远程	忽略	忽略
设置 ACCOUNTING 为本地	n/a	n/a	n/a
设置 AUTHOR 为远程	忽略	远程	忽略
设置 ACCOUNTING 为远程	忽略	忽略	远程
禁用 ACCOUNTING	忽略	忽略	禁用
禁用 AUTHENT	n/a	n/a	n/a
禁用 AUTHOR	n/a	n/a	n/a

使用注册

可以选择 AAA 注册配置为远程或本地。如果选择本地认证，则必须同时使用本地授权。如果选择远程认证，则必须使用远程授权。不支持本地记帐，所以当本地授权和认证时必须禁用记帐。

注意： 在启用控制台注册之前，保存具有禁用控制台注册的配置。如果将注册认证设置为在远程服务器上使用 Radius、TACACS 或 TACACS+ 进行，而路由器不能达到认证服务器，则将拒绝对此路由器的访问。禁用控制台注册将避免出现锁闭的情况。

当配置远程认证时，可将授权设置为其他远程授权协议 Radius 或 TACACS+，并将记帐设置为使用 Radius 或 TACACS+。

- 将 AAA 设置为本地，则会将认证设置为本地、将授权设置为本地并将记帐设置为禁用。
- 将 AAA 设置为远程，则会将认证设置为远程、将授权设置为远程并将记帐设置为远程。
- 将认证协议设置为本地，则会自动将授权协议设置为本地并禁用记帐。
- 仅当授权协议设置为本地并忽略记帐协议时，若将认证协议设置为远程，则自动将授权协议设置为远程。
- 仅当认证协议设置为本地并忽略记帐协议时，若将授权设置为远程，则自动将认证协议设置为远程。
- 仅当将认证协议设置为本地时，若将记帐协议设置为远程，则自动将认证协议设置为远程；仅当将授权设置为本地时，若将记帐协议设置为远程，则自动将授权协议设置为本地。
- 将记帐协议设置为禁用不影响认证或授权协议。
- 不允许禁用认证或授权。

有效的注册/管理安全协议

以下是有效的注册/管理安全协议。

认证/授权方式

本地、RADIUS、TACACS Plus

记帐方式

RADIUS、TACACS Plus

表 23. 设置注册安全协议

操作	认证	授权	记帐
设置 AAA 为本地	本地	本地	禁用
设置 AAA 为远程	远程	远程	远程
设置 AUTHENT 为本地	本地	本地	禁用
设置 AUTHOR 为本地	本地	本地	禁用
设置 AUTHENT 为远程	远程	如果忽略本地，则设置为远程	忽略
设置 AUTHOR 为远程	如果忽略本地，则设置为远程	远程	忽略

使用本地或远程认证

表 23. 设置注册安全协议 (续)

操作	认证	授权	记帐
设置 ACCOUNTING 为远程	如果忽略本地，则设置为远程	如果忽略本地，则设置为远程	远程
禁用记帐	忽略	忽略	禁用
禁用 AUTHEN	n/a	a	n/a
禁用 AUTHOR	n/a	n/a	n/a

使用隧道

将隧道认证设置为与隧道授权相同。将隧道认证设置为本地或远程后，就可以启用记帐。隧道授权和认证服务器必须相同。

有效的隧道安全协议

以下是有效的隧道安全协议:

认证/授权方式

本地、RADIUS

记帐方式

RADIUS、TACACS Plus

表 24. 设置隧道安全协议

操作	认证	授权	记帐
设置 AAA 为本地	本地	本地	忽略
设置 AAA 为远程	远程	远程	远程
设置 AUTHENT 为本地	本地	本地	忽略
设置 Author 为本地	本地	本地	忽略
设置 AUTHENT 为远程	远程	远程	忽略
设置 AUTHOR 为远程	远程	远程	忽略
设置 ACCOUNTING 为远程	忽略	忽略	远程
禁用 ACCOUNTING	忽略	忽略	禁用
禁用 AUTNENT	n/a	n/a	n/a
禁用 AUTHOR	n/a	n/a	n/a

口令规则

本地认证允许用户用口令控制注册访问。可以根据以下规则检查口令。

- 口令具有最少的字符。设置必需的字符数。
- 至少包括一个字母字符。
- 至少包括一个非字母字符。
- 第一位置为非数字字符。
- 最后一个位置为非数字字符。
- 最多包括三个以前口令所使用的连续字符。
- 最多包括两个连续的字符。

- 不包括口令中的用户 ID。
- 与以前使用的三个口令不同。
- 一些天后更改。设置口令更改的间隔天数。

理解认证服务器

认证服务器是验证网络用户 ID 和口令的网络服务器。如果通过认证服务器将设备配置为认证，并且该设备接收到认证协议发送的一个包，则该设备向认证服务器发送用户 ID 和口令以进行认证。如果用户 ID 和口令正确，则服务器则作出正面响应。此时设备可以与请求的发出者通信。如果服务器未找到设备发送的用户 ID 和口令，则作出负面响应。此时设备放弃认证请求的会话。

SecurID 支持

2212 可以使用安全动态 ACE/服务器认证使用 SecurID 的拨入客户机。这一支持可以使用 ACE/服务器 上的 TACACS、TACACS+ 或 RADIUS 对客户机进行认证。对该拨入客户机的配置与对 2212 上其它拨入客户机的配置相同。

拨入客户机照常注册，但口令使用 SecurID 口令代码。SecurID 口令代码由后跟 SecurID 令牌卡号的 4 到 n 位 PIN 编号组成。(PIN 的最大位数根据服务器的不同而不同。)用户 ID 和口令显示如下:

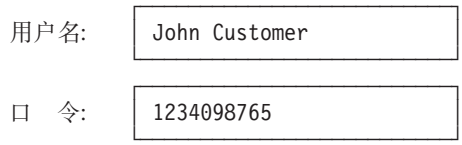


图 14. SecurID 用户名和口令代码

当 ACE/Server 对注册进行认证时，可能向客户机请求下一个令牌。下一个令牌是令牌卡上的下一个令牌。下一个令牌的最大位数随客户机使用 SecurID 令牌卡不同而不同。当提示以口令*令牌的格式时，客户机可以输入口令代码和下一个令牌，如下所示:

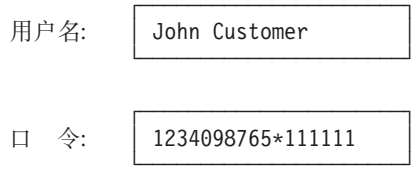


图 15. 带有下一个令牌的 SecurID 口令代码

注: 当服务器请求客户机输入下一个令牌时，客户机必须:

1. 输入 PIN
2. 从令牌卡等待一个新令牌并输入该令牌
3. 在来自令牌卡的下一个令牌之后输入 *

ACE/Server 管理员配置相关条件，以允许服务器请求下一个标记或新的 PIN。

拨入客户机应使用 SPAP，这样在需要输入下一个令牌时就可以接收认证系统发出的警报。如果客户机未使用 SPAP 且注册失败，则应按口令代码*标记的格式输入新的口令代码。如果客户机仍失败，则可能是客户机和 ACE/服务器之间存在其他问题。

限制

存在以下限制:

- 不支持 Security Dynamics Inc. (SDI) 和 DES 加密。
- 不支持 SecurID 『New PIN』 功能。
- TACACS 不支持 『New PIN』 或 『Next-Token』 功能。客户机可以在注册时指定下一个令牌，但服务器不可使用该令牌。
- 不支持为回呼配置的客户机。
- 当使用具有 TACACS 或 TACACS+ 的 CHAP 时，将 CHAP rechallenge 间隔设置为 0。
- 在使用 RADIUS 认证时不使用 CHAP。
- 使用 TACACS+ 和 SPAPY 时客户机可以获得最佳结果。
- 不支持使用多路连接的进行 SecurID 认证的 Windows 3.1 DIAL 客户机。
- 在使用 SecurID 认证时，建议使用最新的客户机软件(例如，Windows 95 或 OS/2)。

第13章 配置认证

本章节说明了认证的配置和操作命令。它包括以下部分:

- 『访问认证配置提示符』
- 『认证配置命令』

访问认证配置提示符

如果要访问 `Authent config >` 提示符:

1. 在 `*` 提示符下，输入 **talk 6**。
2. 在 `Config >` 提示符下，输入 **feature auth**。

认证配置命令

表25列出了 `Authent config >` 提示符下可用的命令。

表 25. 认证配置命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Disable	禁用 AAA 记帐。
List	显示 AAA 配置参数。
Login	对 AAA 的注册进行配置。
Nets-info	显示有关本地 PPP 认证的信息。
Password-rules	配置口令规则(启用或禁用)。
PPP	配置 PPP 的 AAA。
Quickset	快速配置认证方式。
Servers	配置单一远程 AAA 服务器。
Set	配置认证参数，不考虑参数类型。
Tunnel	配置 L2TP 隧道的 AAA。
User-profile	配置本地 PPP 用户。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Disable

使用 **disable** 命令禁用记帐。

语法:

disable accounting

List

使用 **list** 命令显示 AAA 参数。

语法:

list accounting

authentication

authorization

all

config

```
AAA Config> list all
ppp AAA configuration...
 ppp authentication        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 ppp authorization         : locallist
 ppp accounting            : Disabled
tunnel AAA configuration...
 tunnel authentication     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel authorization      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel accounting         : Disabled
login AAA configuration...
 login authentication      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login authorization       : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login accounting          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>


AAA Config> list accounting all
accounting AAA configuration...
 accounting ppp            : Disabled
 accounting tunnel         : Disabled
 accounting login          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
```

```
     Request interval        3
   Key for encryption        <notSet>
AAA Config> list accounting config
accounting ppp             : Disabled
accounting login           : Radius        serv01
accounting tunnel          : Disabled


AAA Config> list authentication all
authentication AAA configuration...
 authentication ppp        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 authentication tunnel     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
```

Login

使用 **login** 命令对 AAA 的注册进行配置。

表26 列出与 **login** 命令一起使用的子命令。

表 26. 注册子命令

命令	功能
Disable	禁用注册记帐。
List	显示用于注册的 AAA 配置参数。
Set	设置用于注册的 AAA 配置参数。

Disable

使用 **login disable** 命令禁用记帐。

语法:

login disable accounting

List

使用 **login list** 命令显示 AAA 的配置参数。

语法:

login list all
accounting
authentication
authorization
config

Set

使用 **login set** 命令配置认证参数。

语法:

login set aaa
accounting
authentication
authorization

aaa *authtype*
设置认证类型、授权类型及记帐类型。*Authtype* 为下列各项之一:

local 设置认证类型、授权类型及记帐类型以使用本地维护的用户数据库。

remote
设置认证、授权和记帐类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

accounting *authtype*
设置记帐类型。*Authtype* 为下列各项之一:

remote
设置认证类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

authentication *authtype*
设置认证类型。*Authtype* 为下列各项之一:

local 设置认证类型以使用本地维护的用户数据库。

remote
设置认证类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

authorization *authtype*
设置授权类型。*Authtype*为下列选项之一:

local 设置授权类型以使用本地维护的用户数据库。

remote
设置授权类型以使用远程用户数据库。

server id
指定远程数据库的标识符。

Nets-info

使用 **nets-info** 命令以显示各 PPP 接口上的当前所配置的 PPP 认证协议。

语法:

nets-info

Password-rules

使用 **password-rules** 命令配置口令(启用或禁用)。

表27 列出与 **password-rules** 命令一起使用的子命令。

表 27. Login 的子命令

命令	功能
Disable	禁用 password rule 命令。
Enable	启用 password rule 命令。
List	显示 password rule 的当前状态(启用或禁用)。

Disable

使用 **password-rules disable** 命令禁用任一或所有的 password rule。

语法:

password-rules disable all
compare-ident-prev
change-days
first-non-numeric
force-change
ident-chars
last-non-numeric
lockout
minimum-length
one-alpha
one-nonalpha
prev-three
userid-contained

compare-ident-prev

将请求更改口令的用户标识符与先前的用户标识符相比较。

change-days

要求更改口令之前的最大天数。

有效值: 0 到 360

缺省值: 180

first_non-numeric

口令的第一个字符不能为数字。

有效值: 任何非数字型的字符

缺省值: 空

force-change

超过最大更改天数之后强行改变口令。为了验证新口令，该命令向您显示旧口令与新口令。

有效值: 0 到 360

缺省值: 180

ident-chars

在相同位置上不能有 3 个以上的旧命令所使用的字符。

last-non-numeric

口令中的最后一字符不能为数字。

有效值: 任何非数字型的字符

缺省值: 空

lockout

在锁定前您可以尝试口令的次数。

有效值: 0 到 360

缺省值: 3

minimum-length

为使口令有效而至少需要的字符数目。

有效值: 1 到 31

缺省值: 8

maximum-length

口令所能包含的字符的最大数目。

有效值: 1 到 31

缺省值: 8

one-alpha

口令中至少有一个字母字符。

one-nonalpha

口令中至少有一数字字符。

prev-three

此口令不能与前面三条口令中的任何一条相同。

userid-contained

不能将用户 ID 作为此口令的一部分。

Enable

使用 **password-rules enable** 命令启用任一或所有的 password rule。有关 password rule 描述的列表，请参阅 **disable** 命令部分。

语法:

password-rules enable all
compare-ident-prev
change-days

first-non-numeric

force-change

ident-chars

last-non-numeric

lockout

minimum-length

one-alpha

one-nonalpha

prev-three

userid-contained

List

使用 **password-rules list** 命令显示 password rule (启用或禁用)的当前状态。

语法:

password-rules list

PPP

使用 **ppp** 命令配置 PPP 的 AAA。

表28列出可与 **ppp** 命令一起使用的子命令。

表 28. PPP 子命令

命令	功能
Disable	禁用 PPP 的记帐。
List	显示 PPP 的 AAA 配置参数。
Set	设置 PPP 的 AAA 配置参数。

Disable

使用 **ppp disable** 命令禁用 PPP 的记帐。

语法:

ppp disable accounting

List

使用 **ppp list** 命令显示 PPP 的 AAA 配置参数。

语法:

ppp list all

accounting

authentication

authorization

config

Set

使用 **ppp set** 命令设置 PPP 的 AAA 配置参数。

语法:

ppp set aaa

accounting

authentication

authorization

aaa *authtype*

设置认证类型、授权类型及记帐类型。*Authtype* 为下列选项之一:

local 设置认证类型、授权类型及记帐类型以使用本地维护的用户数据库。

remote

设置认证类型、授权类型及记帐类型以使用远程用户的数据库。

server id

指定远程数据库的标识符。

accounting *authtype*

设置记帐类型。*Authtype* 为下列选项之一:

remote

设置认证类型以使用远程用户的数据库。

server id

指定远程数据库的标识符。

authentication *authtype*

设置认证类型。*Authtype* 为下列选项之一:

local 设置认证类型以使用本地维护的用户数据库。

remote

设置认证类型以使用远程用户的数据库。

server id

指定远程数据库的标识符。

authorization *authtype*

设置授权类型。*Authtype* 为下列选项之一:

local 设置授权类型以使用本地维护的用户数据库。

remote

设置授权类型以使用远程用户数据库。

server id

指定远程数据库的标识符。

Servers

使用 **servers** 命令以配置单一的远程 AAA 服务器。

表29列出可与 **servers** 命令一起使用的子命令。

表 29. Server 的子命令

命令	功能
Add	添加远程 AAA 服务器概要文件。
Change	更改远程服务器概要文件。
Delete	删除远程服务器概要文件。
Lists	显示 AAA 服务器概要信息。

Add

使用 **servers add** 命令以添加远程服务器概要文件。

语法:

servers add name

radius 设置认证类型以使用 radius 认证服务器协议。

以下参数的数值可设置为:

key-for-encryption:

指定密钥。

有效值:32 个字符以内的任何字母数字字符串。

缺省值: 无。

primary-server-address:

指定主认证服务器的地址。

有效值: 任何有效的 IP 地址

缺省值: 0.0.0.0

retries

有效值: 1-100

缺省值: 3

retry-interval

有效值: 1-60

缺省值: 3

secondary-server-address:

指定次级认证服务器的地址。

有效值: 任何有效的 IP 地址

缺省值: 0.0.0.0

Author-Authent

指定是否在认证中传送认证属性。

有效值: yes, no

缺省值: yes

tacacs

设置认证类型以使用 TACACS 认证服务器协议。

可设置以下参数数值:

primary-server-address:

指定主认证服务器的地址。

有效值: 任何有效的 IP 地址

缺省值: 0.0.0.0

retries

有效值: 1-100

缺省值: 3

retry-interval

有效值: 1-60

缺省值: 3

secondary-server-address:

指定次级认证服务器的地址。

有效值: 任何有效的 IP 地址

缺省值: 0.0.0.0

tacacsplus

设置认证类型以使用 TACACS+ 认证服务器协议。

可设置以下参数数值:

encryption:

指定是否进行加密。

有效值: yes, no

缺省值:

key-for-encryption:

指定将要使用的密钥。

有效值: 任何十六进制位值

缺省值:

primary-server-address:

指定主认证服务器的地址。

有效值: 任何有效的 IP 地址

缺省值: 0.0.0.0

privilege-level

有效值: 0-15

缺省值: 0

restarts

设置重新启动的次数。此参数不包括超时的重新启动，仅与服务器请求的重新启动有关。

有效值: 0-3200

缺省值: 0

time-to-connect

从服务器获得认证的许可时间。

有效值: 1-60

缺省值: 9

secondary-server-address:

指定次级认证服务器的地址。

有效值: 任何有效的 IP 地址

缺省值: 0.0.0.0

Change

使用 **servers change** 命令更改远程服务器概要文件。有关远程服务器概要文件的说明，请参阅 **add** 命令部分。

语法:

servers change	radius
	tacacs
	tacacsplus

有关远程服务器概要文件的说明，请参阅 **servers add** 命令部分。

Delete

使用 **servers delete** 命令删除远程服务器概要文件。有关远程服务器概要文件的说明，请参阅 **add** 命令部分。

语法:

servers delete	radius
	tacacs
	tacacsplus

有关远程服务器概要文件的说明，请参阅 **servers add** 命令部分。

List

使用 **servers list** 命令显示 AAA 服务器的概要信息。

语法:

servers list	all
	names

profile

Set

使用 **set** 命令设置注册、PPP 和 L2TP 隧道的参数。

语法:

set aaa
accounting
authentication
authorization

aaa *authtype*
设置认证类型、授权类型及记帐类型。*Authtype* 为下列选项之一:

local 设置认证类型、授权类型及记帐类型以使用本地维护的用户数据库。

remote
设置认证类型、授权类型及记帐类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

accounting *authtype*
设置注册、PPP 和通道的记帐类型。*Authtype* 为下列选项之一:

remote
设置认证类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

authentication *authtype*
设置注册、PPP 和通道的认证类型。*Authtype* 为下列选项之一:

local 设置认证类型以使用本地维护的用户数据库。

remote
设置认证类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

authorization *authtype*
设置注册、PPP 和通道的授权类型。*Authtype* 为下列选项之一:

local 设置授权类型以使用本地维护的用户数据库。

remote
设置授权类型以使用远程用户数据库。

server id
指定远程数据库的标识符。

Tunnel

使用 **tunnel** 命令配置 L2TP 通道的 AAA。

表30列出与 **tunnel** 命令一起使用的子命令。

表 30. Tunnel 的子命令

命令	功能
Disable	禁用 L2TP 通道的记帐。
List	显示 L2TP 通道的 AAA 配置参数。
Set	设置 L2TP 通道的 AAA 配置参数。

Disable

使用 **tunnel disable** 命令禁用 L2TP 通道的记帐。

语法:

tunnel disable accounting

List

使用 **tunnel list** 命令显示 L2TP 通道的 AAA。

语法:

tunnel list all
accounting
authentication
authorization
config

Set

使用 **tunnel set** 命令设置 L2TP 通道的 AAA 配置参数。

语法:

tunnel set aaa
accounting
authentication
authorization

aaa *authtype*

设置认证类型、授权类型及记帐类型。*Authtype* 为下列选项之一:

local 设置认证类型、授权类型及记帐类型以使用本地维护的用户数据库。

remote

设置认证类型、授权类型及记帐类型以使用远程用户的数据库。

server id

指定远程数据库的标识符。

accounting *authtype*

设置记帐类型。*Authtype* 为下列选项之一:

remote
设置认证类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

authentication *authtype*
设置认证类型。*Authtype* 为下列选项之一:

local 设置认证类型以使用本地维护的用户数据库。

remote
设置认证类型以使用远程用户的数据库。

server id
指定远程数据库的标识符。

authorization *authtype*
设置授权类型。*Authtype* 为下列选项之一:

local 设置授权类型以使用本地维护的用户数据库。

remote
设置授权类型以使用远程用户数据库。

server id
指定远程数据库的标识符。

User-profiles

使用 **user-profiles** 命令存取 `User profile config>` 命令提示符。从该提示符下，您可使用下列命令。

表 31. 用户-概要文件配置命令。

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	添加 PPP 用户概要文件。
Change	更改 PPP 用户概要文件。
Delete	删除 PPP 用户概要文件。
Disable	禁用 PPP 用户概要文件。
Enable	启用 PPP 用户概要文件。
List	列出 PPP 用户概要信息。
Report	生成 PPP 用户概要文件的报告。
Reset-user	重置 PPP 用户概要文件。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add

使用 **user profiles add** 命令，向本地 PPP 用户数据库添加远程用户的用户概要文件，或者使用该命令，通过 IP 网络授予路由器隧道对等访问权。

语法:

add ppp-user
tunnel

ppp-user

向本地 PPP 的用户数据库添加远程用户的用户概要文件。您进行添加的用户可多达 500 个。您可以为每个远程路由器添加 PPP 用户，或者，也可以为能够与正在配置的设备连接的 DIALS 客户机添加 PPP 用户。

有关命令的语法和选项说明，请参阅*Access Integration Services 软件用户指南*中 “配置 CONFIG 进程”一章的 Add 部分。

实例:

```
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
```

实例:

```
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
```

tunnel 将通过 IP 网络隧道对等访问的权利授予路由器。然后，对等实体便可以得到授权以将隧道连接的 PPP 会话启动至路由器。

有关命令的语法和选项说明，请参阅 *Access Integration Services 软件用户指南*中 “配置 CONFIG 进程”一章的 Add 部分。

实例:

```
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
```

Change

使用 **change** 命令更改用户概要文件。

语法:

change ppp-user

tunnel

Delete

使用 **delete** 命令删除用户概要文件。

语法:

delete ppp-user

tunnel

Disable

使用 **disable** 命令禁用用户概要文件。

语法:

disable *name*

Enable

使用 **enable** 命令启用用户概要文件。

语法:

enable *name*

List

使用 **list** 命令列出用户概要文件信息。

语法:

list ppp-user

tunnel

```
User profile config> list ppp-user
List  (Name, Verb, User, Addr, Encr, zdump): [Verb]
     PPP user name: ppp01
            Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
```

List 指定如何存取列表信息。

有效值: name, verb, user, addr, encr, zdump

缺省值: verb

PPP user name
列出用户名。

Expiry
列出截止日期。

User IP address
列出用户 IP 地址。

Encryption
显示是否启用加密。

Status
显示是否禁用 status。

Login attempts
显示用户尝试注册的次数。

Login failures
显示注册尝试的失败次数。

Lockout attempts
显示锁定尝试的次数。

Report

使用 **report** 命令以生成 PPP 用户概要文件报告。

语法:

report addresses
all
callback
dump
encrypt
name
password
time
user

```
User profile config> report addresses
PPP user name      User IP address
-----------------  ------------------
ppp01              Interface Default
1 record displayed.


User profile config> report all
     PPP user name: ppp01
            Expiry: <unlimited>
   User IP address: Interface Default
```

```
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
1 record displayed.


User profile config> report callback
PPP user name      Callback type        Phone Number
-----------------  -------------------  --------------------
ppp01
1 record displayed.


User profile config> report dump
Enter user name:  []? user01


User profile config> report encrypt
PPP user name      Encryption
-----------------  --------------
ppp01              Not Enabled
1 record displayed.


User profile config> report name
PPP user name
-----------------
ppp01
1 record displayed.


User profile config> report password
PPP user name      Expiry        Grace
-----------------  ------------  ------
ppp01              <unlimited>
1 record displayed.


User profile config> report time
PPP user name      Time alotted
-----------------  -------------------
ppp01
1 record displayed.


User profile config> report user
Enter user name:  []? login01
     PPP user name: login01
        Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
```

Reset-user

使用 **reset-user** 命令重置用户概要文件。

语法:

reset-user *name*

第14章 使用和配置加密协议

注: 加密支持是可选的，必须使用 **load add** 命令将其添加到软件安装中。请参阅 *Access Integration Services 软件用户指南* 中的 CONFIG process(配置进程) **load** 命令。

加密的目的在于将数据转换为不可读的格式，以保证数据的专用性。必须将***加密***数据解密后，才能得到原始数据。

221x 支持:

- 具有 40 或 128 位密钥的 RC4 加密算法，用于 PPP 接口上的 Microsoft 点到点加密 (MPPE)。
- 具有 56 位密钥的 “密码字组链接中的数据加密标准 (DES-CBC)” 算法，它支持 RCF (1968 和 1969) 中说明的 PPP 加密控制协议。
- 使用 40 位密钥的帧中继加密的商业数据屏蔽工具 (CDMF)。该项支持是专用的。

PPP 使用加密控制协议加密

加密控制协议 (ECP) 在路由器中可协商使用 PPP 协议在点到点链接通信时使用加密。加密控制协议提供了一个一般化机制，以协商 PPP 链接中的加密和解密算法。PPP 链路的每个方向可以使用不同的加密算法。

加密和解密的方法也称为***加密算法***。加密算法用密钥控制加密和解密。与压缩不同，路由器在链接的两个方向加密，这是因为仅在一个方向上加密会有安全风险性。一旦 ECP 无法在两个方向上协商加密算法，链接将会中断。

配置 PPP 的 ECP 加密

要配置在数据链接层使用加密的设备，应:

1. 为远程设备和本地 PPP 接口设置密钥。

   在 `Config>` 提示符处使用 **add ppp-user** 命令设置远程设备的密钥。请参阅 *Access Integration Services 软件用户指南* 中章节 “配置 CONFIG progress” 的 Add 命令，以获得对命令语法和选项的说明。

   使用 **enable ecp** 命令设置本地 PPP 接口的密钥(请参阅 *Access Integration Services 软件用户指南* 章节 talk 6 `PPP Config>` 中的 **enable** 命令)。
2. 在 `PPP Config>` 提示符处使用 **enable ecp** 命令将个别 PPP 链接配置为使用加密控制协议 (ECP)。
3. 启用 PAP、CHAP 或 SPAP。

用户也可以禁用加密、更改用户的密钥、列出加密状态或设置请求加密时设备所使用的名称。有关

- 禁用加密的信息，请参阅 *Access Integration Services 软件用户指南* 中 `PPP Config>` 的 **disable ecp** 命令。
- 更改远程用户密钥和口令，请参阅 *Access Integration Services 软件用户指南* 中 `Config>` 的 **change ppp-user** 命令。

- 要列示加密状态，请参阅 *Access Integration Services 软件用户指南* 中 PPP Config> 的 **list ecp** 命令。
- 要获取设置设备名称的信息，请参阅 *Access Integration Services 软件用户指南* PPP Config> **set name** 命令。

监视 PPP 的 ECP 加密

可以通过以下方式监视接口上的不同加密设置:

1. 使用 **talk 5** 命令进入监视提示符状态。
2. 使用 **network x** 命令选择希望监视的接口。执行该命令使用户处于 PPP x> 提示符状态。

在该提示符处，可以:

- 列出加密的当前状态、最新的加密协商情况、加密状态更改后经过的时间和加密者所使用的算法。(请参阅 *Access Integration Services 软件用户指南* 中的 **list control ecp** 命令。)
- 列出在接口上接收和传输的加密控制包。 (请参阅 *Access Integration Services 软件用户指南* 中的 **list ecp** 命令。)
- 列出接口上传输或接收的加密包。 (请参阅 *Access Integration Services 软件用户指南* 中的 **list edp** 命令。)

Microsoft 点到点加密(MPPE)

对于远程连接的 Windows 工作站，即熟知的 Microsoft 拨号联网 (DUN) 客户机，Microsoft 点到点加密 (MPPE) 提供了一种在客户机与 2212 之间通过 PPP 链接加密传输数据的方法。 MPPE 也可以用于加密在路由器之间通过 PPP 链路传输的数据。通常在链路的两个方向上协商使用 MPPE。

MPPE 使用密钥算法执行加密。在密钥算法中，加密和解密使用相同的密钥。该密钥不是用户配置的，而是工作站之间在发送和接收 MPPE 协商过程生成的。要使用 MPPE，必须配置认证协议 Microsoft Challenge/Handshake Authentication Protocol(MS-CHAP)。

如果通过 MS-CHAP 认证 PPP 接口，路由器转入 『Microsoft 模式』，则启用压缩时仅可使用 MPPC，启用加密时仅可使用 MPPE。在 『Microsoft 模式』下，路由器忽略压缩算法的优先级列表并禁用 ECP 协商。

配置 MPPE

要配置 MPPE，应在每个接口上执行以下操作:

1. 配置 MS-CHAP。在 *Access Integration Services 软件用户指南*，请参阅 『Microsoft PPP CHAP Authentication (MS-CHAP)』 和 『Configuring and Monitoring Point-to-Point Protocol Interfaces (配置和监控点对点协议接口)』，以获取有关使用并配置 MS-CHAP 的信息。
2. 如果正在配置路由器之间的连接，则使用 **set name** 命令设置本地 PPP 接口名称 (请参阅 *Access Integration Services 软件用户指南* 中 PPP Config> 的 **set name** 命令)。

3. 如果要压缩数据，可在 PPP Config> 提示符处使用 talk 6 **enable ccp** 命令启用 MPPC。MPPE 不需要压缩数据。
4. 启用 MPPE。在 PPP Config> 提示符处使用 **enable mppe** 命令 (请参阅 *Access Integration Services 软件用户指南* 中 PPP Config> 的 **enable** 命令)。
5. 重新启动路由器以激活配置。

也可以禁用 MPPE 并列出 MPPE 选项。

- 在 PPP Config> 提示符处使用 talk 6 **disable mppe** 命令以禁用 MPPE。
- 在 PPP Config> 提示符处使用 talk 6 **list ccp** 命令以列出配置的 MPPE 选项。

监视 MPPE

如第160页的『监视 PPP 的 ECP 加密』 中所述，进入 PPP> 提示符状态。使用 **list mppe** 命令可查看 MPPE 数据统计信息，使用 **list control ccp** 命令可查看 MPPE 状态。这些命令的输出实例在*Access Integration Services 软件用户指南* 的『配置并监视点对点协议接口』中已有显示。

配置帧中继接口的加密

注: 帧中继使用专用的加密方案。

在所有启用加密的接口上都支持数据加密。可以在启用加密的接口上配置每个线路以根据需要执行或不执行加密。

要将设备配置为在帧中继链接上加密:

1. 使用 **talk 6** 命令进入帧中继配置提示。
2. 使用 **net** # 命令选择希望启用加密的帧中继接口。
3. 使用 **enable encryption** 命令在帧中继接口上启用加密。请参阅 *Access Integration Services 软件用户指南* 中的帧中继命令。
4. **add permanent-virtual-circuit** 命令增加启用加密的永久性虚拟线路并为每个 PVC 定义密钥。请参阅 *Access Integration Services 软件用户指南* 中的帧中继命令。
5. 为配置的每个启用加密接口重复执行步骤 1 到 4。

注: 如果为 FR 永久性虚拟线路启用加密，则在加密对虚拟线路另一端的设备做了成功协商之前，数据不会流过该线路。由于必须配置 PVC 才能输入密钥，所以孤立的线路不支持加密。

用户也可以禁用接口加密、更改 PVC 的加密设置或列出加密状态。有关

- 禁用接口加密的信息，请参阅 *Access Integration Services 软件用户指南* 中的帧中继 **disable encryption** 命令。
- 更改 PVC 的加密设置，请参阅 *Access Integration Services 软件用户指南* 中的 **change permanent-virtual-circuit** 命令。
- 列出加密状态，请参阅 *Access Integration Services 软件用户指南* 中的帧中继 **list all**、**list lmi** 和 **list permanent-virtual-circuit** 命令。

监视帧中继接口上的加密

可以通过以下方式监视接口上的不同加密设置:

1. 使用 **talk 5** 命令访问监视提示。
2. 使用 **network** # 命令选择要监视的接口。执行该命令使用户处于 FR *x*> 提示处。

在该提示下，可列出接口、PVC 或线路的当前加密状态。请参阅 *Access Integration Services 软件用户指南* 中的 Frame Relay list monitoring commands (帧中继列表监视命令)。

第15章 使用 IP 安全

对于通过 Internet 协议 (IP) 发送的信息包，可以使用 2212 的 IP 安全功能部件来保证其安全。IP 安全特性包括认证进程和加密进程。

注: 在某些国家，由于美国出口条款限制，所以不支持加密，也没有加密参数。但是，通常可使用 ESP-NULL 算法。有关 ESP-NULL 算法的定义，请参阅第164页的『ESP 加密算法』。

按照 RFC 1825 安全结构为 Internet 协议所定义的，安全包括:

可认证性
可确知所接收的数据与所发送的数据相同，且声明发送数据的发送者是实际的发送者。

完整性 确保数据在从信源传到信宿的过程中，没有受到未能检测的修改。

机密性 以相关接收者可了解发送内容而无关方不能了解发送内容的方式进行通信。

不可否认性
进行通信，即使发送者以后可能会否认发送过某些数据，接收者也能确证发送者确实发送过这些数据。

2212 的 IP 安全功能部件提供 3 种特性: 可认证性、完整性和机密性。IPv4 和 IPv6 均可支持 IP 安全。

安全通道

为保护发送到另一个主机、路由器或防火墙的数据，您可配置安全通道。IP 安全 (IPsec) 通道是将所保护的 IP 信息包传输到远程主机、路由器或防火墙的双向逻辑连接。IP 认证头 (AH) 和 IP 封装安全有效负荷 (ESP) 是使用特殊 IP 头(经过认证和加密)的技术，从而确保了通道的安全。

安全通道可用多个参数标识，例如通道 ID 和通道远端的信宿主机地址。通过为每个必须保证安全的 IP 路由手工配置安全通道，就在 2212 上建立了 IP 安全。每个指定的参数集可创建一个安全通道。

注: 在每个安全通道中，以下列表中的参数在安全通道的两端必须相匹配；也就是说，必须为发送者和接收者配置相同的参数值:

- AH 算法和 AH 认证关键字(请参阅第165页的『配置算法』。)
- ESP 加密算法与 ESP 密钥和解锁密钥(请参阅第165页的『配置算法』。)
- 安全参数指数 (SPI) (请参阅第165页的『安全关联』。)

IP 认证头 (AH)

AH 在 draft-ietf-ipsec-auth-header-06 认证头中有说明。该头保留有 IP 数据报的认证数据。数据报的发送者使用加密的认证功能，该功能要取决于秘密的认证密匙。可向数据报的内容使用加密认证功能。

AH 认证算法

使用 AH 通道策略的安全通道必须使用以下两种认证算法之一:

- 具有“避免重复接收”的 HMAC-MD5 IP 认证
- 具有“避免重复接收”的 HMAC-SHA-1 IP 认证

这两种算法采用带有密匙的消息认证(使用了加密散列函数(缩写为 HMAC) 并可“避免重复接收”。“避免重复接收”是可选的，它使用 AH 中提供的序列号来确认以前未接收过此信息包。“避免重复接收”可使接受者免受“拒绝服务”的攻击，在此攻击中，相同的信息包不断被传送给接受者。路由器可能因忙于处理重复的信息包，而不能处理合法的通信。有一个滑动窗口可保存足够的序列号，可以拒此确定以前是否收到过该序列号。

IP 封装安全有效负荷 (ESP)

ESP 在 draft-ietf-ipsec-esp-v2-05 封装安全有效负荷中有说明。ESP 为部分或所有 IP 信息包加密，以保证机密性，同时也确保可认证性和完整性。在 ESP 中，认证功能是可选的。如果选择 ESP-NULL 算法，则 ESP 不执行加密，仅检查可认证性和完整性。

ESP 认证算法

ESP 认证可用的认证算法与 AH 的认证算法相同。请参阅『AH 认证算法』以获取详细信息。

ESP 加密算法

要配置 ESP，必须选择以下三种加密算法之一，也可选择 ESP-NULL 算法:

- 密码字组链接模式中的数据加密标准(DES-CBC)
- 商业数据屏蔽工具(CDMF)
- 三重 DES (3DES)

注: 除了 ESP-NULL，其他所有 ESP 加密算法都遵守美国出口法规。如果您的 2212 不允许您配置其中的部分或全部算法，则可能是因为在您所在的国家禁止出售这些算法。请与您的 IBM 代表进行核实，以获取详细信息。

NULL 加密算法 ESP-NULL 在所有国家都可用，但无法为纯文本数据加密。它为 ESP 提供了仅进行提供可认证性和完整性的一种方法，不包括加密。在配置 ESP-NULL 时，***必须***配置 ESP 认证算法其中的一种。

通道策略

使用隧道策略可配置安全隧道，通道策略包括以下几种: AH、ESP、AH-ESP 或 ESP-AH。

当同时配置了 AH 和 ESP 时，要用到以下几种关系:

- 策略 AH-ESP 表示将出站的信息包配置为在认证之前加密。在这种情况下，AH 认证先检查入站信息包。仅通过 AH 认证的传送信息包才转发给 ESP 以进行解密。
- 策略 ESP-AH 表示将输出包配置为在加密之前认证。在这种情况下，先由 ESP 为输入的包解密。只有成功解密的信息包才能转发给 AH 认证。

安全关联

安全关联 (SA) 是使用 AH 或 ESP 以保护连接通信量的单向安全连接。需要为各安全通道--出站和入站--分别配置两个安全关联或一个 SA 集。每个安全关联都将由其自己的安全参数指数 (SPI) 进行标识，该指数是一个任意的 32 位的值。

传送模式和通道模式

传送模式或通道模式确定了 IPsec 处理 IP 信息包的方式。缺省模式为通道模式，仅当路由器作为安全网关时必须处于该模式。仅当路由器作为主机时必须处于传送模式。

使用 AH 的模式

在传送模式下，在 IP 头之后、上层协议(例如 TCP 或 UDP) 的头之前插入 AH。在此模式下，AH 可认证上层协议的头和 IP 信息包的内容，但不包括能认证 IP 头中的不定字段(例如生存时间 [TTL]、校验和、段标记、段偏移和服务类型 [TOS])。

在通道模式中，AH 位于 IP 信息包之前，创建新的 IP 头信息并将其放在 AH 之前。被传送的信息包 IP 头(称为内部 IP 头)中带有信息包的最终信源和信宿地址。新的 IP 头(称为外部 IP 头)可能包括作为通道端点的安全网关的地址。 AH 保护除了新 IP 头中的不定字段以外的所有其他的新信息包，包括新的 IP 头和所传送的 IP 信息包。

使用 ESP 的模式

在使用 ESP 的传送模式下，有效负荷数据包括上层协议数据，例如 TCP 或 UDP 数据。可为上层协议数据加密。如果使用认证，则认证 ESP 头、上层协议数据和 ESP 尾记录。

在通道模式下，有效负荷数据包含整个 IP 信息包，并且，创建新的 IP 头并将其置放到 ESP 之前。传送信息包的 IP 头(称为内部 IP 头)带有信息包的最终信源和信宿地址，而新的信息包(称为外部 IP 头信息)带有安全网关的地址。ESP 为所传送的 IP 信息包加密。如果使用 ESP 认证，则认证 ESP 头信息、传送的 IP 信息包和 ESP 尾记录。

配置算法

根据通道策略，将算法配置如表32中所示。

表 32. 配置有不同通道策略的算法

通道策略	算法
AH、AH-ESP 或 ESP-AH	• 本地 AH 认证算法--必选 • 远程 AH 认证算法--可选
ESP、AH-ESP 或 ESP-AH	• 本地加密算法--必选 • 远程加密算法--可选 • 本地 ESP 认证算法--可选 • 远程 ESP 认证算法--可选 **注:** 如果软件装载不包括加密，则您将不会看到与加密关联的参数。

本地算法适用于出站信息包，远程算法适用于入站信息包。远程算法的值是可选的，因为每个远程算法都使用相应的本地算法作为缺省算法。本地 ESP 认证算法是可选的，因为作为 ESP 一部分的认证是可选的功能。

发送者为特定安全通道配置的本地算法，必须与接收者在安全通道远端配置的远程算法相同。例如，如果发送者隧道策略为 AH，AH 本地认证算法为 HMAC-MD5，则接收者必须将隧道策略配置为 AH，且接收者的 AH 远程认证算法必须为 HMAC-MD5。

配置密匙

在配置每个算法时，同时也必须配置密匙。各密匙必须与通道远端主机上相同算法的关键字相匹配。例如，如果出站信息包的本地密钥为 0098B1C588A109D5，则安全通道远端主机中入站信息包的远程密钥也应配置为 0098B1C588A109D5。请参阅第175页的『第16章 配置和监控 IP 安全』中的 **add tunnel** 命令的密匙说明，以获取详细信息。

通道中的通道

在某些情况下，为增强安全，则应在两个 IPsec 通道上发送信息包。通道中的通道是允许信息包封装两次并使其在两个通道中有顺序地传送的功能部件。信息包过滤器访问控制规则，标识出其中一个 IPsec 通道的信息包以进行封装。在发送信息包之前，第二个访问控制规则将该信息包提交给第二个 IPsec 通道以进行第二次封装。

两个 IPsec 通道从相同路由器起始，但两个通道的远端是不同的机器。第二个 IPsec 通道的远端必须是安全网关路由器；第一个通道的远端可以是安全网关也可以是主机。因为第一个和第二个 IPsec 通道具有不同的信宿，所以它们必须具有不同的远程 IP 地址。通道中的通道所使用的两个 IPsec 通道必须在通道模式下配置。在第二个 IPsec 通道中不允许进行附加的填充。

将第二次封装信息包后，在第二个 IPsec 通道上发送信息包。在第二个通道的端口，除去第二个封装，并根据第一个通道封装创建的头，将信息包转发给第一个 IPsec 通道。在该通道的端口，将第一个封装除去，并将该信息包转发给最终信宿。

路径 MTU 查找

对于 IPv4 和 IPv6 中，当2212作为安全网关时，IPSec 支持路径 MTU (PMTU) 查找。仅在安全通道处于通道模式且信息包不能被分段的情况下，支持 PMTU 查找。如果设置了 Don’t Fragment (DF) 位，则不能在 IPv4 中将信息包分成不同的段。信息包在 IPv6 中不能在通过中介路由器分段。在这些情况下，从安全通道一端到另一端的路径链路上，如果信息包不宜传送，则会产生 『packet too big』 ICMP 错误消息并将该信息包重新返回信息包的原始发出者。

因为路由器作为安全网关的，所以错误信息包将返回到原始发送路由器，而非真正的信息包的发出者。接收路由器必须将所报告的 MTU 正确地传送回真正的发出者。然后发出者缩小发送信息包的大小，使其能够达到最终的信宿。对 PMTU 查找的支持，在 Internet 协议的安全结构 draft-ietf-ipsec-arch-sec-05 - Internet 协议的安全结构 - 中有说明。

在 IPv4 中，有三个选项，用于在将发送的信息包外部头中设置 DF 位:

1. 从内部头中复制

2. 通常设置
3. 通常不设置

在通道模式下配置安全通道时(例如，使用 Talk 6 中的 **add tunnel** 命令时)会显示这些选项。在满足以下条件时，根据选定的选项处理 DF 位(除非出现特殊情况):

- 通道 MTU 等于最小 MTU。
- 入站信息包的长度等于或小于最小 MTU。
- 封装信息包长度小于最小 MTU。

在这种情况下，在 IPv4 中不设置 DF 位，无论如何配置，在连接远程通道端点的路径上都可将安全信息包根据需要分成不同的段。在 IPv6 中，当信息包离开安全网关时被分成不同的段，以适合在通道的路径 MTU 上传送。这项专门的操作是必要的，因为入站信息包已小于或等于最小 MTU，所以发出信息包的主机将不会再缩小信息包的大小。如果不允许分段，则该信息包将不会达到其最终信宿。

因为路径 MTU 可以根据网络拓扑结构或配置的更改而更改，路径 MTU 值必须定期地更换旧值并重设为最大值。更换旧值计时器缺省值为 10 分钟，并可使用 Talk 6 中的 **set path** 命令配置其他值。设置更换旧值参数为 0 可禁用 PMTU 旧值。

实例 1: 配置网络中的 IPsec 通道

在图16中显示的网络提供了 IPsec 通道的实例，该 IPsec 通道将具有 IPsec 的路由器连接到具有 IPsec 和网络地址转换 (NAT) 的路由器。

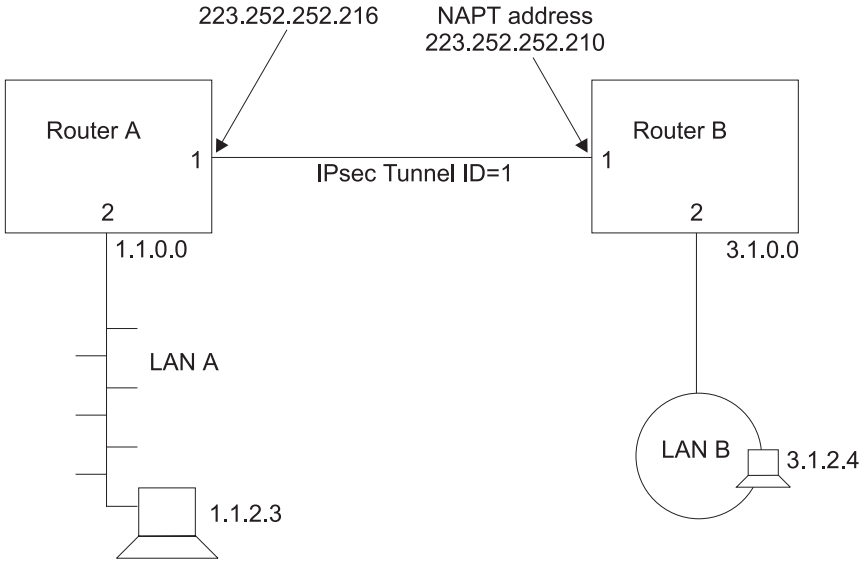


图 16. 具有 IPsec 和 NAT 的网络

在该网络中，配置具有 IPsec 通道 ID 1 的 IPsec 通道，将路由器 A 中的 IP 地址 223.252.252.216 更改为路由器 B 中的 IP 地址 223.252.252.210。将路由器 A 配置为具有 IPsec。将路由器 B 配置为具有 IPsec 和 NAT。以下部分说明了配置网络的过程。

注: 如果在网络中不计划使用 NAT，则将更加关注路由器 A，而不是路由器 B。但是，阅读有关配置路由器 B 的说明可以帮助您更深地理解 IPsec 通道两端的参数之间的关系。

配置仅具有 IPsec 的路由器 A

首先，按以下步骤配置路由器 A。

- 使用 **enable ipsec** 命令在路由器上启用 IPsec。
- 创建 IPsec 通道。
- 在作为 IPsec 通道端点的路由器接口上，分别创建出站和入站信息包过滤器。
- 创建信息包过滤器的访问控制规则。
- 重设 IPsec。
- 重设 IP。

创建路由器 A 的 IPsec 通道: 以下实例显示如何配置路由器 A 的 IPsec 通道 1。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> add tunnel
IPsec Tunnel ID (1 - 65535) [1]
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600)[46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1.1.1.1]? 223.252.252.216
Local Authentication SPI (256-65535)[256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 223.252.252.210
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set, or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
Ipsec config>
```

如本实例所示，会对您提示所需要提供的参数。ESP、AH-ESP 或 ESP-AH 安全通道需要相似的参数。

注: 在输入时并不显示密匙。所以，在本实例中看不到这些密匙值。如果 HMAC-MD5 认证密匙是可见的，则会看到这些关键字为 32 位十六进制字符。例如，密匙的值为 X'1234567890ABCDEF1234567890ABCDEF'。

为路由器配置信息包过滤器: 创建路由器 A 的 IPsec 通道后，必须设置两个 IP 信息包过滤器：一个出站信息包过滤器，一个入站信息包过滤器。如何创建信息包过滤器 *out-router-A*，在下列实例中有说明。请参阅 *Protocol Configuration and Monitoring Reference, Vol. 1* IP 章的 IP 访问控制部分，以获取有关配置 IP 信息包过滤器和访问控制规则的详细信息。

```
*talk 6
Config> Protocol IP
Internet protocol user configuration
IP Config> set access-control on
IP Config> add packet-filter
Packet-filter name [ ]? out-router-A
Filter incoming or outgoing traffic? [IN]? OUT
Which interface is this filter for [0]? 1
IP Config>update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

用同样的方式，在路由器 A 的接口 1 上创建的路由器 A 的入站信息包过滤器，称为 *in-router-A*。在接口 1 上创建信息包过滤器是因为它是 IPsec 通道 1 的端点。

配置路由器 A 的信息包过滤器访问控制规则: 然后就可以配置信息包过滤器访问控制规则。应在出站信息包过滤器 *out-router-A* 上创建两个访问控制规则，并在入站信息包过滤器 *in-router-A* 上创建两个访问控制规则。

注: 每个 IPsec 通道都必须配置入站和出站信息包过滤器，并为每个信息包过滤器配置两个访问控制规则。

出站信息包过滤器上的访问控制规则执行以下功能:

- 一个访问控制规则定义了将信息包传送到 IPsec 通道的信源地址和信宿地址的域。
- 另一个访问控制规则允许 IPsec 通信量通过信息包过滤器。

入站信息包过滤器上的访问控制规则执行以下功能:

- 一个访问控制规则允许入站 IPsec 通信量通过信息包过滤器传输。
- 另一个访问控制规则是检查 IPsec 处理信息包的信源和信宿地址的冗余校验。该访问控制规则确保了这些信源地址和信宿地址与从 IPsec 通道远端输出的信息包的信源地址和信宿地址相匹配。

in-router-A 的第一个访问控制规则通过标识 IPsec 通道的两个端点在 IPsec 通道上传送信息。协议 50 - 51 标识了 IPsec。

```
IP Config> update packet-filter
Packet-filter name [ ]? in-router-A
Packet-filter 'in-router-A' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.210
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.216
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
50
Enter ending protocol number [50]? 51
(Enable logging? (Yes or [No]):
Packet-filter 'in-router-A' Config>
```

in-router-A 的第二个访问控制规则检查路由器 A 上 IPsec 处理信息包的信源地址和信宿地址，以确认它们与从路由器 B 中发送信息包的信源地址和信宿地址相同。对 IPsec 通道安全进行冗余检查是不必要的，因为路由器 A 上的出站信息包过滤器不使这样的信息包通过，其信源地址和信宿地址与路由器 B 上入站信息包的信源地址和信宿地址不同。但是，建议在 IETF 安全结构计划中进行冗余检查。

注: 由于路由器 B 正在使用 NAT，所以路由器 A 不能访问路由器 B 的 3.1.0.0 地址。因此，*in-router-A* 的第二个访问控制规则使用地址 223.252.252.210，作为远程信源地址，而将非子网 3.1.0.0 作为远程信源地址。

```
Packet-filter 'in-router-A' Config>
add access
Enter type [E]? IS
Internet source [0.0.0.0]? 223.252.252.210
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 1.1.0.0
Destination mask [255.255.255.255]? 255.255.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
(Enable logging? (Yes or [No]):
Packet-filter 'in-router-A' Config> exit
```

如果希望将与任何访问控制规则都不匹配的包全部发送出去，而不丢弃任何包，则可以配置全部通配的访问控制规则以传送所有的包。但是这项访问控制规则使输入过滤器上的第二个输入访问控制规则无效，因为它传输访问控制规则指定要丢弃的信息包。下例显示了一个访问控制规则:

```
Packet-filter 'in-router-A' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]? 0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable Logging (Yes or [No]):
Packet-filter 'in-router-A' Config> exit
```

然后，配置信息包过滤器 *out-router-A* 的第一个访问控制规则。该访问控制规则将信息包从子网 1.1.0.0 传送到路由器 B 中的信宿地址 223.252.252.210。

```
IP Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config> add access
Enter type [E]? IS
Internet source [0.0.0.0]? 1.1.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
(Enable logging? (Yes or [No]):
Packet-filter 'out-router-A' Config>
```

out-router-A 的第二个访问控制规则允许信息包在 IPsec 通道的两端传输。

```
Packet-filter 'out-router-A' Config>
add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.216
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
50
Enter ending protocol number [50]? 51
(Enable logging? (Yes or [No]):
Packet-filter 'out-router-A' Config>
```

与使用信息包过滤器相同，可为 *out-router-A* 配置全部通配的访问控制规则，以传送与所有访问控制规则都不匹配的通信量。

在路由器 A 上重设 IPsec 和 IP: 完成 IPsec 配置后，请使用 Talk 5 中的 **reset ipsec** 命令，可重新装入具有新 IPsec 配置(在 Talk 6 中创建) 的 SRAM。使用 **reset ipsec** 命令不会影响任何 IP 配置。然后，使用 Talk 5 中的 **reset ip** 命令，动态地重设路由器中的 IP。或者如果要重设所有的组件，在可重新启动路由器。重设 IPsec 和 IP 或重新启动路由器是必要的，以确保重新装入信息包过滤器和访问规则。否则，在接口上可能无法正确支持用户的配置。请参阅第175页的『第16章 配置和监控 IP 安全』和 *Protocol Configuration and Monitoring Reference, Vol.1* 中的 **reset ip** 命令以获取详细信息。

配置路由器 B (IPsec 和 NAT)

IPsec 通道 1 在路由器 B 中接口 1 上有一端点，同时为 IPsec 和 NAT 配置路由器 B 配置。在配置 NAT 时，使用路由器上的出站信息包过滤器，以通过 NAT 转换和 IPsec 封装传输出站信息包。入站信息包先传送给 IPsec 解密，再传送给 NAT 以进行网络地址转换。

配置路由器 B，执行如下:

- 配置 NAT。
- 创建 IPsec 通道。
- 在作为 IPsec 通道端点的路由器接口上，分别创建入站和出站信息包过滤器。
- 创建信息包过滤器的访问控制规则。
- 重设 IPsec。
- 重设 NAT。
- 重设 IP。

本节内容不涉及在路由器 B 中配置 NAT。请参阅第211页的『第19章 网络地址转换的使用』 和第217页的『第20章 配置和监控网络地址转换』以获取有关配置 NAT 的信息。该实例假定已配置 NAT，且 NAPT 地址 223.252.252.210 也是 IPsec 通道的端点。此实例中使用的 NAT 专用地址池为 3.1.0.0，其子网为 255.255.0.0。通过 IPsec 通道 1 传输的入站信息由 IPsec 进行处理，然后传输给 NAT 以转换其中一个地址。

注:

1. 在该实例中，IPsec 通道端点地址和 NAPT 地址是相同的。但是，在相似的情况下，当同时使用 IPsec 和 NAT 时，IPsec 通道端点的地址可以是任何有效的 IP 地址，不一定是 NAPT 地址或一个 NAT 公用地址。
2. 如果不需要 NAT，则可将地址 223.252.252.210 当作 IPsec 通道 1 的端点，将地址域 3.1.0.0 仅当作传送到 IPsec 的信息包的地址域。

创建路由器 B 的 IPsec 通道: 必须配置路由器 B 的 IPsec 通道 1，它与为路由器 A 配置的 IPsec 通道 1 相同。路由器 B 中该通道的本地 IP 地址为 223.252.252.210，远程 IP 地址为 223.252.252.216。所有其他 IPsec 通道参数必须与为路由器 A 配置的参数相同。

配置路由器 B 的信息包过滤器: 与为路由器 A 配置信息包过滤器相同，在路由器 B 中的接口 1 上分别配置入站信息包过滤器 (*in-router-B*) 和出站信息包过滤器 (*out-router-B*)，路由器 B 是 IPsec 通道 1 的端点。

配置路由器 B 的信息包过滤器访问控制规则: 首先，在路由器 B 上配置入站信息包过滤器 *in-router-B* 的第一个入站访问控制规则。该访问控制规则标识出 IPsec 通道的两个端点，并允许路由器 B 接收来自通道的信息包。该信息包滤器 *in-router-B* 的类型为 inclusive (I)。

```
IP Config>
update packet-filter
Packet-filter name [ ] in-router-B
Packet-filter 'in-router-B' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.216
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
50
Enter ending protocol number [50]? 51
Enable logging? (Yes or [No]):
Packet-filter 'in-router-B' Config>
```

然后，可以将第二个访问控制规则添加到 *in-router-B*。

在 IPsec 中不需要对 IPsec 通道的安全进行冗余检验。但是，这项附加的访问控制规则对于 NAT 来说是必须的。注意访问控制规则的类型为 I、N 和 S。

```
Packet-filter 'in-router-B' Config>
add access
Enter type [E]? INS
Internet source [0.0.0.0]? 1.1.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable logging? (Yes or [No]):
Packet-filter 'in-router-B' Config>
```

如果希望将与任何访问控制规则都不匹配的信息包全部发送出去，而不丢弃任何信息包，则可以为 *in-router-B* 配置全部通配的访问控制规则，以传送所有的信息包。但是这项访问控制规则使输入过滤器上的第二个输入访问控制规则无效，因为它传输第二个访问控制规则指定要丢弃的信息包。

然后，在 *out-router-B* 上配置访问控制规则，以将出站信息包从子网 3.1.0.0 传输到 NAT 进行转换，然后传送给 IPsec 处理后通过 IPsec 通道 1 传输。该访问控制规则的类型为 I、N 和 S。

```
Packet-filter name [ ]?
out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? INS
Internet source [0.0.0.0]? 3.1.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 1.1.0.0
Destination mask [255.255.255.255]? 255.255.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable logging? (Yes or [No]):
Packet-filter 'out-router-B' Config>
```

此时为 *out-router-B* 创建 inclusive 访问控制规则，以使经过 IPsec 处理的信息包通过 IPsec 通道 1 传送。

```
Packet-filter 'out-router-B' Config>
add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.210
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.216
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
50
Enter ending protocol number [50]? 51
(Enable logging? (Yes or [No]):
Packet-filter 'out-router-B' Config>
```

如果希望传输与两个访问控制规则均不匹配的信息包，而不丢弃任何信息包，例如，不以 IPsec 通道 1 为目的地的通信量，则可为 *out-router-B* 创建类型为 inclusive 的全部通配的访问控制规则。

重设路由器 B 上的 NAT、IPsec 和 IP: 在启用 NAT 和 IPsec 功能和 IP 访问控制规则发生作用之前，必须重设 NAT、IPsec 和 IP。使用 talk 5 中的 **reset NAT** 和 **reset IPsec** 命令可重设 NAT 和 IPsec。请参阅第217页的『第20章 配置和监控网络地址转换』以获取有关重设 NAT 的详细信息，并参阅第170页的『在路由器 A 上重设 IPsec 和 IP』以获取有关重设 IPsec 的信息。重设 NAT 和 IPsec 后，使用 talk 5 **reset IP** 命令可重设 IP。或者，如果要重设各组件，在可重新启动路由器。

实例 2: 配置具有 ESP 的 IPsec 通道

注意，当通道处于通道模式且通道策略为 ESP 时，将会提示您设置 DF 位。该实例仅显示 IPsec 通道的配置，而未显示信息包过滤器的配置。

```
IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 3
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
IP version (4 or 6) [4]?
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? (Yes or [No]):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0.0.0.0]?
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? (Yes or [No]):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No][No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPsec config>
```

实例 3: 使用 ESP-NULL 算法配置具有 ESP 的 IPsec 通道

注意必须有认证。

```
IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 3
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
IP version (4 or 6) [4]?
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 10.11.12.11
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPsec config>
```

IPv6 通道的 IP 安全

所有 IPsec 功能都适用于 IPv6。在配置 IPv6 的 IPsec 时，查看以下对 IPsec 配置问题的更改:

- 在配置 IPv6 的 IPsec 时，按 IPv6 地址格式(例如，8:0:9:8::1) 输入地址。
- 不会要求您查询对 DF 位的设置。
- 在请求本地和远程信息之前，将对您询问有关请求指定 IPv4 或 IPv6 的附加问题。

第16章 配置和监控 IP 安全

本章说明如何配置和监控 IP 安全及如何使用 IP 安全监控命令。包括以下部分:

- 『访问 IP 安全配置环境』
- 『IP 安全配置命令』
- 第183页的『访问 IP 安全监控环境』
- 第183页的『IP 安全监控命令』

注: 如果您创建 IPsec 隧道以传输 TN3270、APPN-ISR 或 APPN-HPR 通信，并计划使用 BRS 的设置通信优先级，则您需要使用 BRS 的 IPv4 优先权位设置功能。详细信息，请参阅第8页的『将 IP 版本 4 优先位处理用于 IP 安全隧道和次级分段中的 SNA 通信』。

访问 IP 安全配置环境

如果要访问 IP 安全配置环境，请在 Config> 提示符下输入下列命令:

```
   Config>
feature ipsec
   IP Security feature user configuration
   IPsec config>
```

IP 安全配置命令

这部分说明 IP 安全配置命令。请在 IPsec config> 提示符下输入这些命令。

表 33. IP 安全配置命令概述

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add tunnel	添加安全隧道。
Change tunnel	更改安全隧道配置参数值。
Delete tunnel	删除安全隧道。
Disable	在安全方式下禁用所有 IP 安全进程(丢弃同信息包过滤器相匹配的信息包)，或者，在非安全方式禁用所有 IP 安全进程(传送同信息包过滤器相匹配的信息包)，或者，禁用安全隧道。
Enable	启用所有 IP 安全进程，或者启用安全隧道。
List	列出有关全局 IP 安全信息或有关已定义的隧道信息。
Set	设置 Path MTU (PMTU) 时效定时器。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add Tunnel

使用 **add tunnel** 命令，添加定义 IPsec 隧道的参数。

语法:

add tunnel...

tunnel-id

指定要添加的安全隧道标识符的编号。每个 id 在 2212 中必须是唯一的。

有效值: 1 - 65535

缺省值: 无

tunnel-name

可选参数，用于标记隧道。其在 2212 中必须是唯一的。

有效值: 至多 15 个字符；第一个字符必须是字母；不许使用空格。

缺省值: 无

lifetime

隧道处于活动状态的时间，以秒计。数值 0 指示隧道处于永久活动状态。

有效值: 0 - 525600 (0 = 永久活动状态; 525600 = 365 天)

缺省值: 46080 (即 32 天)

encapsulation-mode

加封 IP 信息包的方式。在隧道模式下，加封整个 IP 信息包并生成一个新的 IP 首部；在传输模式下，则不加封 IP 首部。如果安全隧道的一端是路由器，则按照 Internet 工程任务部 (IETF) 的安全结构草案，***必须***使用隧道模式。

有效值: tunnel (*TUNN*) 或 translate (*TRANS*)

缺省值: tunnel (*TUNN*)

tunnel-policy

定义以下隧道策略的四种选项之一: IP 认证首部 (AH)、IP 封装安全有效负载 (ESP) 或这些协议的组合 (AH-ESP 和 ESP-AH)。在 AH-ESP 协议下，首先对出网信息包运行 ESP 加密方式；在 ESP-AH 协议下，则首先对出网信息包运行 AH 认证。对于 ESP 或 AH，有些参数是唯一的。仅在选定了 ESP、AH-ESP 或 ESP-AH 时，才配置加密参数；而仅在选定了 ESP、AH-ESP 或 ESP-AH 并选定了认证时，才对认证参数进行配置。

有效值: AH、ESP、AH-ESP、ESP-AH

缺省值: AH-ESP

IP-version

用于隧道的 IP 版本。

有效值: IPv4 或 IPv6

缺省值: IPv4

local-IP-address

隧道这一端的 IP 地址。根据已配置的 IP 版本，该地址是 IPv4 或 IPv6。

有效值: 已为接口而配置的、或已配置为 2212 内部地址的有效 IP 地址。

缺省值: 为路由器而配置的 IP 地址之一

local-spi

安全关联是使用 AH 或 ESP 以保护连接通信的单向安全连接方式。安全参数的指数 (SPI) 是任意的 32 位数值，与安全隧道相关的安全关联有两种(入站或出站)，该数值能将其中之一单独标识出来。该参数是必需的，对于在本地隧道端接收到的入站信息包，该参数标识出隧道中预期的 SPI。但该数值与另外一

条隧道(具有相同的本地 IP 地址)的本地 SPI 不相匹配。不论隧道的策略是哪一种 (ESP、AH、AH-ESP 或 ESP-AH)，对于一条 IP 安全性隧道的入站通信，仅可配置一种本地 SPI。

有效值: 256 - 65535

缺省值: 256

local-encryption-algorithm

加密算法规则，是用于自本地路由器发送的出站信息包上的 ESP，在配置 ESP 时是必需的。由于受到美国出口法的限制，没有向一些国家提供这些算法规则的一部分或全部。这种加密算法规则必须与远程加密算法规则相匹配。

ESP-NULL 算法规则可防止 ESP 执行加密程序。这种算法规则是提供给所有国家的。如果选定的是 ESP-NULL，则必须通过选择认证算法规则 HMAC-MD5 或 HMAC-SHA-1，以激活用于认证的 ESP。

有效值: DES-CBC、CDMF、3DES 或 ESP-NULL

缺省值: DES-CBC

local-encryption-key

与本地 ESP 加密算法规则一起使用的一个密钥或多个密钥。这些密钥必须和在安全隧道另一端配置的对等密钥相匹配。在选定 ESP-NULL 加密算法规则时则不能配置密钥。

有效值:

- 对于 DES-CBC: 16 进制的字符 (0 - 9、a - f、A - F)
- 对于 CDMF: 16 进制的字符 (0 - 9、a - f、A - F)
- 对于 3DES: 三个分开的、互不相同的密钥，都是 16 进制的字符 (0 - 9、a - f、A - F)

缺省值: 无

padding-for-local-encryption

添加到出站 ESP 信息包的附加填充字符，以字节计大小。当加密算法规则的结果为加密后的信息包与原始信息包大小相同时，附加填充字符可用于掩盖加密的 IP 信息包的真实大小。ESP 填充字符数必须是 8 的倍数。如果配置了不能被 8 整除的数值，则进位舍入，将该数值改成被 8 整除的数值。

当加密算法规则是 ESP-NULL 时，填充字符不是必需的，因为 ESP-NULL 算法规则对原始信息包的大小添加了一字节。如果配置了本地加密填充字符，则忽略该数值。

有效值: 0 - 120

缺省值: 0

local-ESP-authentication

在需要的情况下，选择本地 ESP 认证。如果加密算法规则是 ESP-NULL，则认证是必需的。

有效值: Yes 或 No

缺省值: Yes

local-authentication-algorithm

用于出站信息包的认证算法规则。这是用于 ESP 的可选参数，该参数不是必需

的，除非您选定了 ESP 认证。对于 AH、AH-ESP 或 ESP-AH，该参数是必须的。所使用的认证算法必须与在 IPsec 隧道远端所使用的远程认证算法规则相匹配。

有效值：HMAC-MD5 或 HMAC-SHA

缺省值：HMAC-MD5

local-authentication-key

与本地认证算法规则一起使用的密钥。该密钥必须和在 IPsec 隧道另一端所配置的对等密钥相匹配。如果策略是 AH、AH-ESP 或 ESP-AH，或者，如果策略是 ESP 并且已配置了本地 ESP 认证算法规则，则该密钥是必需的。

有效值：

- 对于 HMAC-MD5：32 位的十六进制的字符 (0 - 9、a - f、A - F)
- 对于 HMAC-SHA：40 位的十六进制字符 (0 - 9、a -f、A - F)

缺省值：无

remote-IP-address

隧道远端的 IP 地址。这个参数是必需的。根据已配置的 IP 版本，该地址是 IPv4 或 IPv6。

有效值：有效的 IP 地址

缺省值：无

remote-spi

安全关联是使用 AH 或 ESP 以保护连接通信的单向安全连接方式。安全参数的指数 (SPI) 是任意的 32 位数值，与安全隧道相关的安全关联有两种(入站或出站)，该数值能将其中之一单独标识出来。该参数是必需的，它在发送给远程主机的出站信息包的 ESP 或 AH 中标识了预期的 SPI。但该数值与另外一条隧道(具有相同的远程 IP 地址)的远程 SPI 不能相匹配。不论隧道的策略是哪一种 (ESP、AH、AH-ESP 或 ESP-AH)，对于一条 IPsec 隧道的出站通信量，仅可配置一种本地 SPI。

有效值：1 - 65535

缺省值：256

remote-encryption-algorithm

解密算法规则，用于从远程主机接收的入站信息包。它必须与本地加密算法规则相匹配。

ESP-NULL 算法规则可防止 ESP 执行加密程序。如果选定的是 ESP-NULL，则必须通过选择认证算法规则 HMAC-MD5 或 HMAC-SHA-1 认证算法规则中的一种，以激活用于认证的 ESP。

有效值：DES-CBC、CDMF、3DES 或 ESP-NULL

缺省值：本地加密算法规则

remote-encryption-key

与远程 ESP 加密算法规则一起使用的密钥。这些密钥必须和在安全隧道另一端配置的对等密钥相匹配。在选定 ESP-NULL 加密算法规则时不能配置密钥。

有效值：

- 对于 DES-CBC：16 进制的字符 (0 - 9、a - f、A - F)

- 对于 CDMF: 16 进制的字符 (0 - 9、a - f、A - F)
- 对于 3DES: 三个分开的、互不匹配的密钥，都是 16 进制的字符 (0 - 9、a - f、A - F)

缺省值: 无

verification-of-remote-encryption-padding

确定是否验证所接收信息包的加密填充字符大小。

有效值: Yes 或 No

缺省值: No

padding-for-remote-encryption

在所接收的 ESP 信息包中预期的附加填充字符，以字节计大小。仅当数值 *verification-of-remote-encryption-padding* 是 Yes 时，该参数才是必需且有效的。ESP 填充数值必须是 8 的倍数。如果配置了不能被 8 整除的数值，则将进行进位舍入，把该数值改成被 8 整除的数值。

有效值: 0 - 120

缺省值: 0

remote-ESP-authentication

如果需要，选择入站信息包的远程 ESP 认证。

有效值: Yes 或 No

缺省值: Yes

remote-authentication-algorithm

用于入站信息包的认证算法规则。这是用于 ESP 的可选参数，该参数不是必需的，除非您选定了 ESP 认证。对于 AH 或 AH 和 ESP 的组合 (AH-ESP 或 ESP-AH)，该参数是必需的。所使用的认证算法必须与在 IPsec 隧道远端所使用的本地认证算法规则相匹配。

有效值: HMAC-MD5 或 HMAC-SHA

缺省值: HMAC-MD5

remote-authentication-key

与远程认证算法规则一起使用的密钥。该密钥必须和在安全隧道另一端所配置的对等密钥相匹配。如果配置了远程 ESP 认证算法规则，则该密钥在 AH、AH-ESP 和 ESP-AH 及 ESP 中是必需的。

有效值:

- 对于 HMAC-MD5: 32 位十六进制的字符 (0 - 9、a - f、A - F)
- 对于 HMAC-SHA: 40 位的十六进制字符 (0 - 9、a -f、A - F)

缺省值: 无

enable-replay-prevention

指定是否启用“避免再次处理功能”。如果启用“避免再次处理功能”，则监控 IP 安全首部的顺序号，以防止隧道接受器处理重复的信息包。建议不要使用“避免再次处理功能”，因为当发送器顺序号计数器达到极限时，隧道安全关联必须处于不活动状态。当出现这种情况时，需要人工干预，重新启动现存的安全关联或创建新的安全关联。

此外，如果在启用“避免再次处理功能”时，您使用 **reset ipsec** 命令重置 IPsec，则您必须确保在 IPsec 隧道的另一端的路由器上对 IPsec 也进行了重置。为在隧道的两端重新初始化顺序号，这样的重置是必需的。如果仅在隧道的一端重置 IPsec，就可能出现因顺序号不匹配，隧道两端的路由器丢弃信息包。

有效值：Yes 或 No

缺省值：No

DF-bit 在隧道模式下，指定对安全隧道外部首部中的 Don’t Fragment (DF) 位执行处理。可在 IPv4 首部中设置该位，以指定不能分段的信息包。DF 位参数指示 2212 应如何处理入网信息包上的 DF 位 - 是否将在内部首部中查找到的 DF 位数值复制到外部首部上，或者，是否设置或清除外部首部中的位。

如果 DF 位已经设定且不能对信息包进行分段，则 IPsec 使用 Path MTU (PMTU) Discovery 功能。详细信息，请参阅第166页的『路径 MTU 查找』。

有效值：Copy、Set、Clear

缺省值：Copy

enable-tunnel

指定是否启用此隧道。所启用的隧道将不过滤信息包；直到配置了信息包过滤器以定义此 IPsec 隧道将要连接的接口，并且在 2212 上重置了或重新启动了 IP 时为止。您可使用 **reset ip** 命令以重置 IP。

有效值：Yes 或 No

缺省值：Yes

Change Tunnel

使用 **change tunnel** 命令，更改先前由 **add tunnel** 命令配置的 IPsec 隧道参数。

语法:

change tunnel... 有关可更改的参数列表，请参阅 **add tunnel** 命令。

Delete Tunnel

使用 **delete tunnel** 命令，删除 IPsec 隧道。

语法:

delete tunnel *tunnel-id tunnel-name* **all**

tunnel-id

指定将要删除的 IPsec 隧道的标识符。

有效值：1 - 65535

缺省值：1

tunnel-name

指定将要删除的 IPsec 隧道名称。

有效值：任何已配置的隧道名称

缺省值：无

all 指定在此接口上将要删除的所有 IPsec 隧道。

Disable

使用 **disable** 命令，以安全方式禁用某个 IPsec 隧道或禁用所有的 IPsec 隧道(丢弃与 IPsec 过滤器相匹配的信息包)，或者，以非安全方式禁用(传送与 IPsec 过滤器相匹配的信息包)。

语法:

disable ipsec drop
ipsec pass
tunnel ...

ipsec drop
以安全方式在路由器上禁用 IP 安全。所有 IPsec 隧道都将被禁用，但使用信息包过滤器规则的安全隧道信息，以标识与 IPsec 隧道信息包过滤器相匹配的信息包。相匹配的信息包被丢弃。

ipsec pass
以非安全方式在路由器上禁用 IP 安全。禁用全部 IPsec 隧道。与 IPsec 隧道信息包过滤器相匹配的信息包，将作为普通的通信被转发。

tunnel *tunnel-id* **all**
在指定隧道或在所有隧道上禁用 IP 安全。

tunnel-id
指定将要禁用的安全隧道标识符。

有效值: 1 - 65535

缺省值: 1

all 全部隧道。

Enable

使用 **enable** 命令，在接口或单一隧道上启用 IP 安全性协议。您必须在单独启用的 IPsec 隧道活动之前，在路由器上全局启用 ipsec。

语法:

enable ipsec
tunnel ...

ipsec 在整个路由器上启用 IP 安全。

tunnel *tunnel-id* **all**
在指定隧道或在所有隧道上启用 IP 安全。

tunnel-id
指定将要启用的安全隧道标识符。

有效值: 1 - 65535

缺省值: 1

all 全部隧道。

List

使用 **list** 命令，显示当前的 IP 安全配置。全局隧道包括路由器中的所有隧道，既包括活动的又包括被定义的。而全部隧道包括在此接口上配置的所有隧道，既包括活动的又包括被定义的。活动的隧道是指当前活动的那些隧道；被定义的隧道是指那些经过定义的、但非活动的隧道。

语法:

list ... all

global

tunnel

active *tunnel-id tunnel-name* all

defined *tunnel-id tunnel-name* all

例 1: 列出所有的 IPsec 隧道

```
IPsec config>list all

IPsec is ENABLED

IPsec Path MTU Aging Timer is 20 minutes

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  test                    1.1.1.1          2.1.1.1  TUNN   Enabled
      2  test2                   1.1.1.1          1.1.1.3  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2          1.1.1.1          1.1.1.3  TRANS  ESP     ******************
    1          1.1.1.1          2.1.1.1  TUNN   AH      ******************
```

例 2: 列出具有 ESP 策略和 ESP 算法规则的 IPsec 隧道

```
IPsec config>li tun 1000

Tunnel  Name             Mode   Policy   Life   Replay  Rcv  IPsec  State
ID                                              Prev    Win  Vers
------  ---------------  -----  ------  ------  ------  ---  -----  --------
1000    t1000            TUNN   ESP      46080    No    ---   V2    Enabled

Handling of DF bit in outer header:  COPY

Local Information:

      IP Address: 10.11.12.10
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: HMAC-MD5
Remote Information:

      IP Address: 10.11.12.11
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: HMAC-MD5
```

Set

设置 Path MTU (PMTU) 的时效定时器。

语法:

set ... path

path-MTU-aging-timer

该参数可定义 2212 将隧道 MTU 重新设置到最大之前所经过的时间，以分钟计算。

有效值: 10 - 60 分钟; 0 表示禁用

缺省值: 10

访问 IP 安全监控环境

访问 IP 安全监控环境，在 OPCON 提示符 (*) 下输入 **t 5**:

```
   *
t 5
```

接着，在 **+** 提示符下输入下列命令:

```
+ feature ipsec
IPsec>
```

IP 安全监控命令

本节说明 IP 安全监控命令。请在 IPsec> 提示符下输入这些命令。

表 34. IP 安全监控命令概述

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add tunnel	动态地添加安全隧道
Change tunnel	动态更改安全隧道配置参数值。
Delete tunnel	动态删除安全隧道。
Disable	在安全方式下动态禁用所有 IP 安全进程(丢弃相匹配的信息包)，或者，在非安全方式下禁用所有 IP 安全进程(转发相匹配的信息包)，或禁用特定的安全信息包。
Enable	动态启用所有 IP 安全进程，或者，启用安全隧道。
List	列出有关全局的 IP 安全信息，或者列出有关活动的和已定义的隧道信息。
Reset	重置 IP 安全或重置安全隧道。该命令重新装入在 Talk 话 6 中创建的配置。重置操作将使由 Talk 6 所配置的参数取代由 Talk 5 所配置的参数。
Restart	重新启动 IP 安全或重新启动安全隧道。该命令重新装入由 Talk 5 命令动态配置的配置信息。
Set	动态设置 Path MTU (PMTU) 的时效定时器。
Stats	显示所有的或某个活动的隧道的统计信息。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add Tunnel

动态添加安全隧道

语法:

add tunnel ...

有关这些参数的说明，请参阅 第175页的『IP 安全配置命令』下的 **add tunnel** 命令。

Change Tunnel

动态更改安全隧道。

语法:

change tunnel ...

有关这些参数的说明，请参阅 第175页的『IP 安全配置命令』下的 **add tunnel** 命令。

Delete Tunnel

使用 **delete** 命令，动态删除某个安全隧道或所有的安全隧道。

语法:

delete tunnel *tunnel-id tunnel-name* **all**

tunnel-id

指定将要删除的 IPsec 隧道的标识符。

有效值: 1 - 65535

缺省值: 1

tunnel-name

指定将要删除的 IPsec 隧道名称。

有效值: 任何已配置的隧道名称

缺省值: 无

all 指定删除此接口上的所有 IPsec 隧道。

Disable

使用 **disable** 命令，在所有接口上或单一隧道上动态禁用 IP 安全协议。

语法:

disable ipsec drop

ipsec pass

tunnel ...

ipsec drop

以安全方式在路由器上禁用 IP 安全。全部 IPsec 隧道都将被禁用，但使用信息包过滤器规则的安全隧道信息，以标识与 IPsec 隧道信息包过滤器相匹配的信息包。相匹配的信息包被丢弃。

ipsec pass

以非安全方式在路由器上禁用 IP 安全。禁用全部 IPsec 隧道。与 IPsec 隧道信息包过滤器相匹配的信息包，将作为普通的通信被转发。

tunnel *tunnel-id* **all**

在指定隧道或在所有隧道上禁用 IP 安全。

tunnel-id

指定将要禁用的安全隧道标识符。

有效值: 1 - 65535

缺省值: 1

all 全部隧道。

Enable

使用 **enable** 命令，动态地在所有接口或单一隧道上启用 IP 安全协议。您必须在单独启用的 IPsec 隧道活动之前，在路由器上全局启用 ipsec。

注: 如果在禁用 IPsec 的状态下重新启动路由器，则不能动态地启用 IPsec。

语法:

enable ipsec

tunnel ...

ipsec 在整个路由器上启用 IP 安全。

tunnel *tunnel-id* **all**

tunnel-id

指定将要启用的安全隧道标识符。

有效值: 1 - 65535

缺省值: 1

all 全部隧道。

List

使用 **list** 命令，显示当前的 IP 安全配置。全局隧道包括路由器中的所有隧道，既包括活动的又包括被定义的。而全部隧道包括在此接口上配置的所有隧道，既包括活动的又包括被定义的。活动的隧道是指当前活动的那些隧道；被定义的隧道是指那些经过定义的、但非活动的隧道。

语法:

list ... all

global

tunnel

active *tunnel-id tunnel-name* all

defined *tunnel-id tunnel-name* all

例 1: 列出所有的活动隧道

```
IPsec>li tunnel ?
ACTIVE
DEFINED
IPsec>li tunnel active
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2          1.1.1.1          1.1.1.3  TRANS  ESP     ****************
    1          1.1.1.1          2.1.1.1  TUNN   AH      ****************
```

例 2: 列出已接收到 『packet too big』 消息的一条活动隧道。

```
IPsec>li tun act 1

Tunnel      Name       Mode  Policy  Life  Replay       Tunnel       PMTU
  ID                                       Prev      Expiration
------ --------------- ----- ------ ------ ------ ------------------ -----
     1 tofran2         TUNN  AH      46080   No   10:49  May  8 1998 1420 1

Local Information:

      IP Address: 2001:1::6101 2
      Authentication:  SPI:   257    Algorithm: HMAC-MD5
      Encryption:  SPI: -----    Encryption Algorithm: --------
                                 Extra Pad: ---
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 2001.1..86
  Authentication:  SPI:   257    Algorithm: HMAC-MD5
      Encryption:  SPI: -----    Encryption Algorithm: --------
                                 Verify Pad?: ---
                                 ESP Authentication Algorithm: ----------
```

1 如果未接收到太大的信息包，则 PMTU 显示为 n/a。

2 这是 IPv6 地址。如果 IP 版本是 IPv4，则显示一条消息，该消息定义了如何处理 DF 位: COPY、SET 或 CLEAR。

例 3: 列出所有的隧道

```
IPsec>li all

IPsec is ENABLED

IPsec Path MTU Aging Timer is 30 minutes

Defined Manual Tunnels for IPv4:
--------------------------------------------------------------------------------
   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------

Defined Manual Tunnels for IPv6:
--------------------------------------------------------------------------------
ID=       1  Name= tofran2           Mode= TUNN    State= Enabled
Local IP address=  2001:1::6101
Remote IP address= 2001:1::86


Tunnel Cache for IPv4:
--------------------------------------------------------------------------------
```

```
 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  --------------  --------------  -----  ------  -----------------

Tunnel Cache for IPv6:
-------------------------------------------------------------------------------
ID=     1  Mode= TUNN   Policy= AH      Expiration= 10:49  May  8 1998
Local IP Address= 2001:1::6101
Remote IP Address= 2001:1::86
```

Reset

使用 **reset** 命令，在路由器或单一隧道上动态启用 IP 安全性。您在重置 IPsec 或隧道之后，要确保使用 **reset IP** 命令重置 IP 配置。对于重新装入存取控制信息，如信息包过滤器及其存取控制规则，这样的操作是必需的。如果您不重置 IP，则信息包过滤器及存取控制规则可能不支持您的新 IPsec 配置。

使用 **reset** 命令时，也可选择重新引导路由器的操作。然而，重新引导路由器将在一定时间内使路由器从网络上断开，相反，**reset** 命令却仅中断 IP 的例程。

语法:

reset ipsec

tunnel *tunnel-id tunnel-name* all

ipsec 在 2212 上重置 IP 安全。暂时禁用 IP 安全，然后再重新启动。当禁用 IP 安全时，将丢弃任何经 IPsec 隧道正常处理的信息包，直到重置操作结束。重置 IP 安全并不影响在 2212 上的其它功能。该命令激活由 Talk 6 创建的 IP 安全配置。Talk 6 IP 安全配置对 Talk 5 的配置进行覆盖。

tunnel 在指定隧道上重置 IP 安全配置。如果在重置期间禁用隧道，则隧道配置通过 SRAM 配置重新建立，但是，重置后的隧道仍处于禁用状态。

tunnel-id

指定将要重置的安全隧道标识符。

有效值: 1 - 65535

缺省值: 1

tunnel-name

指定将要重置的安全隧道名称。

有效值: 任何已配置的隧道名称

缺省值: 无

all 全部隧道。

Restart

使用 **restart** 命令，动态地在路由器上或单一隧道上重新启动 IP 安全。这将重新启动由 Talk 5 创建的临时配置。此时，会话 6 IP 安全性配置并不覆盖 Talk 5 的配置。

语法:

restart ipsec

tunnel *tunnel-id tunnel-name* all

ipsec 在 2212 上重新启动 IP 安全。

tunnel 在指定的隧道上重新启动 IP 安全。

tunnel-id

指定将要重置的安全隧道标识符。

有效值: 1 - 65535

缺省值: 1

tunnel-name

指定将要重置的安全隧道名称。

有效值: 任何已配置的隧道名称

缺省值: 无

all 全部隧道。

Set

动态设置 Path MTU (PMTU) 时效定时器。

语法:

set ... path

有关 *path-MTU-aging-timer* 的说明，请参阅在第 183 页上的 Talk 6 中的 **set** 命令。

Stats

使用 **stats** 命令，显示有关指定隧道或所有隧道的统计信息。例如，**stats** 命令显示发送的和接收的信息包。

语法:

stats *tunnel-id tunnel-name* **all**

tunnel-id

指定安全隧道的标识符。

有效值: 1 - 65535

缺省值: 1

tunnel-name

指定已配置的安全隧道名称。

有效值: 任何已配置的隧道名称

缺省值: 无

all 显示有关在 2212 上配置的所有隧道的统计信息。

实例:

```
IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0
```

```
Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0
```

第17章 使用 2 层通道连接协议 (L2TP)

2 层通道连接协议 (L2TP) 是 IETF 推荐的一种标准协议，此协议主要用于在面向信息包的数据网络，如 UDP/IP 上的通道连接 PPP。L2TP 为面向连接的协议。

L2TP 概要

L2TP 允许多个分离的、或独立的协议域共享公共访问基础设施，其中包括调制解调器、访问服务器和 ISDN 路由器。另外，L2TP 还可允许通道连接 PPP 链路层，如 HDLC 和异步 HDLC。使用这些通道后，已连接上的拨号服务器位置便可与提供网络访问的位置断开关联。

传统上的 Internet 上的拨号网络服务仅向注册的 IP 地址提供。但是， L2TP 定义了一个新级别的虚拟拨号应用程序，此程序允许 Internet 上存在多个协议和未注册的 IP 地址。在现有 Internet 基础设施上，对于通过 PPP 实现私人寻址的 IP、IPX 和 AppleTalk 拨号器，此级别的网络应用程序能够提供极大的支持。

无论是对最终用户、企业，还是对 Internet 服务供应商而言，这些多协议虚拟拨号应用程序提供的支持都极有益处。其原因是，该协议允许共享访问和核心基础设施的重要投资，并在最终用户访问此服务时支持使用本地呼叫。

另外，在现有 Internet 基础设施中，L2TP 还可确保非 IP 协议应用程序中已有投资的安全使用。

图17 展示了使用 ISDN 的 L2TP 网络样本。在 L2TP 网络访问集线器 (LAC) 和 L2TP 网络服务器 (LNS) 之间，此网络可使用任何介质类型。

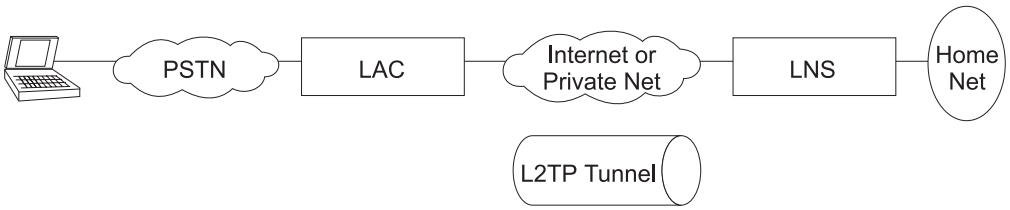


图 17. L2TP 网络样本

L2TP 词汇

描述 L2TP 时将使用如下词汇:

Attribute Value Pair (AVP)(属性值配对)
编码消息类型和消息内容的一种常用方法。在接受 L2TP 互操作性的同时，这种方法又最大可能地提高了其扩展功能。

L2TP Access Concentrator (LAC)(L2TP 访问集中器)
与一个或多个公共服务电话网络 (PSTN) 或 ISDN 线相连的一种设备。此设备能够处理 PPP 操作和 L2TP 协议操作。 LAC 提供了 L2TP 操作所需的介质。L2TP 将通信内容传送到一个或多个 L2PT 网络服务器 (LNS)，并且能够贯穿 PPP 网络携带的所有协议。

L2TP Network Server (LNS)(L2TP 网络服务器)

LNS 在任何可作为 PPP 终端站使用的平台上运作。LNS 负责处理服务器一方的 L2TP 协议。 由于 L2TP 仅依靠 L2TP 通道到达前使用的唯一介质，因此 LNS 仅有一个唯一的 LAN 或 WAN 接口；但是，它仍然可以终止从 LAC 支持的 PPP 接口到来的呼叫。

Network Access Server (NAS)(网络访问服务器)

向用户提供临时请求式网络访问服务的一种设备。这种访问是使用 PSTN 或 ISDN 线路的点到点形式。

Session (Call)(会话(呼叫))

当拨号用户与 LNS 间试图建立端到端 PPP 连接时，L2TP 创建会话。此会话的数据报经由 LAC 和 LNS 间的通道进行传输。LNS 和 LAC 维护每个连接到 LAC 用户的状态信息。

Tunnel (通道)

通道由 LNS-LAC 对定义，主要用于在 LAC 和 LNS 间传输数据报。一个单独的通道可以传送多个会话。对相同通道的控制连接操作既可以控制所有会话的建立、释放和维护，也可以控制通道本身。

支持的功能

L2TP 在 UDP/IP 上运行，并支持如下功能:

- 通道连接单独的用户拨入客户机
- 通道连接小型路由器，例如，以认证的用户概要为基础，只有一条静态路径可以设置的路由器
- 呼叫启动方向可以是从 LAC 到 LNS (入网)、从 LNS 到 LAC (出网)，也可以由任意一个对等实体(两者)启动。出网会话可以使用固定的 L2TP 会话或即时拨号 L2TP 会话。
- 单信道多呼叫
- PAP、CHAP 和 MS-CHAP 代理认证
- 代理 LCP
- LAC 处未使用代理 LCP 时重启 LCP
- 通道端点认证
- 传输代理 PAP 口令时使用的隐藏 AVP
- 使用本地 rhelm (也就是 用户 @rhelm) 查询表实现通道连接
- 在 AAA 子系统中使用 PPP 用户名查询表实现通道连接
- 使用 SNMP 管理 L2TP 通道。见*Protocol Configuration and Monitoring Reference Volume 1*中的 『SNMP 管理』。

注: Rhelm 通道连接要求用户名使用 *名称 @rhelm* 格式。使用这种方法通道连接要求软件查看两个图表，这样可以确定拨入用户将要以通道连接到的目的地。使用此种通道连接方式的益处是: 定义了 rhelm 及其匹配用户名后，您便可以以通道连接至相同的目的地。

基于用户的通道连接在单独的图表中解决。此表赋予您这样一种粒度，即您可以将每个用户以通道连接至唯一的目的地。

- LNS 的 BRS (作为 PPP 端点)
- 使用 **delete interface** 命令删除 L2TP 设备的能力
- 动态重新配置 L2TP 设备的能力
- 建立排序、排队、再传输和流控制通道。L2TP 也在数据通道上执行排序、排队和流控制。
- 设置 L2TP UDP 端口以便在该端口上建立 IP 安全过滤器的能力。
- L2TP 路由器客户机。L2TP 路由器客户机采用『客户机启动』(也常称为自主通道连接)模式。不论服务供应商的拓扑结构如何，此功能都可以提供安全、通道连接和多协议的虚拟专用网络 (VPN)。这样，客户机和 LAC 就同时进入了一个物理硬件。
- 以远程主机名匹配情况为基础，将入网呼叫连至正确的通道。如果远程主机名与任何用于主机名匹配的通道都不匹配，则呼叫将在不使用远程主机名匹配的呼入网上完成。

  注: 如果已在相同的 LAC 和 LNS 配对间配置了多个网络映射，请确保每个映射都只对应一个通道。
- 不使用远程主机名匹配的呼入网络的自动 IP、IPX 和桥接配置。使用远程主机名匹配的呼出网络和呼入网络必须手动配置。

定时注意事项

使用路由后的网络通道传输 PPP 信息包会自然地产生一些值得注意的问题。L2TP 假定 LAC 和 LNS 间连接时可能出现的延迟时间不会使通道连接的对等实体超时。如果对等实体间的等待时间几次达到或超过 PPP 状态机的超时时间(通常为 3 秒)，则可能会阻碍连接。请注意，如果 LAC 和 LNS 间的等待时间真的如此之长，那么即使人工保持 PPP 状态机的活动状态，对等实体间也通常会因连接性如此之差而根本无法实现连接。如果两端的实体都有这种能力，则 PPP 超时延长后还可取得不十分稳定的连接效果。

除等待时间外，LAC/LNS 对和 LAC/Client 对间的带宽不匹配也会带来一些问题。例如，如果 LAC 和LNS 间的实际带宽明显小于 PPP 客户机的带宽，则 LAC 在发送信息包到 LNS 时可能会耗时过多。从另一方面来看，如果和拨入客户机的连接速度相比，LNS 和 LNS 主网络上的主机间的连接速度过高，则 LNS 也可能会因尽力发送数据到 LAC 而负载过重。为解决这一问题，L2TP 使用了一系列内部和外部流控制技术。

LCP 注意事项

使用代理 LCP 时，LAC 协商 LCP，而 PPP 则继续在 LNS 处执行处理。LAC 将 LCP 选项转发到 LNS，以便 LNS 清楚协商的内容。对于客户机和 LAC 协商的参数，LNS 必须保留一定的弹性。如果 LNS 无法接受某些参数，则 L2TP 尝试重新协商 LCP，方法是：通过通道向客户机发送*LCP 配置请求*。

要求 LNS 保留一定的弹性主要是针对 MRU 而言的。在 IBM LNS 上，配置的 MRU 是赋予代理 LCP 的最大额度。如果 LAC 发送的代理 LCP 消息中的值大于 LNS 上配置的 MRU，则 L2TP 将尝试重新协商 LCP。在新 LCP 中，MRU 值等于配置的 MRU 值，而无须更改 LAC 发送的其它 LCP 选项。

配置 L2TP

如要配置 L2TP:

1. 使用 **feature** 命令访问 L2TP 功能部件。

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. 启用 L2TP。

```
Layer-2-Tunneling config> enable l2tp
```

3. 添加所有需要的 L2TP 网络。如果配置严格限制为 LAC，则无须添加任何 L2TP 网络。

```
Layer-2-Tunneling
Config>ADD L2-NETS
Additional L2 nets:  [0]? 10
Add unnumbered IP addresses for each L2 net? [Yes]: yes
Adding device as interface 31
Defaulting Data-link protocol to PPP
Adding device as interface 32
Defaulting Data-link protocol to PPP
Adding device as interface 33
Defaulting Data-link protocol to PPP
Adding device as interface 34
Defaulting Data-link protocol to PPP
Adding device as interface 35
Defaulting Data-link protocol to PPP
Adding device as interface 36
Defaulting Data-link protocol to PPP
Adding device as interface 37
Defaulting Data-link protocol to PPP
Adding device as interface 38
Defaulting Data-link protocol to PPP
Adding device as interface 39
Defaulting Data-link protocol to PPP
Adding device as interface 40
Defaulting Data-link protocol to PPP
```

4. 配置入网 L2TP 通道。

   如要使用 AAA 本地列表配置通道:

```
Config>add tunnel-profile
Enter name:  []? lns.org
Enter hostname to use when connecting to this peer: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: lns.org
      Tunnel Server: 11.0.0.1
      Hostname: lac.org

 User 'lns.org' has been added
 Config>
```

   您可以使用前一实例配置 LAC 上的通道认证，以及用『用户 @lns.org.』格式配置『rhelm』通道连接。

   您可以将通道认证和授权设定为在某一 RADIUS 服务器上完成。详情请参阅*Using and Configuring Features*中的『使用认证、授权和记帐 (AAA) 安全』。

   如要在 LAC 上按 PPP 用户名使用 AAA 本地列表或 RADIUS 通道连接:

```
Config>add ppp-user
Enter name:  []? peter
Password:
Enter again to verify:
Will 'peter' be tunneled? (Yes, No): [No] Y
Enter hostname to use when connecting to this peer: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1
```

```
      PPP user name: peter
      Tunnel Server: 11.0.0.1
      Hostname: lac.org

 Is information correct? (Yes, No, Quit): [Yes]

 User 'peter' has been added
 Config>
```

如果需要，为入网通道配置远程主机名匹配。现在假定前一配置用于网络 10:

```
Config> net 10
     L2TP 10> set remote-hostname
     Remote Tunnel Hostname: [] ibm.com
```

注: 如要关闭远程主机名匹配，请使用下列命令:

```
    Config> net 10
         L2TP 10> set any-remote-hostname
```

5. 配置任意一个 L2TP 出网(或两个)通道。在下面的实例中， LAC 的 IP 地址为 1.1.1.1，而 LNS 的 IP 地址为 1.1.1.2。 LNS 的配置目的是为来自 LAC 的请求发出即时拨号 ISDN 呼叫到 5552160。

   LNS 配置:

```
Config> add tunnel-profile
     Enter name:  []? lac.org
     Enter hostname to use when connecting to this peer: []?
lns.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

            Tunnel name: lac.org
               Endpoint: 1.1.1.1
               Hostname: lns.org

     User 'lac.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lac.org
     L2TP 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN, V34)? [ISDN]
        Outbound calling address: 5552160
        Outbound calling subaddress:
     L2TP 10>
     L2TP 10> encapsulator
     PPP 10> set name vickie 1
     L2TP 10>
     L2TP 10> exit
     Config> add ppp-user larry 2
```

   注:

   a. 设置认证名以备认证 LNS 设备。有些提示本例并未显示，如欲获得这些提示的详细信息，请参阅 *Access Integration Services 软件用户指南* 中的 『配置 PPP 认证』。

   b. 添加需要在 LNS 上认证的用户。有些提示本例并未显示。有关命令语法和选项的说明，请参阅 *Access Integration Services 软件用户指南* 中"配置 CONFIG 进程"一章的 Add 命令。

   LAC 配置:

```
Config>
add tunnel-profile
     Enter name:  []? lns.org
     Enter hostname to use when connecting to this peer: []?
lac.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

            Tunnel name: lns.org
               Endpoint: 1.1.1.1
               Hostname: lac.org

     User 'lns.org' has been added
     Config>
     Config> add dev dial-in  1
```

注:

a. 用于发出物理呼叫。

6. 配置任意一个 L2TP 路由器客户机。下面是使用 L2TP 路由器客户机功能建立的 L2TP 箱到箱连接。此连接的设置为单向即时拨号。

LNS 配置:

```
Config> add tunnel-profile
     Enter name:  []? lac.org
     Enter hostname to use when connecting to this peer: []?
lns.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

            Tunnel name: lac.org
               Endpoint: 1.1.1.1
               Hostname: lns.org

     User 'lac.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lac.org
     L2TP 10> encapsulator
     PPP 10> set name donald   1
     PPP 10> exit
     L2TP 10> exit
     Config>
     Config> add ppp-user bruce  2
     Config>
```

注:

a. 设置认证名以备认证 LNS 设备。有些提示本例并未显示，如欲获得这些提示的详细信息，请参阅 *Access Integration Services 软件用户指南* 中的 『配置 PPP 认证』。

b. 添加需要在 LNS 上认证的用户。有些提示本例并未显示。有关命令语法和选项的说明，请参阅 *Access Integration Services 软件用户指南* 中“配置 CONFIG 进程”一章的 Add。

LAC 配置:

```
Config>
add tunnel-profile
     Enter name:  []? lns.org
     Enter hostname to use when connecting to this peer: []?
lac.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

            Tunnel name: lns.org
               Endpoint: 1.1.1.1
               Hostname: lac.org

     User 'lns.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction inbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lns.org
     L2TP 10> encapsulator
     PPP 10> set name bruce  1
     PPP 10> exit
     L2TP 10> exit
     Config>
     Config> add ppp-user donald  2
     Config>
```

注:

a. 设置认证名以备认证 LNS 设备。有些提示本例并未显示，如欲获得这些提示的详细信息，请参阅 *Access Integration Services 软件用户指南* 中的『配置 PPP 认证』。

b. 添加需要在 LNS 上认证的用户。有些提示本例并未显示，如欲获得这些提示的详细信息，请参阅 *Access Integration Services 软件用户指南* 中的『**add** Config 命令』。

7. 如果需要，使用 **set** 命令配置各种 L2TP 参数。
8. 如果需要，使用 encapsulator 命令为所有 L2 网络配置 PPP 参数。

```
Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>
```

PPP 配置完毕后，输入 **exit** 返回 L2TP 配置环境。

9. 使用 **enable** 命令启用所有 L2TP 功能。

第18章 配置和监视 L2TP

本章主要介绍 L2TP 协议配置和可操作命令。包括以下各节:

L2TP 配置命令

表35总结了 L2TP 配置命令，而本节的其余部分则对这些命令进行了详尽的解释。在 L2TP Config> 提示符下输入这些命令。

表 35. L2TP 配置命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	添加 L2TP 网络或对等实体。
Delete	从配置中删除 L2TP 对等实体。
Disable	禁用 L2TP。
Enable	启用 L2TP。
Encapsulator	允许配置所有 L2TP 网络的 PPP 参数。
List	显示 L2TP 配置的相关信息。
Set	允许设置缓冲区、呼叫接收窗口及其它 L2TP 参数。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add

使用 **add** 命令可添加 L2TP 对等实体 (LAC 或 LNS) 或 L2 网络。每个在此路由器终止的并发 PPP 会话，都需要一个 L2 网络。隧道连接的 PPP 会话的终点便是此隧道的 LNS 端点。

语法: **add**
L2-nets

第194页的『配置 L2TP』 中包含 **add** 命令的一个实例。

L2-nets

注: 此命令输入时可以全部使用小写。第一个字符使用大写只是为了清晰起见。

向 L2TP 配置添加 L2 网络。每个在此路由器终止的并发 PPP 会话都需要一个 L2 网络。如果此路由器严格限制为作为 LAC 使用，则无需任何虚拟 L2 网络。输入此命令时，系统会提示输入附加网络数目，并询问是否需要为每个 L2 网络添加不编号的 IP 地址。

附加网络数是指此时 L2TP 可以自动添加多少网络。这些网络可附加到任何现有的 L2 网络上。

为每个 L2 网络添加未编号 IP 地址后，该网络的 IP 路由表中将自动添加未编号的 IP 项。未编号 IP 地址为操作首选模式。如果需要向 L2 网络添加编号地

址，则可以在 IP 协议配置环境中进行更改(参阅 *Protocol Configuration and Monitoring Reference Volume 1* 中『配置 IP』 一章)。

Disable

使用 **disable** 命令可禁用 L2TP 功能或禁用 L2TP 本身。

语法: disable

- call-rcv-window
- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2tp
- outbound-call-from-lac
- proxy-auth
- proxy-lcp
- tunnel-authentication

call-rcv-window

为便于执行定序和拥塞控制，L2TP 对每个呼叫的信息包进行排队。每个呼叫都有自己的队列或窗口，这些队列或窗口的容量必须传输给对等实体，这样，流控制算法才可正常工作。禁用 *call-rcv-window* 将关闭每个会话的所有流控制程序。只有当 LAC 和 LNS 间的连接质量很高，带宽充足，并且不需要进行大量的信息包重排序时，才可执行上述操作。

fixed-udp-source-port

清除 L2TP UDP 端口设置。禁用此参数将迫使您按 IP 地址在 LAC 和 LNS 间配置 IP 安全过滤器。

force-chap-challenge

禁用 LNS CHAP 再次验证客户机。如果 PPP 客户机处理 CHAP 再次验证比较困难，则可能需要禁用 CHAP 再次验证。

hiding-for-pap-attributes

禁用 LAC 和 LNS 间的代理 PAP 信息加密。

L2tp

注: 此命令输入时可以全部使用小写。第一个字符使用大写只是为了清晰起见。

禁用此路由器上的 L2TP。

outbound-calls-from-lac

阻止 LAC 发出呼叫启动 L2TP 隧道。

proxy-auth

禁用从 LAC 向 LNS 发送 PPP 代理认证信息。

proxy-lcp

禁用从 LAC 向 LNS 发送 LCP 信息。

tunnel-authentication

禁用所有隧道的基于共享秘密的同级认证。

Enable

使用 **enable** 命令可启用 L2TP 功能或 L2TP 本身。

语法:

enable

- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2tp
- outbound-call-from-lac
- proxy-auth
- proxy-lcp
- tunnel-authentication

fixed-udp-source-port

在 1701 处设定 L2TP UDP 端口。启用此参数允许您按 UDP 端口为 L2TP 配置 IP 安全过滤器。这样，您便可以轻易地加密或认证 L2TP 通信了。

force-chap-challenge

即使 LNS 接收到代理 CHAP，仍然启用 LNS CHAP 再次验证客户机。从安全角度考虑，如果已知客户机可以顺利处理再次验证，则建议使用此参数。

hiding-for-pap-attributes

启用 LAC 和 LNS 间的代理 PAP 信息加密。

outbound-calls-from-lac

允许 LAC 发出呼叫启动 L2TP 隧道。软件将提示您输入会话参数。

实例:

```
L2TP 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN, V34)? [ISDN]
        Outbound calling address: 1234
        Outbound calling subaddress:
L2TP 10>
```

L2tp

注: 此命令输入时可以全部使用小写。第一个字符使用大写只是为了清晰起见。

启用此路由器上的 L2TP。

proxy-auth

启用从 LAC 向 LNS 发送 PPP 代理认证信息。

proxy-lcp

启用从 LAC 向 LNS 发送 LCP 信息。

tunnel authentication

启用所有隧道的基于共享秘密的同级认证。

Encapsulator

使用 **encapsulator** 命令可为 L2 网络配置 PPP 参数。

语法: encapsulator

List

使用 **list** 命令可显示各种 L2TP 配置参数的状态。

语法: list

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
------- --------------
  L2TP                                = Enabled
  Maximum number of tunnels           = 20
  Maximum number of calls (total)     = 50
  Buffers Requested                   = 300

CONTROL CHANNEL SETTINGS
------- ------- --------
  Tunnel Auth                         = Enabled
  Tunnel Rcv Window                   = 4
  Retransmit Retries                  = 6
DATA CHANNEL SETTINGS
---- ------- --------
  Force CHAP Challenge (extra security)= Disabled
  Hiding for PAP Attributes           = Disabled
  Call Rcv Window                     = 6

MISCELLANEOUS
-------------
  SEND PROXY-LCP FROM LAC             = Enabled
  SEND PROXY-AUTH FROM LAC            = Enabled
```

Set

使用 set 命令可配置 L2TP 可操作参数。

语法: set any-remote-hostname

buffers

call-rcv-window

connection-direction

idle

max-calls

max-tunnels

remote-hostname

transmit-retries

tunnel-rcv-window

any-remote-hostname

清除出网远程主机名，并在此网上禁用入网远程主机名匹配。

buffers

指定要求的内部 L2TP 缓冲区数目。如果内存不足以满足请求，则重新启动时将只有部分缓冲区可用。如要在 L2TP 活动时肯定内存量，请使用 **memory** 命令(见 第207页的『Memory』)。

有效值: 1-1000

缺省值: 200

call-rcv-window

指定可以作为接收窗口使用的信息包数并启用呼叫接收窗口。如果此数据信道上已经启用流控制，则必须指定接收窗口大小。这一信息既供该路由器上的协议使用，也将用于使用启动报文与对等实体通信。配置值将用于所有由此路由器启动的呼叫。

有效值: 0-100

缺省值: 6

connection-direction [inbound] or [outbound] or [both]

指定在此网上连接能由对等实体启动 (inbound)、还是能有 LAC 启动 (outbound)，或者既能有对等实体也能有 LAC 启动。如果指定，则不能将空闲时间配置为 0。

缺省值: inbound

idle-time *seconds*

指定非活动状态秒数，此秒数过后，L2TP 将断开此网上的隧道。0 值表示隧道已经固定，不能断开。

有效值: 0-1024

缺省值: 0

max-calls

指定所有隧道上的最大呼叫数。在给定的时间内，这些通道应可作为 LAC 或 LNS 处于活动状态。

有效值: 1-500

缺省值: 100

max-tunnels

指定最大隧道数。在给定的时间内，这些隧道应可作为 LAC 或 LNS 处于活动状态。

有效值: 1-100

缺省值: 30

remote-hostname *hostname*

指定隧道上使用的远程主机名。

对于出网隧道，主机名在发出呼叫时发送到对等实体。对等实体使用此主机名确定是否完成该呼叫。主机名必须在认证子系统中进行配置，这样呼叫才能成功完成。详情请参阅第135页的『第12章 使用本地或远程认证』。

对于入网隧道，主机名将用于验证从此隧道接收的，来自对等实体的呼叫是否应完成。

有效值: 由 1 到 64 位 ASCII 字符组成的任何名称

缺省值: 无

transmit-retries

指定在宣布会话或隧道为非活动而将其关闭前，信息包可在控制隧道上重传输的次数。

有效值: 2-100

缺省值: 6

tunnel-rcv-window

指定可靠控制连接传输的接收窗口大小。这一传输过程传送并接收在隧道或会话的建立、拆除和保持时所需的报文。

有效值: 1-100

缺省值: 4

存取 L2TP 监视提示

如要存取 L2TP 监视提示:

1. 在 OPCON (*) 提示符下输入 **talk 5**。
2. 在 GWCON (+) 提示符下输入 **feature layer-2-tunneling**。

L2TP 监视命令

本节总结并介绍 L2TP 监视命令。在 `Layer-2-Tunneling Console>` 提示符下输入命令。

表36 总结了 L2TP 监视命令。

表 36. L2TP 监视命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Call	显示建立过程中的各个呼叫的相关统计数据和信息。
Kill	立即终止呼叫或隧道。
Memory	显示当前 L2TP 缓冲区的分配和使用情况。
Start	启动与另一对等实体的隧道连接。
Stop	停止呼叫或隧道连接并允许各个对等实体执行所需的管理操作。
Tunnel	显示各个现有隧道的相关统计数据和信息。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Call

使用 **call** 命令可显示呼叫统计数据和信息。

语法: call errors

physical-errors

queue

state

statistics

errors 显示呼叫时发生的一般传输错误。

实例:

```
Layer-2-Tunneling Console>
call errors
CallID | Serial # | ACK-timeout | Dropped pkts
 56744 |        1 |           0 |
0
```

CallID 与本呼叫关联的本地标识符。

Serial #
用于注册本呼叫的编号。

ACK-timeout
从对等实体接收到超时通告的次数。

Dropped pkts
呼叫中已经宣布为丢失的信息包数。这些信息包应该已经收到，但却由对等实体确认为已经丢失。

physical-errors
显示呼叫时发生的数据错误。

实例:

```
Layer-2-Tunneling Console> call physical-errors
CallID | Serial# | CRC    |framing|  HW    | buffer|timeout| align-| time since
       |         | Errors| Errors|overrun|overrun| Errors| ment  | updated
 56744 |       1 |     0 |     0 |     0 |     0 |     0 |     0
|
```

CallID 与本呼叫关联的本地标识符。

Serial #
用于注册本呼叫的编号。

CRC Errors
与 CRC 不匹配的信息包数。

framing errors
带有组帧错误的信息包数。

HW overrun
硬件超限发生的次数。

buffer overrun
缓冲区超限发生的次数。

timeout errors
接口超时的次数。

alignment
定位错误发生的次数。

time since updated
上次错误轮询后经过的时间。

queue 为每个呼叫显示队列的相关信息。

实例:

```
Layer-2-Tunneling Console> call queue
CallID | Serial # |Tx Win|Rx Win|   Ns   |   Nr   |Rx Q|Tx Q|priority| out Q
 56744 |        1 |    4 |    4 |    100 |   200  |  0 |  0 |      0 |     0
```

CallID 与本呼叫关联的本地标识符。

Serial #
用于注册本呼叫的编号。

Tx Win
对等实体的最大数据接收窗口。

Rx Win
本地最大传输窗口。

Ns 本呼叫的下一个待发送信息包序列号。

Nr 本呼叫的下一个待接收信息包序列号。

Rx Q 接收队列上的当前信息包数。

Tx Q 传输队列上的当前信息包数。

priority
等待由 L2TP 传输的 PPP 信息包数。

out Q 等待由 L2TP 传输的普通 PPP 信息包数。

state 显示各个呼叫的当前状态。

实例:

```
Layer-2-Tunneling Console> call state
CallID │ Serial # │ Net # │    State    │ Time Since Chg │ PeerID │ TunnelID
 56744 │        1 │     2 │ Established │   00:00:00     │  345   │ 45678
```

CallID 与本呼叫关联的本地标识符。

Serial #
用于注册本呼叫的编号。

Net # 与本呼叫关联的设备号。对于 LNS 呼叫，它是 L2 网络。对于 LAC 呼叫，它是接收初始呼叫的 PPP 设备。

State 当前呼叫状态。有效的呼叫状态为:

Established
已经准备好进行隧道连接的网络通信。

Idle 呼叫空闲。

Wait Cs Answer
等待打开通信链路。

Wait Reply
等待对等实体的答复。

Wait Tunnel
等待建立隧道。

Time since chg
上次状态更改后经过的时间。

PeerID
对等实体的呼叫 ID。

TunnelID
与呼叫关联的本地隧道。

statistics
显示每个呼叫数据传输的相关统计信息。

实例:

```
Layer-2-Tunneling Console>
call statistics
CallID │ Serial # │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │ ATO
 56744 │        1 │      34 │     1056 │      45 │     1567 │   10  │
34
```

CallID 与呼叫关联的本地标识符。

Serial #
用于注册呼叫的编号。

Tx Pkts
本呼叫已传输的信息包数。

Tx Bytes
本呼叫已传输的字节数。

Rx Pkts
本呼叫已接收的信息包数。

Rx Bytes
本呼叫已接收的字节数。

RTT 当前计算出的本呼叫的往返通信时间值。

ATO 当前计算出的呼叫自适应超时值。

Kill

使用 **kill** 命令可立即终止隧道连接。此命令释放隧道的所有本地资源，并进而强制断开连接。隧道断开时，对等实体不会收到任何通告。

注: 仅当 **stop** 命令无法终止隧道连接时才可使用这一命令。

语法: kill tunnel *tunnelid*

tunnel *tunnelid*
指定要终止的隧道。

Memory

使用 **memory** 命令可显示 L2TP 的当前内存使用率。

语法: memory

实例:

```
Layer-2-Tunneling Console> mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free
= 1000
```

此实例中配置了 2000 个缓冲区，但只能分配 1200 个。现在，200 个缓冲区正在使用，尚余 1000 个缓冲区可用。

Start

使用 **start** 命令可启动与另一个对等实体的隧道连接。

语法; start (没有任何参数提示输入主机名)

tunnel *hostname*

hostname
L2TP 用以建立隧道的主机名。

Stop

使用 **stop** 命令可停止隧道连接。隧道连接终止前将结束所有请求的清除操作。

语法: stop tunnel *tunnelid*

tunnel *tunnelid*
指定要终止的隧道。

Tunnel

使用 **tunnel** 命令可显示所有隧道的相关统计数据和信息。

语法: tunnel call
errors
peer
queue
state
statistics
transport

calls 显示所有隧道和为每个隧道中各个呼叫的呼叫状态。

errors 显示隧道上发生的错误。

实例:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID │ Type │ACK-timeouts
 96785    │ L2TP │    0
```

Tunnel ID
与隧道关联的本地标识符。

Retransmissions
在隧道上再传输的信息包个数。

peer 显示各个隧道和与这些隧道关联的对等实体。

实例:

```
Layer-2-Tunneling Console>
tunnel peer
Tunnel ID │ Type │ Peer ID │ Peer Hostname
 96785    │ L2TP │   89777 │
mypeer
```

Tunnel ID
与隧道关联的本地标识符。

Peer ID
指定给隧道的对等实体隧道标识符。

Peer Hostname
本地数据库中显示的对等实体主机名。

queue 显示每个隧道的队列相关信息。

实例:

```
Layer-2-Tunneling Console> tunnel queue
Tunnel ID | Type | Rx Win | Tx Win |   Ns   |   Nr   | Rx Q |  Tx Q
 96785    | L2TP |      4 |      4 |      5 |      6 |    0 |
0
```

Tunnel ID
与隧道关联的本地标识符。

Rx Win
组成接收窗口的本地最大信息包数。

Tx Win
组成接收窗口的对等实体的最大信息包数。

Ns 下一个待发送信息包的序列号。

Nr 下一个待接收信息包的序列号。

Rx Q 接收队列上的当前信息包数。

Tx Q 传输队列上的当前信息包数。

state 显示所有隧道的当前状态。

实例:

```
Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID |    State    | Time Since Chg | # Calls | Flags
 96785    | L2TP |  89777  | Established |    00:00:00   |       1 |
0
```

Tunnel ID
与隧道关联的本地标识符。

Peer ID
指定给隧道的对等实体隧道标识符。

State 隧道的当前状态。有效隧道状态为:

Established
隧道已经建立。

Idle 隧道空闲。

Wait Ctrl Reply
主机正在等待对等实体的答复。

Wait Ctrl Conn
主机正在等待连接指示。

Time since chg
上次状态更改后经过的时间。

 # Calls
隧道上活动的呼叫数。

Flags 用以在隧道上控制连接消息的标识。

statistics
显示与隧道关联的统计数据。

实例:

```
Layer-2-Tunneling Console> tunnel statistics
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes |  RTT  | ATO
 96785    | L2TP |      4  |      78  |      5  |     89   |   10  |
31
```

Tunnel ID
与隧道关联的本地标识符。

Tx Pkts
已传输的信息包数。

Tx Bytes
已传输的字节数。

Rx Pkts
已接收的信息包数。

Rx Bytes
已接收的字节数。

RTT 当前计算出的隧道控制连接消息往返通信时间值。

ATO 当前计算出的隧道控制连接消息自适应超时值。

transport

显示与隧道相关的 UDP 信息。

实例:

```
Layer-2-Tunneling Console> tunnel transport
Tunnel ID │ Type │ Peer IP Address │ UDP Src │ UDP Dest
 96785    │ L2TP │  11.0.0.102    │  1056   │
1089
```

Tunnel ID
与隧道关联的本地标识符。

Peer IP address
隧道的对等实体的 IP 地址。

UDP Src
隧道的 UDP 源端口。

UDP Dest
隧道的 UDP 目的地端口。

第19章 网络地址转换的使用

网络地址转换 (NAT) 和其扩展部分，网络地址以及端口转换 (NAPT) 可扩展企业可用的 IP 地址数，并防止公共网中的用户进入专用网的地址。对公共 IP 地址执行 NAT，成为专用 IP 地址。

公共 IP 地址是 IP 公共网络中有效的主机地址，它们在公共网络中必须是唯一的。如果公共网络为 Internet，公共 IP 地址必须是网络信息中心 (NIC) 提供的唯一 Internet 地址。

路由器已知专用地址，但公共网络并不知道。每个专用网络中的地址都必须是唯一的；但是，两个不同专用网络中可以有相同的地址。专用地址分配给根网络中的主机。根网络是仅通过一个路由器访问公共网络的网络。

NAT 可以多种方式扩展可用 IP 地址数:

- 通过轮流使用几个公共地址，允许一个公共地址表示多个专用地址。
- 只要是在不同的专用网络中使用，便可以允许地址复制。
- 允许网络管理员使用专用网络中的所有 IP 地址，而不限于 NIC 提供的地址。

使用专用地址可使外界无法使用这些地址。该 NAT 功能部件就是作为防火墙保护专用地址的保密性。

重要信息: 如定义 NAT 的 Internet 草本的 5.4 节所述，“具有(并使用)应用程序中的 IP 地址(在 NAPT 的情况下为 TCP/UDP 端口)的所有应用程序将不能通过 NAT...”。应注意， DLSw 和 XTP 根据端点 IP 地址(尤其是哪方具有更高级别的地址)做出决策。由于经过 NAT 的应用程序(例如 DLSw 或 XTP) 认为其地址为专用地址，而另一个路由器中的伙伴应用程序认为该应用程序地址是公共地址，所以会做出不正确的判断。

请参阅 第212页的图18 以获取根网络的工作站图。在该实例中，根网络由其 IP 地址为 10.33.96.0 的 IP 子网(其子网掩码为 255.255.255.0) 组成。

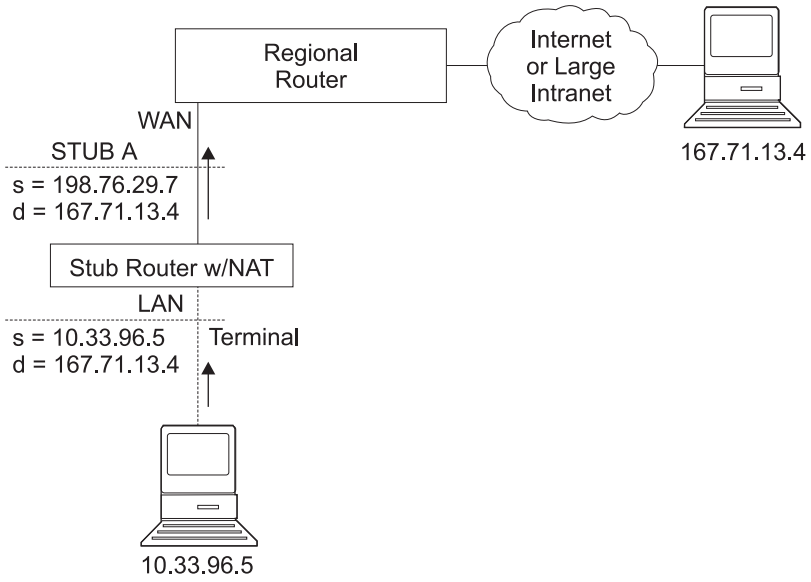


图 18. 网络运行 NAT

要使用 NAT，网络管理员为2212中的公共地址池分配一个或多个公共 IP 地址，并为根网络中的每个工作站分配一个专用 IP 地址。然后将公共 IP 地址放入*保留池*，并将专用 IP 地址放入*转换域*。

NAT 功能先将专用网络中的工作站专用地址绑定到一个公共地址。绑定表示在包出网时，其专用地址将转换为公共 IP 地址。入网包将该公共 IP 地址作为其目的地。NAT 识别公共地址，并将其转换为专用 IP 地址，然后将分组转发。通信停止后，将一直维护地址的连接，直到设置的计时器超时。在超时的情况下，NAT 将终止绑定，该公共地址可做它用。

在该实例中，将包从发送专用源地址 10.33.96.5 转换到 Internet 的目的地地址 167.71.13.4。2212中的 NAT 将专用地址 10.33.96.5 转换为公共地址 198.76.29.7。该转换将专用地址 10.33.96.5 从公共网络隐藏起来，这样就不会再有入网包直接寻址到专用地址 10.33.96.5。实际上，来自 167.71.13.4 的包寻址到公共地址 198.76.29.7。当 NAT 路由器接收到寻址 198.76.29.7 的包时，NAT 将目的地公共地址转换为专用地址 10.33.96.5，然后转发该包。

网络地址端口转换

NAPT 仅可用于 TCP 和 UDP 通信。在 NAPT 中，多个专用地址可同时使用一个公共地址。当 NAT 将一个公共地址转换为一个专用地址时，NAPT 将 NAPT 公共地址*和*公共端口号转换为专用地址和专用端口号。仅可为每个公共地址池配置一个 NAPT 地址。

要配置 NAPT，只需配置用于 NAPT 通信的公共地址。NAPT 的优点在于，它可以启用公共 IP 地址池中的一个地址，以同时支持多个专用 IP 地址。

静态地址转换

有时可能希望在能够直接从公共网络寻址的专用网络中，配置工作站或服务器。此时，应将工作站的专用地址静态转换为特定的公共地址。将所有出网报文的专用地址转换为指定的公共地址，然后所有位于指定公共地址的入网包就自动转发给绑定的专用地址。有两类静态地址映射：NAT 和 NAPT。

NAT 静态地址映射

在 NAT 映射中，所有的 IP 协议都可以访问主机。以下是配置 NAT 映射的实例:

专用地址	10.1.1.2
专用端口	0
公共 NAT 地址	9.67.1.1
公共端口	0

NAPT 静态地址映射

用户要指定 TCP 或 UDP 应用程序，可选择指定具有用户熟知的专用端口的 NAPT 映射。必须为 NAPT 静态地址映射配置 NAPT 公共地址。例如，在专用地址 10.1.1.1 配置 Telnet 主机，以使用 NAPT 公共地址 9.67.1.2，则应配置静态映射如下:

专用地址	10.1.1.1
专用端口	23
公共 NAPT 地址	9.67.1.2
公共端口	23

专用和公共端口映射到 Telnet 熟知的端口 23。此时，如果管理员同时将其专用地址为 10.1.1.1 的 FTP 服务器(熟知的地址为 21) 映射为 NAPT 公共地址 9.67.1.2，则映射如下:

专用地址	10.1.1.1
专用端口	21
公共 NAPT 地址	9.67.1.2
公共端口	21

对于这两个应用程序，位于地址 10.1.1.1 的服务器具有相同的 NAPT 公共地址 9.67.1.2，但 NAPT 可以使用不同的端口号 (23 和 21) 区分这两者。但是 NAPT 不能区分使用相同 NAPT 公共地址、同时具有相同应用程序和端口号的两个服务器。例如，如果 10.1.1.3 端口 21 的 NAPT 公共地址和熟知的端口与 10.1.1.1 端口 21 中的相同，则 NAPT 不能识别将进入的 FTP 通信是发送到服务器 10.1.1.3 还是 10.1.1.1。要配置多个具有相同 NAPT 地址和应用程序的服务器，必须使用服务器上非熟知的端口(例如，在端口 200 上启动 FTP 守护程序)。

设置 NAT 的包过滤器和访问控制规则

除了标识 NAT 或 NAPT 转换的专用地址域，管理员还必须设置包过滤器和2212中 IP 的访问控制规则。NAT 配置要求在连接到公共网络的接口上配置一个入网包和一个出网包过滤器。需要在入网包过滤器上配置一个或多个访问控制规则，同时也要在出网包过滤器上配置一个或多个访问控制规则。入网过滤器访问控制规则将带有正确定义的公共地址的入网包传送给 NAT。出网过滤器访问控制规则将带有正确定义的专用地址的出网包传送给 NAT。

适用于 NAT 的访问控制规则的访问控制规则类型为 ***I*** 和 ***N***，表示包含和 NAT。请参阅 *Protocol Configuration and Monitoring Reference, Vol. 1* 以获取有关配置 IP 访问控制的信息。

注: NAT 也可与 IPsec 隧道一起配置。此配置的实例在第169页的『配置路由器 A 的信息包过滤器访问控制规则』中可以找到。

实例: 配置具有 IP 过滤器和访问控制规则的 NAT

该实例显示了如何在图19中的网络图中配置根路由器的 NAT。请参阅第217页的『第20章 配置和监控网络地址转换』以获取有关命令的说明。

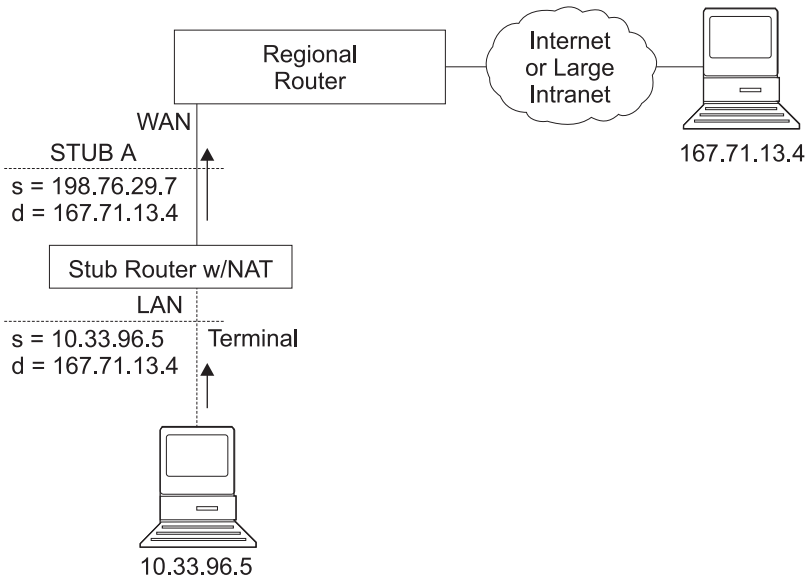


图 19. 网络运行 NAT

步骤如下:

1. 建立公共地址池以供 NAT 和 NAPT 使用。建立时可使用 **reserve** 命令。

```
NAT config>
reserve 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
NAT config> reserve 198.76.29.15 255.255.255.0 3 pool1 0.0.0.0
```

在该实例中，建立了一个名为 *pool1* 的池。池中的 NAPT 地址为 198.76.29.7。地址 198.76.29.13 和 198.76.29.14 是不可用的，所以设置的池不包括这两个地址。输入的参数包括: *public-address*、*mask*、*number-in-group*、*name* 和 *napt-address*。

NAPT 地址 0.0.0.0 表示在该组中没有 NAPT 地址。如果不配置池的 NAPT 地址，则可在所有组中使用 NAPT 地址 0.0.0.0。

2. 使用 **translate** 命令，可创建在 pool1 中由公共地址转换的专用地址域。输入的参数包括：*private-address*、*mask 和 name*。

```
NAT config> translate 10.33.96.0 255.255.255.0 pool1
```

3. 建立专用网络中的工作站的静态映射，这些工作站将永久映射到一个公共地址。以下命令标识接收公共网络中所有通信类型的机器 (10.33.96.5)。第二个机器 10.33.96.4 既是 Telnet 也是 HTTP 服务器。参数包括 *private-address*、*private-port-number*、*public-address 和 public-port-number*。注意：pool1 的 NAPT 地址作为主机的公共地址使用，该主机是用两个端口数配置的。

```
NAT config> map 10.33.96.5 0 198.76.29.8 0
NAT config> map 10.33.96.4 23 198.76.29.7 23
NAT config> map 10.33.96.4 80 198.76.29.7 80
```

4. 启用 NAT。

```
NAT config> enable NAT
```

5. 创建两个 IP 包过滤器，使 IP 可将包传送至 NAT。它们分别为与公共网络连接的接口 0 的入网和出网包过滤器。

```
IP Config> add packet-filter outbound out-0 0
IP Config> add packet-filter inbound in-0 0
```

6. 使用 **update** 命令，可进入 packet-filter '*filter-name*' Config> 提示。将 NAT 的访问控制规则添加到入网包过滤器。应将通过公共接口 (net 0) 接收的包传送到 NAT，这些包预定的地址在 NAT 保留公共地址池中。 NAT 将用正确的专用地址(如果包预定地址为 NAPT ，则还有专用端口)替换公共地址(如果包预定地址为 NAPT ，则还有公共端口)。Internet 信源的 0.0.0.0 地址和掩码表明，公共网络中的所有源地址都会传送到 NAT。

```
IP Config>update packet-filter
Packet-filter name [ ]? in-0
Packet-filter 'in-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 198.76.29.0
Destination mask [255.255.255.255]?255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

访问控制规则中的地址域大于 pool1 中定义的地址域。如果传送到 NAT 的包的地址在访问控制规则定义的范围内，但不是公共地址池中的一个，则 NAT 将包传送回 IP，而不做任何更改。

7. 如果希望路由器传送与访问控制规则不匹配的包，而不丢失任何包，则可以创建一个通配访问控制规则。下例显示了一个访问控制规则：

```
Packet-filter 'in-0' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 0.0.0.0
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 0.0.0.0
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

8. 将 NAT 的访问控制规则添加到入网包过滤器。从 net 0 接口转发的包将进行标识，该接口在专用网络上有源地址，因此 IP 能够将这些包传送到 NAT。NAT 将专用地址转换为 pool1 中的公共地址。

```
Packet-filter 'out-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]? 10.33.96.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'out-0' Config>
```

该包过滤器与过滤器 *in-0*相同，如果要转发与访问控制规则不匹配的包，就可增加通配包含访问控制规则作为最后的访问控制规则。

9. 可在 IP Config> 提示下使用 **list packet-filter** *filter-name* 命令，检查每个包过滤器中访问控制规则的准确性和顺序。
10. 启用 IP 的访问控制。

```
IP Config>
set access-control on
```

11. 使用 talk 5 重设 IP 和 NAT。此时，已在路由器配置中做了更改，但这些更改对路由器还没有影响。IP 和 NAT 的重设命令使用路由器读取新的配置，并按配置中定义的规则运行。

```
NAT>
reset NAT
IP> reset IP
```

第20章 配置和监控网络地址转换

本章描述网络地址转换 (NAT) 的配置和监控命令，包括以下各节:

- 『访问网络地址转换配置环境』
- 『网络地址转换配置命令』
- 第223页的『访问网络地址转换监控环境』
- 第223页的『网络地址转换监控命令』

访问网络地址转换配置环境

要访问 NAT 配置环境，可在 Config> 提示下输入以下命令:

```
   Config>
feature nat
   Network Address Protocol user configuration
   NAT config>
```

网络地址转换配置命令

本节说明了网络地址转换 (NAT) 配置命令。要配置 NAT，可在 NAT config> 提示处输入以下命令:

表 37. NAT 配置命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Change	更改公共 IP 地址保留池、专用地址转换域和静态映射。
Delete	删除公共 IP 地址保留池、专用地址转换域和静态映射。
Disable	禁用 NAT。
Enable	启用 NAT。
List	列出 NAT 配置的有关信息。
Map	建立连接某个工作站或服务器的静态 NAT 或 NAPT。
Reserve	创建公共 IP 地址池并将地址附加到该地址池。
Reset	使路由器读取 NAT 配置并根据所配置的 NAT 规则运行。
Set	设置超时。
Translate	标识由 NAT 公共地址池进行转换的专用 IP 地址。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Change

使用 **change** 命令，可更改公共 IP 地址保留池、专用 IP 地址转换域和静态映射。

语法:

change reserve

translate

mappings

reserve *pools*

提示用户，使用户可以更改任何公共 IP 地址保留池的特性(例如 IP 地址和掩码)。

有效值：标识已配置地址池的索引号。该编号在用户输入 **list reserve pools** 命令时显示。

缺省值：无

translate *ranges*

给出提示，使用户可以改变任何专用 IP 地址转换域的特性(例如 IP 地址和掩码)。

有效值：标识配置转换域的索引号。该编号会在用户输入 **list translate** 命令时显示。

缺省值：无

mappings

给出提示，使用户可以改变任何静态地址映射(例如 IP 地址和端口)的特性。

有效值：标识已配置映射的索引号。该编号在用户输入 **list mappings** 命令时显示。

缺省值：无

Delete

使用 **delete** 命令，可删除公共 IP 地址保留池、专用 IP 地址转换域和映射。

语法:

delete reserve
translate
mappings

reserve *pools*

给出提示，使用户可以删除任何公共 IP 地址保留池。

有效值：标识已配置地址池的索引号。该编号在用户输入 **list reserve pools** 命令时显示。

缺省值：无

translate *ranges*

给出提示，使用户可以删除任何专用 IP 地址转换域。

有效值：标识已配置转换域的索引号。该编号会在用户输入 **list translate** 命令时显示。

缺省值：无

mappings

给出提示，使用户可以删除任何静态地址映射。

有效值：标识已配置映射的索引号。该编号会在用户输入 **list mappings** 命令时显示。

缺省值：无

Disable

使用 **disable** 命令可禁用 NAT。可以禁用 NAT 使之丢弃需要转换的包，也可以禁用 NAT 以传送需要转换的包。

语法:

disable nat

drop

pass

drop 禁用 NAT 以丢弃需要转换的包。

pass 禁用 NAT 以传送需要转换的包。

Enable

使用 **enable** 命令可启用 NAT。启用 NAT 后就可以准备运行，但在运行之前必须输入 **reset** 命令或重新启动路由器。

语法:

enable nat

List

使用 **list** 命令，可列示公共 IP 地址保留池、专用 IP 地址转换域、映射、全局设置或所有的 NAT 信息。

语法:

list reserve

addresses

pools

translate

mappings

global

all

在以下实例中，时间以小时、分钟和秒钟的形式显示。条目寿命是此条目上一次使用后经过的时间。连接表示通信在这两个地址之间进行。超时确定了在上一次通信之后，连接断开之前经过的时间。请参阅 **set** 命令，以获取有关超时的详细信息。

实例:

```
NAT config>list all
NAT Globals:
NAT is ENABLED
Tcp Timeout....:   24:00:00
Non-Tcp Timeout:    0:01:00
NAT Reserved Address Pool(s):
Index First Address    Mask            Count NAPT Address     Pool Name
1     9.8.7.1          255.255.255.0   3     0.0.0.0         pool1
2     9.8.7.6          255.255.255.0   12    9.8.7.9         pool1
```

```
NAT Translate Range(s):
Index IP Address       IP Mask          Associated Pool Name
1     7.1.1.0          255.255.255.0    pool1
2     10.0.0.0         255.0.0.0        pool1
NAT Static Mapping(s):
Index Private Address:Port    Public Address.:Port
1     10.1.2.3        0       9.8.7.1        0
2     7.1.1.1         21      9.8.7.9        21
```

Map

使用 **map** 命令，可将专用网络中的主机或服务器与公共地址进行静态连接。该命令在启动 NAT 时会建立一个不会改变的关联，可用于设置专用网络中的服务器。

具有公共和专用端口号 0 的静态映射是 NAT 映射；具有其他端口号值的静态映射是 NAPT 映射。

语法:

map *private-address private-port-number public-address public-port-number*

private-address

工作站的专用地址。

有效值: 具有有效 IP 格式的 Internet 主机地址。该值应是在存根网络中为工作站分配的地址，公共网络(例如服务器)就固定地访问该地址。

缺省值: 无

private-port-number

在具有专用地址的设备上运行的应用程序的 TCP/UDP 端口号。输入 **0** 可创建 NAT 连接，输入其他值就创建 NAPT 连接。NAPT 的常用值是: Telnet 使用端口 23，FTP 使用端口 21， HTTP 使用端口 80。

有效值: 0 - 65535

缺省值: 0

public-address

专用地址向其映射的公共 IP 地址。对于 NAPT 映射，该地址必须是 NAPT 地址，对于 NAT 映射，该地址必须是 NAT 地址。

有效值: 公共网络中唯一的有效 IP 地址。公共网络可以是 Internet 或 intranet，这取决于网络的设计。

缺省值: 无

public-port-number

将在公共地址上转换的信息包的端口号。0 值表示所有的端口。常用值是: Telnet 使用端口 23，FTP 使用端口 21，HTTP 使用端口 80。

有效值: 0 - 65535

缺省值: 0

在以下实例中，专用 IP 地址为 10.11.12.200 的服务器接受所有来自 Internet 的通信；专用地址为 10.11.12.199 的服务器是 Telnet 服务器和 FTP 服务器。

实例:

```
map 10.11.12.200 0 9.8.7.2 0
map 10.11.12.199 23 9.8.7.9 23
map 10.11.12.199 21 9.8.7.9 21
```

Reserve

使用 **reserve** 命令，可在公共地址池中创建并增加一系列 IP 地址。

语法:

reserve *public-address mask number-in-group name napt-address*

public-address

组成地址池中某个域或组的地址序列中的第一个公共 IP 地址。例如，如果地址池中的一组包括 12 个地址，按顺序从 9.8.7.6 到 9.8.7.17，则该值为 9.8.7.6。

注: 要在公共地址池中增加其他地址域，则对每个组单独使用 **reserve** 命令，通过使用同样的地址池名，使一组与另一组相关联。例如，可在池 1 中将地址 9.8.7.6 到 9.8.7.17 配置为一组，在同一个池中可将 9.8.7.1 到 9.8.7.3 配置为另一组。于是，该池中未配置或未使用地址 9.8.7.4 和 9.8.7.5。

有效值: 公共网络中唯一有效的 IP 地址

缺省值: 无

mask 它是从 IP 地址中选择位的掩码。与 Internet 地址相似，掩码的长度为 32 位。掩码中的 1 选择的是地址的网络或子网部分。0 选择的是地址的主机部分。例如，地址 9.8.7.6 和掩码 255.255.0.0 包括了其前两位为 9.8 的所有地址(也就是从 9.8.0.0 到 9.8.255.255)。

有效值: 任何有效的 IP 掩码

缺省值: 无

number-in-group

指定组中有多少个以 *public-address* 开头的顺序地址。对于地址 9.8.7.6 到 9.8.7.17，该值为 12。

有效值: 1 - IP 掩码可定义的值

缺省值: 无

name 公共地址保留池的名称。该字符串必须与相应的 **translate** 命令中的池名称一致。

有效值: 可以是任意名称，可以使用多达 16 个的可打印字符，忽略开头和结尾的空白字符。

缺省值: 无

napt-address

网络地址端口转换 (NAPT) 使用的公共地址池中的一个 IP 地址。该地址用于 TCP 和 UDP 通信，以便根据协议端口号将多个专用地址映射到一个 NAPT 地址。NAPT 的使用是可选的。如果使用它，则每个公共地址池只能有一个 NAPT 地址。如果池或组中没有 NAPT 地址，则可输入值 **0.0.0.0**。 用户只需为地址池输入一次 NAPT 地址。

有效值: 一个公共 IP 地址。该地址不一定必须包括在公共地址池中所定义的值的范围之内，但必须在同一个子网中定义的值。

缺省值: 0.0.0.0 (表示无 NAPT)

实例:

```
reserve 9.8.7.1 255.255.255.0 3  pool1 0.0.0.0
reserve 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
```

Reset

使用 **reset** 命令，可重设 NAT。该命令会删除所有的连接，释放 NAT 使用的所有内存，并根据当前的 Talk 6 配置重新启动 NAT。重设 NAT 不会中断 2212 的其他任何组件。

语法:

reset nat

注意，如果 NAT 遇到无效的配置，则将会看到相应的消息。复查 NAT ELS 消息，查看 NAT 初始化失败的原因。

Set

使用 **set** 命令，可设置 TCP 和非 TCP 超时。

语法:

set tcp

nontcp

tcp *timeout*

在两个相连接工作站之间进行最后一次消息传送后，NAT 维持 TCP 连接的时间。连接就是保持一个专用地址和一个公共 IP 地址之间维护的关系。

有效值: 0 - 65535 分钟 (0 分钟到大约 45 天)

缺省值: 1440 分钟 (24 小时)

nontcp *timeout*

在两个相连接的工作站之间进行最后一次消息传送后，NAT 维持非 TCP 连接的时间。连接就是保持一个专用地址和一个公共 IP 地址之间维护的关系。

有效值: 0 - 65535 分钟 (0 分钟到大约 45 天)

缺省值: 1 分钟

Translate

使用 **translate** 命令，可将子网添加到 NAT 将转换的地址列表中。每个子网就是一个转换域。对于 NAT 必须知道的每个转换域都必须输入该命令一次。任意数目的转换域都可以使用一个公共地址保留池。

语法:

translate *private-address mask name*

private-address

任何应进行转换的 IP 主机地址或子网地址。

有效值: 合法的点分十进制 IP 地址格式的地址。当该地址与其子网掩码进行与操作时，该地址能辨识存根子网中的所有地址。存根子网是一个网络，它只通过路由器访问公共网络。

缺省值: 无

mask

有效值: 与要转换的存根网络关联的网络或子网掩码。

缺省值: 专用地址的类掩码。

name NAT 用于此专用地址域的公共地址池的名称。

有效值: 可以是任意名称，可以使用多达 16 个的可打印字符。它必须与 **reserve** 命令创建的公共地址池名称正确。

缺省值: 无

访问网络地址转换监控环境

要访问 NAT 监控环境，可输入

```
   *
t 5
```

然后在 **+** 提示下输入以下命令;

```
+ feature NAT
NAT>
```

出现 NAT> 提示。

网络地址转换监控命令

本节描述了 IP 安全监控命令。在 NAT> 提示下输入以下命令:

表 38. NAT 监控命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
List	列示有关 NAT 的信息。
Reset	使路由器读取 NAT 配置，并按照已配置的 NAT 访问规则运行。在输入 **reset NAT** 命令之前，NAT 不会影响路由器的运行。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

List

使用 **list** 命令，可显示 NAT 配置的有关信息。

语法:

list all

binding

fragment

global

reserve

pools

addresses

statistics

translate

在以下实例中，时间以小时、分钟和秒钟的形式显示。条目寿命是此条目上一次使用后经过的时间。连接意味着在两个地址之间建立会话。超时确定了在上一次通信之后，连接断开之前经过的时间。请参阅 Talk 6 中的 **set** 命令以获取有关超时的信息。

实例:

```
NAT>list all
NAT Globals:
Current State    Tcp Timeout    Non-Tcp Timeout    Memory Usage (in bytes)
ENABLED             24:00:00            0:01:00           408

NAT Statistics:
Requests :     Passes      Drops      Holds
       0 :          0          0          0

NAT Address Binding(s):
Private Address//Port  Public Address//Port  Bind Type  Entry Age
        7.1.1.1    21         9.1.1.1    21  STATIC       0:00:13
       10.1.2.3     0         9.1.1.2     0  STATIC       0:00:13

NAT TCP Session Information:
Private Address//Port  Public Address//Port  Tcp State  Data Delta  Entry Age
        7.1.1.1    21         9.1.1.1    21  ESTAB'ED      0        0:00:56

NAT Translate Range(s):
Base Ip Address        Range Mask      Associated Reserve Pool
       7.1.1.0         255.255.255.0   carol
      10.0.0.0         255.0.0.0       carol

NAT Reserve Pool(s):
Reserve Pool     Pool Size    NAPT Address   1st Available Address
carol                21            9.1.1.1          9.1.1.12
-------------------------------------------------------------
Number of Reserve Pools using NAPT.....:     1
Number of configured Reserved Addresses:    21

NAT Fragment Information:
Number of Entries    Number of Saved Fragments
          0                          0
```

Reset

使用 **reset** 命令，可重设 NAT。该命令会删除所有的连接，释放所有 NAT 使用的内存，并根据当前 Talk 6 配置重新启动 NAT。重设 NAT 不会中断2212的其他任何组件。

语法:

reset nat

第21章 使用 Dial-In Access to LANs(DIALs) 服务器

DIALs Server 允许远程用户拨号进入 LAN，存取 LAN 中的资源，进行访问的远程用户好象就是通过 LAN 适配器与本地连接的。类似地， DIALs Server 也允许 LAN 上的用户拨出，存取 WAN 资源，如告示牌、FAX 传真机、Internet 服务提供者 (ISP) 和其它的在线服务，从而减少了工作站对模拟电话线和调制解调器的需求。

可同时为拨入和拨出用户配置 DIALs Server 。 IBM DIALs 拨入客户机运行于远程工作站上，提供拨入功能。 图20显示将一设备用做支持拨入功能的 DIALs Server 的实例。

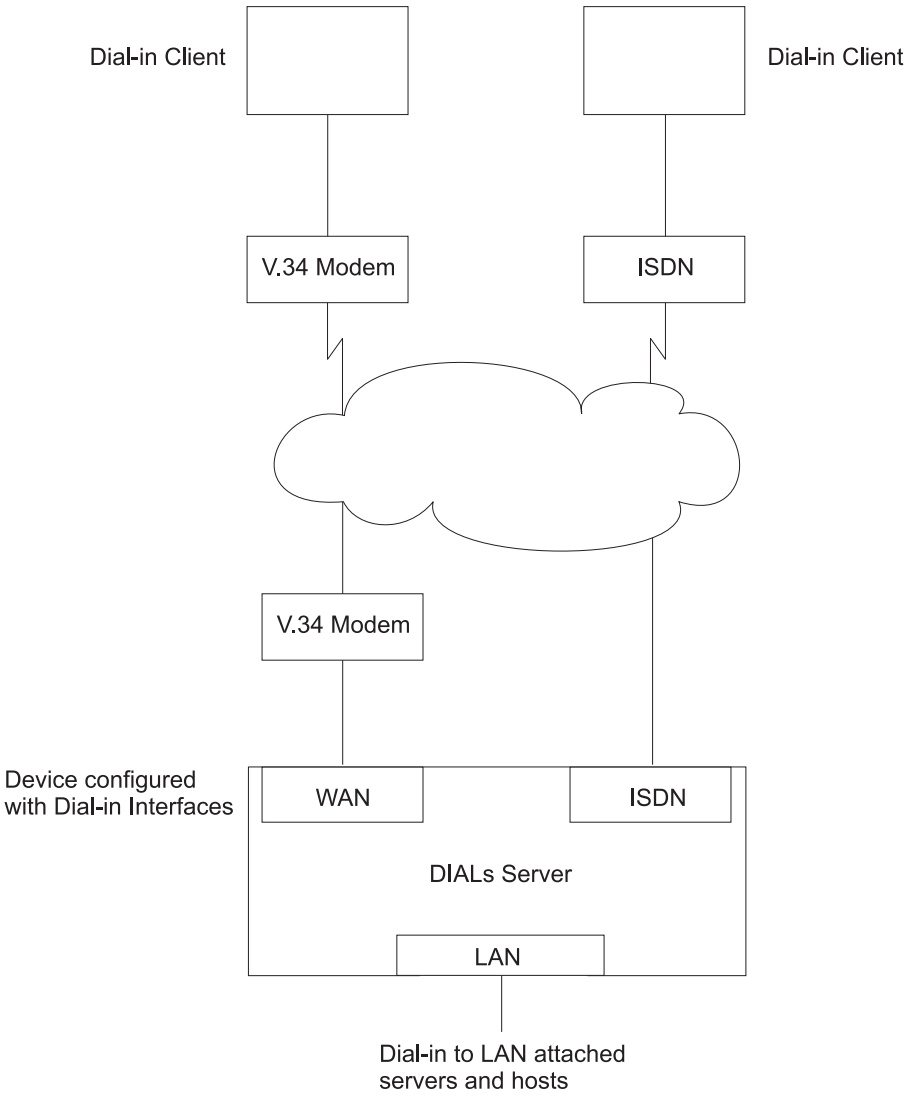


图 20. 支持拨入的 DIALs Server 实例

IBM DIALs 拨出客户机运行于联网工作站上，提供拨出功能。 第226页的图21显示的是将 2212 作为 DIALs Server ，以支持拨出功能的一个实例。

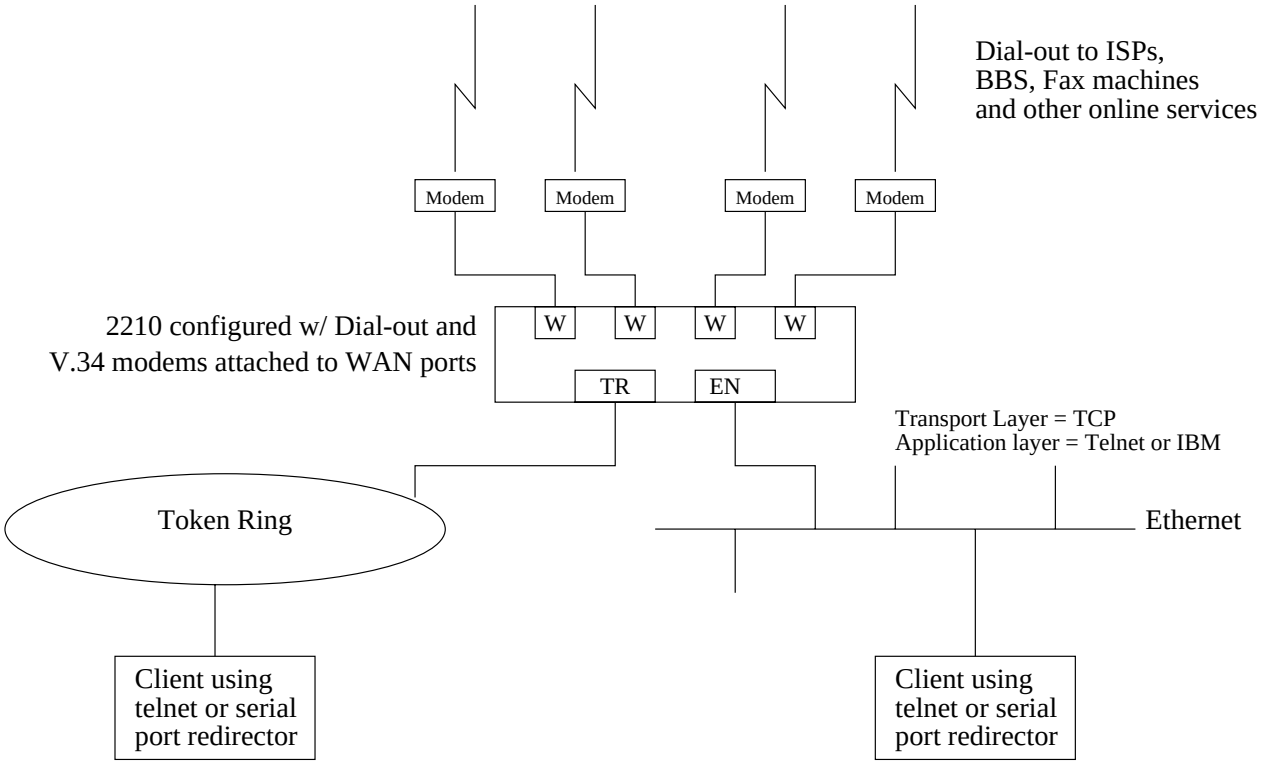


图 21. 支持拨入的 DIALs Server 实例

使用拨入存取之前

使用拨入存取之前，需要:

- 一个工作站，该工作站运行 IBM DIALs 拨入客户机或另一个 PPP 拨入客户机(以下统称为***拨入客户机***或***PPP 拨入客户机***)。
- 客户机上协议配置完整。
- ISDN 接口、或集成式调制解调器接口，或与 2212 (单用户拨入)的 WAN 端口连接的外部 V.34 调制解调器。
- LAN 中配置完备的 DIALs Server 。

配置拨入存取

本章说明如何在 DIALs Server 上配置两个拨入和拨出功能。有关配置客户机使用拨入存取，在工作站使用的有关客户机文档中有说明。

配置拨入接口

2212 上的拨入接口是一种特殊类型的拨号线路。对这种典型的拨号线路的设置，大多数是与单用户拨入应用程序无关的，因此，可新增一种称为***拨入***的设备类型，为这种拨号线路设置适当的缺省值。添加一种拨入设备的同时，设置了 PPP 封装器配置缺省值，在大部分的 PPP 拨入客户机上运行，包括 IBM DIALs 拨入客户机。有关这些缺省值，在第227页的『拨入接口的拨号线路参数缺省值』和第227页的『拨入线路的拨号线路 PPP 封装器参数』中有说明。

注: 只能在拨入线路上启用 DIALs 功能。当基本网是 V.34 网时，仅支持拨入线路。

拨入接口的拨号线路参数缺省值

注:

1. 不要改写本节中所说明的参数。如果改写，将使拨入功能无法正常运行。
2. 有些参数可能不显示，或不能配置。有关参数的详细说明，请参见*Access Integration Services 软件用户指南*中的『配置和监控拨号线路』.

以下缺省值在添加拨入接口时设置:

- 将***空闲时间***设为 0。请注意在该标准线路上，空闲计时器是无意义的。它不是自动拨出的固定线路。只有当 PPP 回呼已协商，或该线路上已启用多链路 PPP 时，才使用拨出。请参见*Access Integration Services 软件用户指南*中的 『Shiva 口令认证协议 (SPAP)』 和『使用多链路 PPP 协议』。
- 允许***入站呼叫***。因为 PPP 拨入客户机不使用 Nways 拨号线路实施的 LID 交换，所以需设置入站。
- 允许***出站呼叫***。

  注: 对于『出站』，在拨入电路上与在拨出线路上是不同的。请参阅第228页的『配置拨出接口之前』。

- 为 『default_address』 设置缺省目标地址。该地址添加到V.34 地址列表中。因为这些呼叫是入站呼叫，而且唯一的出站呼叫是回呼或多链路 PPP 交换的结果，因此目标地址无意义。但是，该地址对于线路参数来说是必需的。请勿删除该地址，否则将禁用您的线路。

拨入线路的拨号线路 PPP 封装器参数

注: 有关下列参数的完整说明，请参阅*Access Integration Services 软件用户指南*中的『使用点对点协议接口』。

以下缺省值在添加拨入接口时设置:

- 为 SPAP、CHAP 和 PAP 而启用的认证。
- 将 PPP MRU 设为 1522。这是IBM DIALs 拨入客户机的 Windows 3.1、OS/2 和 DOS 版本所需的 MRU 大小。不要改变该设置值，除非您已确定自己未使用这些客户机。
- 自动启用 PPP 封装器上的 DIALs 。这将打开一些功能部件，这些功能部件对于 Dial-In Access to LANs用户来说是很重要，如 NetBIOS 控制协议、NetBIOS 帧控制协议、剩余时间、SPAP 认证、回呼、LCP 识别、自动添加和删除到客户机的 IP 静态路。请参阅*Access Integration Services 软件用户指南*中的『使用点对点协议接口』，以获得有关 DIALs 功能的详细信息。

添加拨入接口

要添加拨入接口:

1. 在 2212 的一个可用 WAN 接口上，配置 V.34 基本网。请参阅*Access Integration Services 软件用户指南*中的『使用 V.34 网络接口』，以获得配置细节。
2. 输入 **talk 6**，进入 `Config >` 提示状态。

3. 在 Config > 提示状态下，输入 **add device dial-in** 命令，添加拨入接口。您将要被问到要添加多少拨入线路。执行该命令将创建新的网络，报出这些网的编号，并且对基本网编号做出提示，以及提示为多链路 PPP 而启用网络。

   实例: 假定当前最大网是 3，用户想在基网 2 中添加 1 个拨入网。

图22是定义拨入接口的一个实例。

图 22. 添加拨入接口

```
Config>add dev dial-in
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Base net for this circuit [0]? 2

Enable as a Multilink PPP link? [no]

Disabled as a Multilink PPP link.

Use "set data-link" command to change the data-link  protocol
Use "net " command to configure dial circuit parameters.
Config>li dev
Ifc 0     Ethernet               CSR  81600, CSR2  80C00, vector 94
Ifc 1     V.34 Base Net          CSR  81620, CSR2  80D00, vector 93
Ifc 2     V.34 Base Net          CSR  81640, CSR2  80E00, vector 92
Ifc 3     PPP Dial-in Circuit
Ifc 4     PPP Dial-in Circuit
```

配置拨出接口之前

在 2212 上配置和使用拨出接口之前，需要:

- 2212 上装有带 DIALs 支持的IBM 软件。
- 一个外部 V.34 调制解调器，或一个集成式调制解调器。请参阅*Access Integration Services 软件用户指南*中『使用 V.34 网络接口』，以获得配置信息。
- 连接到 LAN 上的工作站，该工作站可访问 2212 DIALs Server 。
- 客户机软件，如 telnet、telnet 重定向器或IBM DIALs 拨出客户机。必须在客户机上正确配置 IP，以使拨出客户机工作。

配置拨出接口

以下步骤是说明如何在您的设备上配置拨出接口。

1. 连接 V.34 调制解调器与 WAN 端口，该端口将用做拨出接口。
2. 连接 2212 DIALs Server 控制台。
3. 在 * 提示符下输入 **talk 6**。
4. 设置 V.34 接口。请参阅*Access Integration Services 软件用户指南*中的『使用 V.34 网络接口』，以获得详细说明。
5. 使用 **add device dial-out** 命令添加拨出接口。当提示输入接口时，请使用一个可用的 V.34 接口号。

   注:

   a. 可以在 V.34 基本网的顶层配置多个线路。然而，在任何给定时间内只有一条线路是活动的。

b. 该软件定义一个 V.34 地址，名为 ***default_address***。不要删除该地址，因为该地址在执行拨出时需要，如果删除，则拨出无法执行。

6. 如果正在使用IBM DIALs 拨出客户机，则配置 PPP 认证服务器，并且，按照*Access Integration Services 软件用户指南*中的 『PPP 认证协议』所说明的，添加 PPP 用户。添加的 PPP 用户应能够启用拨出。使用 telnet 的拨出不需要认证，因此，不要为 telnet 会话配置认证。
7. 使用 **feature dials** 命令配置全局拨出参数。请参阅*Access Integration Services 软件用户指南*中的 **feature** 命令。

   在该环境下，您可以配置拨出空闲计时器、拨出服务器名、调制解调器池及其它参数。
8. 为了使IBM DIALs 拨出客户机工作正常，必须定义一个 SNMP 共同体，它向所有能使用拨出服务器的拨出客户机授予读取和访问权。为使拨出选择器应用程序发现网络上的拨出服务器，这是必需的。请参见*Protocol Configuration and Monitoring Reference Volume 1*中的 『SNMP 管理』，以获得有关如何配置 SNMP 共同体的信息。
9. 重启该设备。

配置调制解调器池

调制解调器池是一组调制解调器，而在用户看来，调制解调器池只象是一个调制解调器。用户需要拨出时，使用池中第一个可用的调制解调器。用同一个端口名定义拨出接口组，可在 2212 DIALs Server 中创建调制解调器池。缺省地，将所有拨出接口命名为 『ALL_PORTS』，用来创建一个调制解调器存储池。分别命名这些拨出接口，使用户可选择一个特殊的调制解调器执行拨出。

要配置调制解调器池:

1. 在 * 提示符下输入 **talk 6**。
2. 输入 **net *n***，其中 ***n*** 是拨出接口号，这是在*Access Integration Services 软件用户指南*中的『使用 V.34 网络接口』里所定义的。通过该操作，用户进入接口配置环境。
3. 请在 Circuit Config> 提示符下输入 **encapsulator**，请参见 *Access Integration Services 软件用户指南*中的『配置和监控拨号线路』。通过该操作，用户进入拨出配置环境。
4. 在 Dial-out Config> 提示符下，输入 **set portname**。该操作提示您输入端口名(可达 30 个字符)。如果指定现有端口名，该调制解调器以这个名字加入池中。
5. 重启 2212。

配置全局 DIALs 参数之前

本章对全局 DIALs Server 参数做了说明。

服务器提供 IP 地址

配置路由器，使其向拨入客户机提供一个 IP 地址，以用于持续连接。路由器分配给客户机的地址可通过四种不同的方法检索到。它们是(按优先级排列):

1. 通过用户 ID

IP 地址可存储在每一客户机的 PPP 用户概要中。客户机连接并请求 IP 地址时，路由器对在用户的 PPP 用户概要中所配置的地址进行检索。这就允许每次用户都可获得同样 IP 地址，但这要求各用户的 IP 地址是唯一的。

使用 Config> **add ppp-user** 命令，在 PPP 用户概要中配置一个 IP 地址。

2. 通过接口

   IP 地址可存储在拨入接口配置中。客户机连接并请求 IP 地址时，路由器从进行连接的接口检索地址。该方法要求每一拨入接口拥有唯一的 IP 地址。

   为设置接口的 IP 地址:

   - 使用 Config> **list devices** 命令，显示分配给该硬件接口的接口号。
   - 使用 Config> **net 'x'** 命令，进入接口的命令提示状态，其中 'x' 是配置的接口号。
   - 使用 PPP Config> **set ipcp** 命令，设置接口 IP 地址。

3. 通过池

   IP 地址块可存储在 IP 地址池中。客户机连接并请求地址时，路由器从池中检索地址。客户机中断连接时，地址返回池中。该方法提供了一个位置，用来配置拨入客户机 IP 地址，而无需地址服务器。

   使用 DIALs config> **add ip-pool** 命令，添加一个 IP 地址池。

4. 通过 DHCP 代理

   可以向 DHCP 服务器租借 IP 地址。客户机连接并请求地址时，路由器以客户机的名义，向 DHCP 服务器请求一个地址。该方法要求 LAN 上配有 DHCP 服务器。一个 DHCP 服务器可以为多个路由器上的多个客户机提供地址。请参阅第231页的『动态主机配置协议 (DHCP)』以获得更多的信息。

   使用 DIALs config> **add dhcp-server** 命令，添加一个 DHCP 服务器。

IP 地址分配方法

拨入客户机在持续连接过程中所用的 IP 地址，可有五种不同出处。它们是(按优先级排列):

1. 所提供的客户机
2. 分配的用户 id
3. 指定的接口
4. 地址池
5. DHCP 服务器

拨入客户机连接时，路由器依次查找这些源，直到找到一个地址为止，或直至查找完所有的源。如果 IP 地址未找到，IPCP 协商失败。可将以上方法结合使用。

缺省配置是:

```
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

注: PPP 用户概要、接口或 IP 地址池中没有缺省配置的地址。

动态主机配置协议 (DHCP)

动态主机配置协议 (DHCP)是为网络上的主机提供配置参数的。不同于其它配置参数，DHCP 提供分配网络地址给主机的某种机制。

代理 DHCP 功能部件可*代表*一个拨入 PPP 用户的客户机。这就允许在进行拨入会话时，或在租约到期之前，设备可获得可一个租借的 IP 地址。由 DHCP 服务器分配的 IP 地址通过 PPP IPCP 传送到拨入客户机(请参阅*Access Integration Services 软件用户指南*中的『IP 控制协议』，以获得 IPCP 的详细说明)。该拨入客户机软件不知道已将 DHCP 用来分配 IP 地址，因此它不要求 DHCP 进行任何活动。

代理 DHCP 要求至少配置一个 DHCP 服务器，并且可从路由器存取。

代理 DHCP 要求分配给拨入用户的地址在与 LAN 直接连接的同一子网内。在该典型的配置中，需要启用代理 ARP 子网路由选择，以允许路由器答复对本地网上代表拨入客户机的主机的 ARP 请求。

基本 DHCP 设置

最基本的配置需要一个 DHCP 服务器，与路由器处于同一网络，且待租借的拨入地址是在与该 LAN 类似的子网范围内。

客户机拨入时，从 DHCP 服务器获得一个 IP 地址租契，用于与客户机的 IPCP 协商中。

1. 将 2212 和 DHCP 连至同一个 LAN。
2. 配置并启动 DHCP 服务器(关于如何设置服务器租借 IP 地址，请参阅 DHCP 服务器文档。记住，待租借的 IP 地址 “必须” 在直接连接的 LAN 的子网内，2212 上的代理 ARP 必须启用)。
3. 典型地，代理 DHCP 设置禁用指定的客户机、 用户 ID、接口和池 IP 地址协商选项:

   ```
   Dials Config>list ip
   DIALs client IP address specification:
   Client : disabled
   UserID : disabled
   Interface : disabled
   DHCP Proxy : enabled
   ```

4. 添加 DHCP 服务器 (`Dials Config>` **`add dhcp 10.0.0.111`**)
5. 为*指定服务器*设置拨入客户机软件。

   注:

   a. *指定服务器*配置随拨入客户机实现方式的不同而不同。

   b. 该客户机软件不应配置成从 DHCP 获取自身地址。而应通过在最初的配置请求中，向 IPCP 发送一个地址 0.0.0.0 来获取。
6. 对于该设置，使 DHCP GATEWAY ADDRESS 缺省为 0.0.0.0。

多驿站到 DHCP 服务器

配置的 DHCP 服务器的 IP 地址应当是从连接的路由器上可到达的地址。应始终能从远程存取框对服务器执行 ping 命令。

当 DHCP 服务器在多个驿站之外的位置，它需要知道一个用于答复的地址，并指明从哪一个池分配 IP 地址。这一点很重要，因为可利用 DHCP 服务器为若干子网提供地址，因此必须指明是从哪个地址池中选取。这里使用 DHCP 网关地址 (*giaddr*)，该术语是基于 RFC 2131 中的定义的。对于如令牌环网或以太网的 LAN 端口而言，该 *giaddr* 相对于 2212 必须是一本地地址，另外，因为该 *giaddr* 地址还是 DHCP 服务器用作答复的地址，请确保用户从 DHCP 服务器这里能够 ping 该地址。

多 DHCP 服务器网络

可以为冗余配置多个 DHCP 服务器。配置多个服务器时，代理 DHCP 客户机向所有服务器征询一个地址，接受返回的第一个响应。如果所有 DHCP 服务器都远在一个驿站之外，或这些服务器连接到一个与池中地址无关的子网，则必须配置 *giaddr*。请参阅第231页的『多驿站到 DHCP 服务器』。

然而，可能有多个 DHCP 服务器提供地址，不允许服务器上配置的地址池出现交叠，是很重要的。此外，因为只有一个 *giaddr* 用于 DHCP 服务器响应，并通过它进行查找，每一个地址池必须与其它地址池在同一个子网中。

动态域名服务器 (DDNS)

域名服务器 (DNS) 将 IP 地址映射到主机名，典型情况下，它是静态的。动态 DNS 是一种功能部件，当与 DDNS DHCP 服务器和 DNS 服务器同时使用时，可通过 IP 地址和主机名映像，使 DHCP 动态更新 DNS 服务器。该功能只可与代理 DHCP 同时使用。

当您启用 2212 上的动态 DNS，并在用户概要(请参阅*Access Integration Services 软件用户指南*中的『PPP 认证协议』)中配置主机名时，请使用选项 81 (DDNS) 作为主机名，并将其传送给 DHCP SERVER。如果为 DDNS 配置了正确的 DHCP 服务器，则 DHCP 服务器通过其租借给路由器的 IP 地址，和路由器发送给它的主机名来更新 DDNS 服务器。这将允许其它用户通过主机名访问拨入客户机，而客户机无需知道动态选择的 IP 地址。

第22章 配置 DIALs

本章说明 DIALs 配置及可操作命令。其中包括:

- 『进入 DIALs 全局配置环境』
- 『DIALs 全局配置命令』
- 第240页的『存取 DIALs 全局监控环境』
- 第241页的『DIALs 全局监控命令』
- 第244页的『监控拨入接口』
- 第244页的『监控拨出接口』

进入 DIALs 全局配置环境

按以下步骤进入全局配置进程。

1. 在 OPCON 提示符下，输入 **talk 6**。 (有关该命令的详细说明，请参阅 Access Integration Services 软件用户指南 中的 *OPCON 进程和命令*。)例:

```
* talk 6
Config>
```

   输入 **talk 6** 命令后，终端将显示 CONFIG 提示符 (Config>)。如果首次输入配置，提示符将不出现，这时请再按下 **Return**。

2. 在 CONFIG 提示符下，输入 **feature dials** 命令，出现 DIALs Config> 提示符后，进入 DIALs 全局参数配置环境。

DIALs 全局配置命令

表 39. DIALs 全局配置命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	添加一个 DHCP (动态主机配置协议)服务器到 DHCP 服务器列表，或添加一个 IP 地址池。
Delete	从列表中删除一个 DHCP 服务器，或从 IP 地址池中删除一个地址块
Disable	禁用 IP 地址分配方法、拨出协议、多底架 MP、SPAP 标志和动态 DNS。
Enable	启用各种 IP 地址分配方法、拨出协议、多底架 MP、SPAP 标志和动态 DNS。
List	列出全局 DIALs 参数和参数值。
Set	设置允许的时间、dhcp 网关地址、NetBIOS 名字服务器地址、本地分配的 MAC 地址、虚拟连接 (VC) 动态名字服务器地址、拨出空闲计时器和拨出服务器名。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add

使用 **add** 命令，添加一个新代理 DHCP 服务器到服务器列表，或添加一个 IP 地址池。

代理 DHCP 服务器列表中列有 DHCP 服务器的 IP 地址，这些服务器轮流将 IP 地址租借给拨入客户机。可以为冗余添加多个服务器。最多可添加 20 个。

IP 地址池功能部件提供一种方法，通过该方法，路由器可自本地定义的地址池到一个拨入客户机检索 IP 地址。客户机可能在连接路由器的过程中使用该地址。一个池包括一个或多个 IP 地址块。最多为 20 个。通过基本 IP 地址和块中的地址号来定义各地址块。块中地址从基地址开始，以升序递增排列。

语法:

add dhcp-server *ipaddress*

ip-pool *baseaddress #addresses*

dhcp-server *ipaddress*

以指定的 IP 地址添加一个 dhcp-server。

例:

```
DIALs Config> add dhcp-server
DIALs Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

ip-pool *baseaddress #addresses*

在 IP 池中添加一个地址块。

例:

```
DIALs Config> add ip-pool
Base address []? 192.1.100.18
Number of addresses [1]? 57
DIALs config>add ip-pool
Base address []? 192.2.200.1
Number of addresses [1]? 250
DIALs config>list ip-pools
     Configured IP address pools:
          Base Address      Last Address        Number
          ------------      ------------        ------
          192.1.100.18      192.1.100.74            57
           192.2.200.1     192.2.200.250           250
```

Delete

使用 **delete** 命令，从服务器列表中删除一个当前的代理 DHCP 服务器，或从 IP 地址池删除一个地址块。

语法:

delete dhcp-server *ip address*

ip-pool *baseaddress #addresses*

dhcp-server *ipaddress*

通过指定的 IP 地址删除 dhcp-server。

例:

```
DIALs Config> delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

ip-pool *baseaddress #addresses*

从 IP 池中删除一个地址块。

例:

```
DIALs Config> delete ip-pool
Base IP address of the block to be removed []? 192.2.200.1
```

Disable

使用 **disable** 命令，禁用 IP 地址分配方法、拨出协议、SPAP 标志和动态 DNS。

语法:

disable dynamic-dns

dial-out

ip-address-assignment *type*

spap-banner

dial-out *type*

禁止使用从 telnet 或IBM DIALs 拨出客户机的拨出。可指定:

dials 禁用全部IBM DIALs 拨出客户机

telnet 禁用全部 telnet 客户机。

要禁用上面两种客户机，必须针对每种类型输入 disable dial-out 命令。禁用两类客户机，将禁止 2212 上的拨出功能。

dynamic-dns

禁止发送做为用户主机名的 DHCP 选项 81。请参阅第232页的『动态域名服务器 (DDNS)』以获得更多的信息。

IP-address-assignment *type*

禁用各种 IPCP 地址分配技术。可指定:

- 客户机 - 禁止分配已分配的客户机 IP 地址。
- 用户 ID - 禁止使用 IP 地址的认证用户概要。
- 接口 - 禁止路由器使用接口的 IPCP 设置值。
- 池 - 禁止路由器使用 IP 地址池为客户机分配地址。
- DHCP-代理 - 禁止路由器从 DHCP 服务器租借地址。

请参阅第229页的『服务器提供 IP 地址』以获得有关分配技术的其它信息。

spap-banner

禁止将 SPAP 标志发送到一个通过 SPAP 认证的远程用户。

注: 输入\n，强行使客户机显示标志中新的一行字符。

Enable

使用 **enable** 命令，启用 IP 地址分配、拨出协议、SPAP 标志和动态 DNS。

语法:

enable dynamic-dns

ip-address-assignment . . .

spap-banner

dial-out ***type***

启用从 telnet 或IBM DIALs 拨出客户机的拨出。缺省地，两类客户机均启用。可指定:

dials 启用全部IBM DIALs 拨出客户机

telnet 启用全部 telnet 客户机。

dynamic-dns

取消发送作为用户主机名的 DHCP 选项 81。请参阅第232页的『动态域名服务器 (DDNS)』以获得更多的信息。

IP-address-assignment ***type***

启用各种 IPCP 地址分配技术。路由器按所列顺序试用各方法。可指定:

- 客户机 - 允许客户机指定要使用的地址。
- 用户 ID - 路由器将在认证的 PPP 用户概要中查找 IP 地址。如果地址非零，将把它提供给客户机。
- 接口 - 路由器将查找接口上配置的 IP 地址。如果地址非零，将把它提供给客户机。
- 池 - 路由器将从 IP 地址池中请求一个地址。如果地址可用，将把它提供给客户机。
- DHCP-代理 - 路由器试图从 DHCP 上租借地址。如果成功，客户机使用该地址。

请参阅第229页的『服务器提供 IP 地址』以获得有关分配技术的其它信息。

spap-banner

启用发送 SPAP 标志到一个通过 SPAP 认证的远程用户。使用 **set spap-banner** 命令(该命令在第238页的『Set』中有说明)，输入 SPAP 标志文本。请参阅 *Access Integration Services 软件用户指南* 中的『Shiva 口令认证协议 (SPAP)』，以获得更多的信息。

List

使用 **list** 命令显示当前配置。可以从点对点控制台上监控每个网络的 DHCP 状态和租借时间。请参阅 *Access Integration Services 软件用户指南* 中的 **listipcp** 命令 示例。

语法:

list all

dhcp-servers

dial out

dynamic-dns

ip-address-assignment

ip-pools

name-servers

spap-banner

time-allowed

vc-parameters

例:

```
DIALs config>li all
DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Configured IP address pools:
     Base Address      Last Address        Number
     ------------      ------------        ------
       11.0.0.100        11.0.0.129           30
       11.0.0.210        11.0.0.229           20

Configured DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10

Dynamic DNS: Enabled

Primary Domain Name Server     (DNS): 11.0.0.2
Secondary Domain Name Server   (DNS): None
Primary NetBIOS Name Server   (NBNS): 11.0.0.2
Secondary NetBIOS Name Server (NBNS): None

Time allowed for connections: Unlimited

SPAP banner  :Enabled
Welcome to the network...

Box-level dial-out settings
Inactive timer:                                      15
LAN Protocols enabled for dial-out:         TELNET DIALs
Server name:                                   DIALOUT_SERVER

Number of Mac Addresses defined = 0
Base MAC Address: 000000000000

VC: Maximum Virtual Connections = 50
VC: Maximum suspend time (hours) (0 is unlimited) = 12
VC: Idle timeout period (seconds) = 30

Multi-chassis MP: Endpoint discriminator (0 means use box s/n) = 0

DIALs config>
```

示例中显示了:

DIALs client IP address specification

显示 IP 地址分配技术及是否启用之。您会接收到这部分显示，其中包含外壳层拨出设置值，以响应 **list ip-address-assignment** 命令。

IP address pools

显示已配置的 IP 地址池。用户会接收到这部分显示，以响应 **list ip-pool** 命令。

Configured DHCP servers

显示当前配置为 DHCP 服务器的 IP 地址列表。这部分还列出用作 DHCP 网关的接口。用户会接收到这部分显示，以响应 **list dhcp-servers** 命令。

Dynamic Name Servers
显示是否启用动态 DNS。用户会接收到这部分显示，以响应 **list dynamic-dns** 命令。

primary domain server (dns)
该行和下列各行显示配置的主、辅名字服务器。用户会接收到这部分的显示，以响应 **list name-servers** 命令。

time allowed
显示拨号用户可使用的最长时间(以分钟为单位)。用户会接收到这部分显示，以响应 **list time-allowed** 命令。

spap banner
显示 spap 标志的内容。用户会接收到这部分显示，以响应 **list spap-banner** 命令。

vc connections
显示已配置的虚拟连接信息。

multi-chassis mp
显示已配置的终点鉴别器。

Set

使用 **set** 命令，设置允许的时间、dhcp 网关地址、NetBIOS 名字服务器地址、动态名字服务器地址、拨出空闲计时器和拨出服务器名。

语法:

set
- dhcp-gateway-address
- dial-out . . .
- dns . . .
- laa
- multi-chassis-mp
- nbns . . .
- spap-banner . . .
- time-allowed
- vc-parameters

dhcp-gateway-address *interface# ipaddress*
设置与 DHCP 网关相关的 IP 地址。DHCP 将这些地址用做:

1. DHCP 所要答复的地址
2. 指示地址池，DHCP 从中分配 IP 地址

如果 DHCP 服务器不在直接连接的 LAN 接口上，则必须将该地址配置成一个 LAN 接口地址，该接口具有到 DHCP 服务器的 IP 连通性。请参阅第231页的『动态主机配置协议 (DHCP)』和 RFC 1541 中的 『giaddr』 定义，以获得更多的信息。

dial-out *parameter*
为拨出网络设置非活动计时器或服务器名。***参数***可以是:

inactivity-timer

为拨出网络设置拨出非活动计时器。这是一个时间值，以分钟为单位，用户在该时间内连接，但无数据通信量流通。例如，如果非活动计时器设为 5 分钟，在任何 5 分钟间隔内，不接收数据或传输数据，则连接断开，调制解调器成为可用的。缺省为 0，表示禁用非活动计时器，无限期地保持连接。

servername

设置拨出服务器的名称。该名称字串可达 30 个字符。缺省为『2210_DIALS_SERVER』。该名称是 IBM DIALs 拨出客户机在使用『Chooser』 应用程序，以查找拨出服务器时所看到的名称。该参数对于 telnet 拨出客户机无意义。

dns ***type ipaddress***

配置主、辅域名字服务器 (DNS)。***类型***可以是:

primary

为拨入客户机设置要使用的主 DNS 服务器的 IP 地址。该值是在某些拨号客户机(特别是使用 Windows 95) 的 IPCP 过程中协商的。

secondary

为拨入客户机设置要使用的辅 DNS 服务器的 IP 地址。该值是在某些拨号客户机(特别是使用 Windows 95) 的 IPCP 过程中协商的。

laa *#MAC_addresses MAC_address_base*

为本地管理的地址 (LAA) 表设置 MAC 地址号和基网地址。只有 Layer-2-Tunneling 网络才使用 LAA 地址。

#MAC_addresses

从 *MAC_Address_Base* 开始，指定 Mac 地址号，并将它们添加到 LAA 表中。

有效值是: 0 到 256

缺省值为: 0

MAC_address_base

指定 LAA 表中的基 MAC 地址。

有效值是: 任何有效 MAC 地址

缺省值为: 000000000000

例:

```
DIALs
config>set laa
    Number of Mac Addresses:  [0]? 20
    Locally Administered Mac Address Base (hex) [000000000000]?
002210aaaaaa
    DIALs Config>
```

multi-chassis-mp

设置要使用的终点鉴别器。所有加入同一束的链接必须具有同样的终点鉴别器。

例:

```
DIALs Config> set multi-chassis-mp
   Enter Endpoint Discriminator to use from stacked group (0 for box S/N):
2345
```

nbns *type ipaddress*

配置主、辅 NetBIOS 名字服务器。*类型*可以是:

primary

设置主 NetBIOS 名字服务器的 IP 地址。

secondary

设置辅 NetBIOS 名字服务器的 IP 地址。

spap-banner

允许配置一条消息，该消息发送给所有成功完成 SPAP 认证的客户机。

例:

```
DIALs config>set spap-banner
SPAP banner  :Disabled

Enter Banner: Welcome to the network...
```

time-allowed

设置 PPP 拨入用户和拨出用户可使用的时间。该参数定义用户可使用的最长连接时间(以分钟为单位)。缺省值为 0，表示用户的连接时间不限。

vc-parameters

使用该参数设置全局缺省虚拟连接属性。系统提示您输入最大连接数、最大挂起时间和非活动超时值。

例:

```
Config> feature DIALs
DIALs Config> set vc-parameters
Maximum Virtual Connections [50]? 40
Maximum suspended time (hours) (0 is unlimited) [10]? 18
Inactivity Timeout (seconds) [30]? 60
DIALs Config>
```

Maximum Virtual Connections

活动的或挂起的最大虚拟连接数。使用带 MP 的 VC 时配置该值，使它比实际连接值大 1。

有效值是: 0 到 255

缺省值为: 50

Maximum suspended time

系统结束连接前，虚拟连接可挂起的最大时间值，以小时为单位。指定该参数为 0，即允许虚拟连接挂起的时间无限。

有效值为: 0 到 48

缺省值为: 12

Inactivity Timeout

在虚拟连接挂起前，处于非活动连接的秒数。

有效值为: 10 到 1024

缺省值为: 30

存取 DIALs 全局监控环境

按以下步骤使用 DIALs 监控命令。

1. 在 OPCON 提示符下，输入 **talk 5**。 (有关该命令的详细说明，请参阅 *Access Integration Services 软件用户指南* 中的 “OPCON 进程和命令”一章。)例:

```
* talk 5
+
```

输入 **talk 5** 命令后，终端将显示 GWCON 提示符 (+)。如果首次输入配置，提示符将不出现，这时请再次按 **Return**。

2. 在 + 提示符下，输入 **feature dials** 命令后，出现 DIALS Console> 提示符，于是进入全局监控环境。

例:

```
    +
feature dials
    DIALS Console>
```

DIALs 全局监控命令

表 40. DIALs 全局监控命令

命令	功能
Clear	清除特定的挂起虚拟连接。
List	显示各种虚拟连接状态，或所有的虚拟连接状态。
Reset	动态激活 DIALS 参数。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Clear

使用 **clear** 命令清除特定的挂起虚拟连接。

语法:

clear vc *connection_id*

vc *connection_id*

指定要结束的挂起虚拟连接。要获得 *connection_id*，请输入 **list all-vc** 或 **list suspended-vcs** 命令。

List

使用 **list** 命令，显示所有虚拟连接、活动虚拟连接、挂起虚拟连接或 vc-parameters 的值。

语法:

list

all

active-vcs

all-vcs

dhcp-servers

ip-address-assignment

ip-pool

suspended-vcs

active-vcs

显示所有活动虚拟连接的属性。请参阅 **all-vcs** 参数说明，以获得对属性的解释。

all-vcs

显示所有活动的和挂起的虚拟连接的属性。是将由 **list active-vcs** 和 **list suspended-vcs** 两命令所显示的一起显示。

例:

```
+ feature dials
DIALS console> list all
 DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*      11.0.0.100        11.0.0.129           30            30
       11.0.0.210        11.0.0.229           20            19

Current DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10


Active VCs:
Conn ID    Interface Idle-Timeout Connected Username
========== ========= ============ HHH:MM:SS ================
1656494850         8           30   0:26:15 don
7293521502         9           30   1:41:57 jane


Suspended VCs:
           Hrs.Max
Conn ID    Suspend Suspended Username
========== =======  HH:MM:SS ======================
9256166098      12   0: 4:13 joe
```

活动的和挂起的 VC 属性如下:

Conn ID

虚拟连接的连接 id。系统在建立连接时分配 id。

Username

AAA。RADIUS 或建立虚拟连接的本地列表用户。

对于活动 VC:

Interface

管理虚拟连接的网络接口。

注: 不要使用接口分配来分配 IP 地址给拨号客户机，以免因其它用户使用该接口 (VC 挂起)引发问题。

Idle Timeout

非活动时间值，以秒为单位，经过该时间后，系统将挂起 VC。它与 **set** 命令中设置的非活动计时器值相一致。

Connected HHH:MM:SS

VC 已连接接口多少小时、分钟、秒的总计数。

对于挂起的 VCs:

Hrs. Max Suspended
系统结束连接前，VC 处于挂起状态的最大小时数。它与 **set** 命令中设置的最大挂起时间值相一致。

Suspended HH:MM:SS
VC 已挂起多少小时、分钟、秒的总计数。

dhcp-servers
显示关于 DHCP 服务器及其 IP 地址的配置信息。

ip-address-assignment
显示 IP 地址分配给客户机的方法。

ip-pool
显示当前池的使用率。

例:

```
DIALs Console> list ip-pool
Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*    192.1.100.18      192.1.100.74            57            57
      192.2.200.1     192.2.200.250           250           250

Note: The * indicates from which block the next address will be retrieved.
```

suspended-vcs
显示所有挂起虚拟连接的属性。请参阅 **all-vcs** 参数说明，以获得对属性的解释。

vc-parameters
显示使用 **set vc-parameters** 命令设置的 vc-parameters 的值。

Reset

在 talk 6 中使用 **reset** 命令动态激活对 DIALs 接口的配置更改。

语法:

reset all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all 动态激活 DHCP、IP 地址分配和 IP 池配置更改。

dhcp-parameters
动态激活 DHCP 配置。

ip-address-assignment
动态激活 IP 地址分配方法配置。

ip-pool
动态激活 IP 地址池配置。

vc-parameters
动态更新 VC 配置更改。

拨出接口配置命令

要进入拨出接口参数环境:

1. 在 * 提示符下，输入 **talk 6**。
2. 在 Config > 提示符下，输入 **net*n***。
3. 在 Circuit config: n> 提示符下，输入 **encapsulator**。

在 dial-out config> 提示符下，表41列出可用命令。

表 41. 拨出接口配置命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Set	定义与调制解调器有关的端口名。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Set

使用 **set** 命令为调制解调器定义端口名。

语法:

set portname *name*

端口名 定义与调制解调器有关的端口的名称。使用该名称定义***调制解调器池***。 名称长度可达 30 个字符。

缺省值: ALL_PORTS

例: dial-out config>**set portname localcalls**

监控拨入接口

监控拨入接口类似于监控其它 PPP 拨号线路。详细说明，请参阅 *Access Integration Services 软件用户指南* 中的『配置和监控点对点协议接口』。

监控拨出接口

表42 列出在监控拨出接口时用到的命令。

表 42. 拨出接口监控命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Clear	复位拨出接口统计信息。
List	列出拨出接口的当前状态、在该接口上传输和接收到的字节数，以及客户机的当前参数。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Clear

使用 **clear** 命令复位该接口所接收和传输的八位字节数统计信息。

语法:

clear

例:

```
clear
Statistics reset.
```

List

使用 **list** 命令，显示拨出接口的当前状态。**list** 命令始终显示拨出网络的当前状态、自状态更改后经过的时间，以及接收和传输的字节数。

语法:

list

非活动接口示例:

```
list
Dial-out Settings for current session:

Dial-out state is DOWN
Time since change           = 52 minutes and 34 seconds

Dial-out Octets transmitted = 0
Dial-out Octets received    = 0

Session down, no valid settings
```

注: 客户机使用 telnet 连接拨出端口时，不显示用户名，因为服务器未执行任何认证。

活动接口示例:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 3 seconds

Dial-out Octets transmitted = 14
Dial-out Octets received    = 765

Current user                = not available
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = TELNET
Options negotiated:
        Will Suppress Go Ahead
        Wont' Echo characters
```

活动 **IBM DIALs** 拨出客户机示例:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 12 seconds

Dial-out Octets transmitted = 11
Dial-out Octets received    = 756
```

```
Current user                = ebooth
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = DIALs
```

第23章 使用 Thin Server(瘦服务器)功能部件

本章说明说明如何使用 IBM 2212 中的 Thin Server(瘦服务器)功能部件 (TSF)。

网络工作站概述

一个网络工作站类似于一台个人计算机 (PC)，具有键盘、显示器和鼠标。网络工作站与 PC 机的主要差别在于，网络工作站文件驻留在网络服务器上，而不是机器的硬盘上。网络工作站提供给用户一个图形用户界面 (GUI)，从这里能够存取多种资源，如仿真器、远程 X 应用、Web 浏览器、应用程序和打印机。

网络工作站使用 TCP/IP ，通过令牌环网或以太网，与服务器实现连接通信。网络工作站加电进程是:

- 启动非易失性随机存取内存驻留引导监控程序，执行加电自检。
- 网络工作站与 BootP 或 DHCP 服务器联系，这两服务器可向网络工作站提供有关的信息，如 IP 地址、它的服务器地址、引导文件的路径和名称。此外，网络工作站还可从它的非易失性随机存取内存中存储的值检索以上信息。
- 网络工作站使用日常文件传输协议 (TFTP)、远程文件系统/400 (RFS/400) 或网络文件系统 (NFS)，从基本代码服务器上下载如操作系统、硬件配置和应用程序的基本代码。
- 网络工作站从终端配置服务器下载基于终端的配置信息，如连接网络工作站的打印机，或网络工作站键盘语言配置方面的信息。
- 工作站显示注册屏。您可输入用户 ID 和口令。
- 认证服务器验证您的用户 ID 和口令，允许存取个人用户文件。
- 下载您的个人化的环境喜好设置。
- 网络工作站显示您的个人化桌面。

请参阅 *IBM Network Station Manager Installation and Use*, SC41-0664，以获取有关网络工作站的更多的信息。

Thin Server(瘦服务器)功能部件概述

在 TSF 环境下，一物理设备可起到 BootP/DHCP 服务器、引导服务器、终端配置服务器和认证服务器的功能，或者，也可认为各服务器是一独立的设备。例如，您可将 AS/400 连接到网络工作站上，并且 AS/400 是用做 BootP 服务器、基本代码服务器、终端配置服务器和认证服务器的。那么，这当中的各服务器也就可以是一独立的物理单元。例如，可将网络工作站连接到一个网络上，在该网络上，DHCP 服务器是一台 NT 服务器，基本代码服务器是一台 AS/400，终端配置服务器是另一台 AS/400，认证服务器也是另外的一台 AS/400。

Thin Server 功能部件允许将 2212 作为基本代码服务器。为什么要使用 TSF，在第248页的图23和第249页的图24中给出了一个例子，对此做了说明。在第248页的图23中，网络工作站所需要的任何文件，都可以从一个服务器上下载。网络工作站加电时，下载的内容可达若干兆字节。这就对网络基础设施及作为基本代码/终端配置服务器或认证服务器有着极大的需求，特别是当许多网络工作站同时加电时。第249页的图24显示

带有在远程站点使用的 Thin Server 的网络。许多与网络工作站引导代码相关的文件将由该 Thin Server 高速缓存。网络工作站加电时，大部分引导代码从该 Thin Server 上装入，而只有少量数据需要通过网络设施结构传送。在任一服务器上的这种减量处理将降低网络通信量，缩短网络工作站完成加电所需时间。

因为 Thin Server 高速缓存的文件是主文件服务器上驻留的文件的副本，而主文件服务器上文件版本已修改，所以 Thin Server 需要更新相应文件版本。在下列情况下，Thin Server 将验证所有高速缓存的文件与主文件服务器版本是同一的:

1. 对 IBM 2212 加电
2. 重装或重启 IBM 2212
3. 重启 TSF
4. TSF 配置中指定的时间间隔到点
5. SNMP MIB 操作参数触发 Thin Server
6. 发出 TSF `talk 5` **refresh** 命令
7. 每次存取文件(除 TFTP)。TSF 将验证存取的每个文件匹配主文件服务器上的版本。如果检测出差异，则文件更新。接着 TSF 验证其余文件是否匹配主文件服务器上的版本。

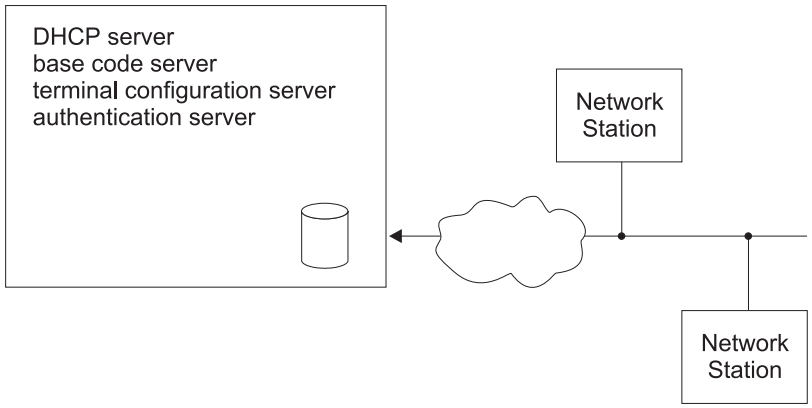


图 23. 不带 Thin Server 的远程网络工作站,

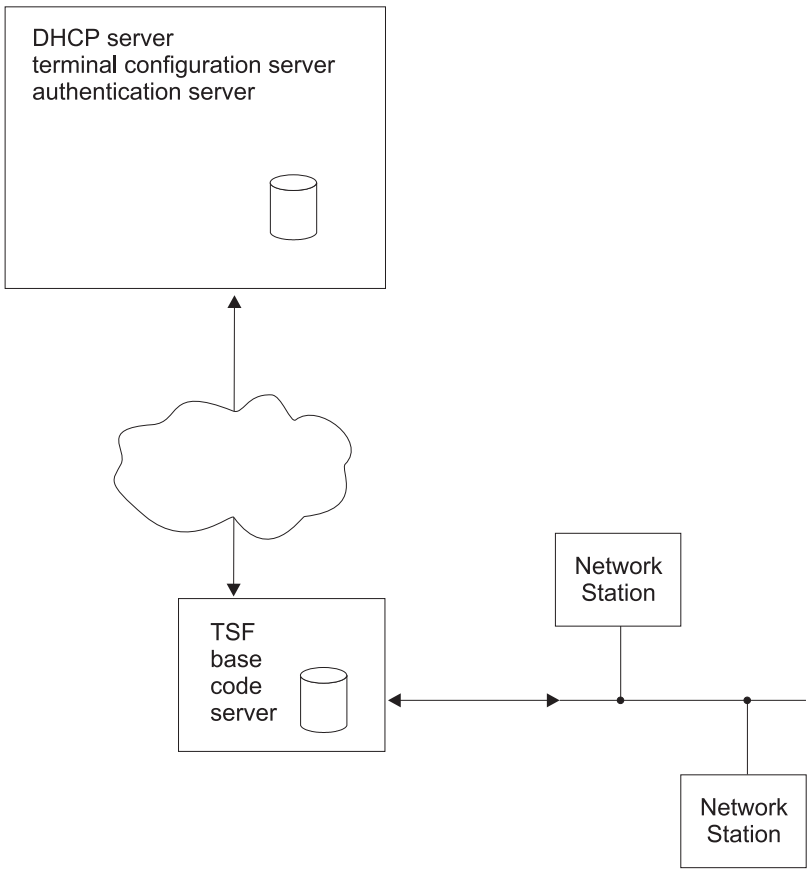


图 24. 带 Thin Server 的远程网络工作站

BootP/DHCP 支持

2212 本身不充当 BootP/DHCP 服务器。而应将 2212 配置成 BootP/DHCP 请求的中继代理。

请参阅 *IBM Network Station Manager Installation and Use*, SC41-0664, 以获取多服务器环境更多的信息。

用于网络工作站通信的协议

网络工作站和服务器通信使用的协议，是由 BootP/DHCP 配置所确定的，或是由网络工作站 NVRAM 配置所确定的。不论是怎样确定的，网络工作站使用的协议，都必须与配置 TSF 的方式兼容。

如果配置 TSF，使其使用 RFS 与主文件服务器通信，则 TSF 将接受来自网络工作站上的 RFS 和 TFTP 请求，而不响应网络工作站的 NFS 请求。

同样，如果将 TSF 配置成使用 NFS 与主文件服务器通信，它将接受来自网络工作站的 NFS 和 TFTP 请求，而不响应网络工作站的 RFS 请求。

使用 RFS

TSF 使用 RFS 建立与 AS/400 的连接。网络工作站请求打开文件时，TSF 将该请求转发给 AS/400 以获得许可。如果不许可，TSF 将不把所请求的文件发送给网络工作站。如果许可，而请求文件的 AS/400 版本与 IBM 2212 TSF 上存储的版本不同，则将网络工作站的请求中继给 AS/400。如果 AS/400 上的文件与 TSF 高速缓存文件版本相同，则 TSF 将文件提供给网络工作站。

如果 TSF 无法建立与 AS/400 的连接，TSF 则将当前高速缓存的文件提供给网络工作站。

使用 TFTP

如果 TFTP 正用于网络工作站和 TSF 之间的通信，则 TSF 将提供网络工作站所请求的文件，只要这些文件可用。TSF 和主文件服务器之间不进行版本验证。如果 TSF 高速缓存中的文件不可用，则将网络工作站的请求转发给主文件服务器。

使用 NFS

如果 NFS 正用于网络工作站和 TSF 之间的通信，则当网络工作站请求文件时，TSF 将开始提供文件，只要文件已高速缓存。同时验证该文件是否与主文件服务器版本相同。如果不同，TSF 中断提供文件并立刻开始从主文件服务器上下载新的版本。

如果 TSF 未高速缓存该文件，TSF 将返回一条“文件未找到”消息。另外，如果被请求的文件驻留在一目录下，该目录是通过使用 *include subdirectories* 而为 TSF 所配置的，或者，被请求的文件驻留在如此配置的目录的子目录下，则 TSF 启动高速缓存文件，只要该文件在主文件服务器上存在。

文件高速缓存更新

在 IBM 2212 上用于文件高速缓存的协议由 TSF 配置确定。用户将使用 **add master-file-server** 命令指定一个主服务器。

如果指定 *rfs*，系统提示您提供一个预安装列表文件名。该预安装列表是一个 ASCII 文件，用来指定 TSF 将高速缓存的每个文件的全限定文件名。

如果指定 *nfs*，系统将提示您提供将高速缓存的目录名(可能提供一些缺省值)。当指定一个目录时，将提示您是否包括子目录。指定否(即不包括子目录)，TSF 则预安装指定目录中的所有文件到 TSF 高速缓存中。指定是(包括子目录)，则当网络工作站请求文件时，TSF 不预安装该目录中的文件，而是动态检索该目录及其子目录中的这些文件。

处于刷新进程中的文件将不发送到网络工作站。

配置 Thin Server 环境

安装 TSF 时，除 TSF 自身配置以外，还需要考虑几项配置。这部分讨论一些更改，这些更改对于 BootP/DHCP 服务器、主文件服务器、IBM 2212 BootP 中继、IBM 2212 内部 IP 地址和 IBM 2212 TSF 配置来说，可能是必要的。第253页的『配置样本』中讨论了一个 Thin Server 连接 AS/400 的例子，该 AS/400 运行网络工作站管理器发行版 2.5。

以下部分说明 Thin Server 环境配置进程:

- 『配置建议』
- 第252页的『配置 BootP/DHCP 服务器』
- 第252页的『配置 Thin Server 环境下的服务器』
- 第252页的『配置 BootP 中继』
- 第252页的『配置内部 IP 地址』
- 第252页的『配置 TSF』
- 第253页的『配置样本』

配置建议

下面的配置建议能帮助您从 TSF 中得到最大收益:

- 使用硬文件。

  尽管 TSF 不需要硬文件，但是在 TSF 内存高速缓存配置过小，或由于 2212 中的其它功能的影响而无法配置充分时，硬文件能提高性能，当 TSF 或 2212 重启或重装时，就可发生这种作用。
- 建议最大网络工作站数为 30。

  尽管 TSF 允许的网络工作站可达 200 个，但这个建议值是建立在如果网络工作站在同时 IPL 情况下，例如出现断电，启动网络工作站需多长时间。
- 主文件服务器应当是运行网络工作站管理程序的服务器。

  尽管 TSF 允许主文件服务器 IP 地址可取任何值，但是建议使用可运行网络工作站管理程序 (NSM) 的设备的地址，这样，文件结构就可与网络工作站兼容，因而也可与 TSF 兼容，从而可提供 TSF 请求的文件。
- 定义足够内存以容纳所有高速缓存文件。

  如果无硬文件，则必须执行这一点。如果有，内存存取则快于硬文件存取。所需内存大小随特定环境而变。使用 `Talk 5` **list config** 命令，及时确定特殊情形下您的文件集的大小。*Thin Server 正在使用的硬文件存储池* 显示的值是文件集的大小值，以千字节为单位。但是，如果在系统环境中添加或删除了不同类型的网络工作站或应用程序，则该值可能改变。
- 如果使用的是 NFS，则 TSF 查找需要哪些文件。

  该查找过程可能消耗若干网络工作站加电序列，以使 TSF 能够识别所有必需的文件。

配置 BootP/DHCP 服务器

运行网络工作站管理器发行版 3 时，如果使用 Thin Server，则需要 DHCP。如果将 AS/400 作为主文件服务器，则可能使用网络工作站管理器发行版 2.5，此时，采用 BootP 而非 DHCP。

对于 BootP，只能指定一个服务器地址。使用 **sa** 标签指定该地址。该标签可能已存在于给定网络工作站的 BootP 记录中，也可能不存在。当不存在时，则创建它，并将其值设为 2212 内部 IP 地址。如果已存在，则改成 2212 内部 IP 地址。

对于 DHCP，在使用 Thin Server 时，需要对某些字段进行修改，它们是:

- 选项 66 或 bootstrap server - 基本代码服务器 IP 地址

  该值应设置为 IBM 2212 内部 IP 地址
- 选项 211 - 用于基本代码服务器的协议

  如果将 Thin Server 作为 NFS 的主文件服务器类型，则必须使用 *nfs* 或 *tftp*。如果 Thin Server 原先配置为 RFS 的主文件服务器类型，则必须使用 *rfs/400* 或 *tftp*。
- 选项 212 - 终端配置服务器

  该地址应当是主文件服务器的 IP 地址。该地址不应是 Thin Server 的 IP 地址。

有关 NS 与 BootP 和 DHCP 交互作用的细节，请参阅 *IBM Network Station Manager Installation and Use*，SC41-0664。

配置 Thin Server 环境下的服务器

对于 RFS，预安装列表应安装在 AS/400 上。可从 Internet 站点 `http://www.networking.ibm.com/netprod.html#routers` 得到可用的预安装列表。您应当从该站点 ftp 该 LoadList.file，将它放在 AS/400 的 `/QIBM/ProdData/OS400/NetStationRmtController` 下。可能需要创建该 NetStationRmtController 目录。

对于 NFS，不需要为 Thin Server 作特别改动。

配置 BootP 中继

应启动 IBM 2212 的 BootP 中继代理，还应配置适当的 BootP 和 DHCP 服务器，以使 BootP 中继转发这些服务器。请参阅 *Access Integration Services 软件用户指南* 以获取更多的信息。

配置内部 IP 地址

如果内部 IP 地址已存在，则无需特别的改动。如果当前未指定内部 IP 地址，则应指定。请参阅 *Protocol Configuration and Monitoring Reference Volume 1* 以获取更多的信息。

配置 TSF

使用第259页的『第24章 配置和监控 Thin Server(瘦服务器)功能部件』中讨论的命令配置 Thin Server。

至少需要输入以下命令:

1. **load add package thin-server**
2. **set mode enable**
3. **add master-server**

配置样本

下面是连接有 AS/400 (运行网络工作站管理器 R2.5) 的 TSF 的配置实例。

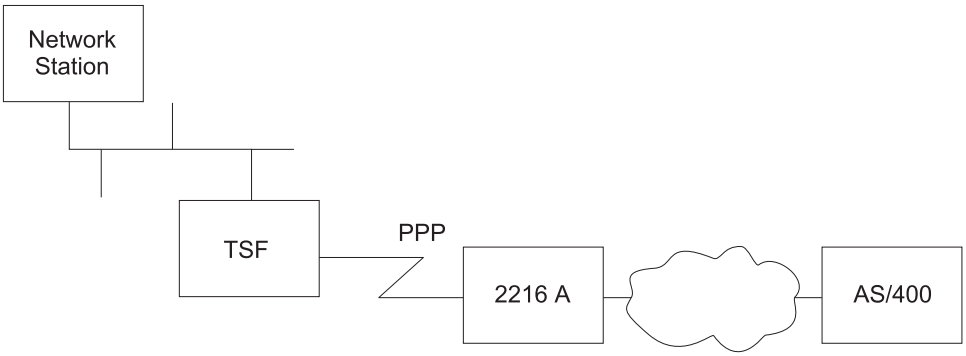


图 25. TSF 样本配置

以下论述是说明如何配置基于以上网络的 Thin Server 功能部件，并假定以下情形:

- AS/400 将作为 BootP 服务器。
- 2216 A 是一个路由器 (无 TSF 配置或无 TSF 特殊配置)。
- 网络 IP 连通性已通过验证，例如，AS/400 能 PING IBM 2212 (TSF)，IBM 2212 能 PING AS/400。
- IBM 2212 (TSF) 上当前未启用 BootP 中继
- IBM 2212 (TSF) 中当前未配置 IP 内部地址

配置 AS/400

BootP (NSM 发行版 2.5)

1. 用 NSM 定义 NS
2. ftp BootP 表到有 ASCII 编辑器的系统

```
c:\>ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password. Password:
230 QSECOFR logged on.
ftp> ascii
ftp> get qusrsys/qatodbtp.bootptab bootp.tab
ftp> quit
```

3. 使用 ASCII 编辑器编辑文件，增加 “sa” 标签，指定 2212 (TSF) 的内部 IP 地址:

```
OLD LINE
--------
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
```

```
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION

MODIFIED LINE
-------------
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION:sa=192.9.250.6
```

其中 192.9.250.6 是 2212 (TSF) 的内部 IP 地址

4. ftp 该 BootP 表返回 AS/400

```
c:\> ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> ascii
ftp> put bootp.tab qusrsys/qatodbtp.bootptab
ftp> quit
```

设置预安装列表

您可以从 internet 站点: http://www.networking.ibm.com/netprod.html#routers 上获得一个预安装列表。

一旦获得预安装列表，您即可将它 “ftp” 至 AS/400。

1. 确保您的本地目录位置在 “LoadList.file” 处。
2. ftp 到 AS/400 - “test400” 是本例中 AS/400 的名称。

```
ftp test400
Connected to test400.raleigh.ibm.com.
Name (test400:root): qsecofr
Enter password.
Password:
QSECOFR logged on.
```

3. 改至目标 AS/400 的正确目录下:

```
ftp> cd /
Current directory changed to /.
ftp> cd qibm/proddata/os400/
Current directory changed to /qibm/proddata/os400.
ftp> dir
PORT subcommand request successful.
 List started.
QTCP            34816 04/30/97 02:50:36 *DIR     REXEC/
QSECOFR         33792 07/24/98 08:04:55 *DIR     NetStationRmtController/
 List completed.
```

4. 如果目录 “NetStationRmtController” 不存在，则创建它。

```
ftp> MKD
(directory - name) NetStationRmtController
Created directory /qibm/proddata/os400/netstationrmtcontroller
```

5. 改至 NetStationRmtController 目录:

```
ftp> cd NetStationRmtController
Current directory changed to /qibm/proddata/os400/Netstationrmtcontroller.
```

6. 传送文件到 AS/400:

```
ftp> ascii
Representation type is ASCII nonprint.
ftp> put LoadList.file
 PORT subcommand request successful.
 Sending file to /qibm/proddata/os400/Netstationrmtcontroller
 File transfer completed successfully.
```

配置 TCP/IP

您的 TCP/IP 配置取决于您的特定环境。

配置 IBM 2212 (TSF)

BootP 中继

1. 确定 BootP 中继是否已配置:

```
*
*
t 6
Config>protocol ip
Internet protocol user configuration
IP config>list bootp
BOOTP forwarding: enabled
Max number of BOOTP forwarding hops: 4
Min secs of retry before forwarding: 0
Configured BOOTP servers:      192.9.220.21
IP config>
```

2. 如果尚未启用，则启用:

```
IP config>enable bootp
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
IP config>
```

3. 如果您的网络工作站 BootP 或 DHCP 服务器不在配置的服务器列表中，则添加之:

```
IP config>add bootp-server
BOOTP server address [0.0.0.0]? 9.37.121.6
IP config>
```

内部 IP 地址

1. 确定内部 IP 地址是否已配置:

```
 Config>protocol ip
 Internet protocol user configuration
 IP config>list addresses
 IP addresses for each interface:
    intf     0   9.37.177.97      255.255.248.0    Local wire...
    intf     1   192.9.220.2      255.255.255.0    Local wire...
    intf     2   192.9.250.6      255.255.255.0    Local wire...
    intf     3   192.9.222.2      255.255.255.0    Local wire...
    intf     4                                     IP disabled...
    intf     5                                     IP disabled...
    intf     6   192.9.223.2      255.255.255.0    Local wire...
IP config>
```

2. 配置内部 IP 地址。

```
IP config>set internal-ip-address
Internal IP address [192.9.223.2]? 192.9.250.6
IP config>
```

3. 再次列出地址。

```
IP config>list addresses
IP addresses for each interface:
   intf     0   9.37.177.97      255.255.248.0    Local wire
   intf     1   192.9.220.2      255.255.255.0    Local wire
   intf     2   192.9.250.6      255.255.255.0    Local wire
   intf     3   192.9.222.2      255.255.255.0    Local wire
   intf     4                                     IP disabled
   intf     5                                     IP disabled
   intf     6   192.9.223.2      255.255.255.0    Local wire
Internal IP address: 192.9.250.6
IP config>
```

Thin Server 功能部件

1. 增加加载包 thin-server

   配置 Thin Server 功能部件之前，必须配置该加载包。

   首先，查看该 thin 服务器包是否可用。

   ```
   Config>load list available
   Available Packages
   ------------------
   appn package
   tn3270e package
   thin-server package
   Config>
   ```

   如果不可用，则在继续执行前，取得正确的软件版本。

   如果可用，验证该包尚未装入。

   ```
   Config>load list configured
   Configured Packages
   -------------------
   thin-server package
   Config>
   ```

   如果已装入或配置(如上所示)，则可继续配置 TSF。如果尚未装入，则需增加该 Thin Server 包:

   ```
   Config>load add package thin-server
   thin-server package configured successfully
   This change requires a reload.
   Config>
   ```

2. 重装

   如果必须增加该 Thin Server 信息包，则必须现在写配置，并重装 IBM 2212。

3. 设置启用模式

   信息包装入时，Thin Server 最初禁用。在配置 Thin Server 参数前，必须将模式置为启用。

   ```
   *
   *
   t 6
   Config>feature tsf
   Thin server config>set mode enable

   Thin server feature (TSF) is fully enabled once
   you have entered a Master File Server for either
   RFS or NFS. Please add a master-file-server if one is not already configured.
   Thin server config>
   ```

4. 添加主文件服务器。

一旦 Thin Server 功能部件启用，则必须配置主文件服务器。这里，主文件服务器是一个 AS/400，因此需要增加一个 RFS 主文件服务器。对于该网络，缺省 TFTP 超时参数和重试参数值必须适当。

```
Thin server
config>add master-file-server rfs-as400
File Server IP address [0.0.0.0]? 9.37.100.68
TFTP Packet Timeout in seconds (5 - 10) [5]?
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (有效值 are 512, 1024, 2048, 4096, 8192) [8192]?
Pre-load File name [/QIBM/ProdData/OS400/NetstationRmtController/Load list.file]?
Thin server config>
```

在令牌环网接口上，我们的 AS/400 的 IP 地址是 9.37.100.68。在 AS/400 上安装预装入列表文件时，我们指定了它的名称以匹配 Thin Server 缺省名，这样就不需要修改。

5. 设置 time-to-refresh-pre-load-list (任选)

   执行刷新的缺省时间点是白天 1:00 AM。如果大文件已修改，需要 Thin Server 下载，则选择此选项，在最小程度上降低对性能的影响。

6. 设置 interval-pre-load-list (任选)

   验证与主文件服务器处于同一层的高速缓存文件的缺省时间间隔是每隔一天。该参数值和 time-to-refresh-pre-load-list 参数值确定验证文件的频率。如果网络工作站文件更改不频繁，也许应设置这些参数，一星期刷新一次，或一月刷新一次。

7. 设置内存(任选)。

   文件高速缓存所需的缺省 16 MB RAM 高速缓存内存应足够。如果几个网络工作站同时使用 TSF，请参阅第251页的『配置建议』寻求建议。

8. 设置 hard file (任选)

   建议使用一个硬文件。如果没有硬文件，该参数应设为 *no*。

使用 TSF

第24章 配置和监控 Thin Server(瘦服务器)功能部件

本章说明如何使用 Thin Server 功能部件 (TSF) 配置和操作命令，它包括以下几个部分:

- 『进入 TSF 配置环境』
- 『TSF 配置命令』
- 第267页的『进入 TSF 监控环境』
- 第268页的『TSF 监控命令』

进入 TSF 配置环境

按以下步骤进入 TSF 配置进程。

1. 在 OPCON 提示符下，输入 **talk 6**。 (有关该命令的细节，请参阅*Access Integration Services 软件用户指南*中的 "OPCON 进程和命令"。)例如:

   ```
   * talk 6
   Config>
   ```

   输入 **talk 6** 命令后，终端将显示 CONFIG 提示符 (Config>)。如果首次输入配置，提示符将不出现，这时请再次按 **Return**。
2. 在 CONFIG 提示符下，输入 **feature tsf** 命令，以进入 Thin server config> 提示状态。

TSF 配置命令

要配置 TSF，请在 Thin server config> 提示符下，输入这些命令。

表 43. TSF 配置命令摘要

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Add	添加主文件服务器 (RFS 或 NFS)。
Delete	删除主文件服务器 (RFS 或 NFS)。
List	列出 thin server 配置。
Modify	修改主文件服务器 (RFS 或 NFS)。
Set	设置 thin server 参数。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Add

使用 **add** 命令，添加一个主文件服务器配置。

如果选取 *nfs* 作为主文件服务器类型，Thin Server 将使用 NFS 与主文件服务器通信，实现文件同步传输，而 NS 可使用 TFTP 或 NFS 与 Thin Server 通信。如果选取 *rfs* 作为主服务器类型，Thin Server 将使用 RFS 与主文件服务器通信，实现文件同步传输，而 NS 可使用 TFTP 或 RFS 与 Thin Server 通信。

语法:

add master-file-server nfs-s390
nfs-nt
nfs-aix
nfs-other
rfs-as400

nfs-s390

当 TSF 与 S/390 连接时使用。

文件服务器 IP 地址

有效值: 任何有效的 IP 地址

缺省值: 无

tftp packet timeout

有效值: 5 - 10 秒

缺省值: 5

tftp maximum retry limit

有效值: 1 - 10

缺省值: 1

maximum segment size

指定最大信息包分段的大小。

有效值: 512, 1024, 2048, 4096, 8192 (字节)

缺省值: 8192

additional Include subdirectories

指定是否添加附加的 Include 子目录。如果 TSF 需要高速缓存不在缺省目录中的文件，则可能指定附加的子目录。

有效值: 是或否

缺省值: 是

additional Include subdirectory path

指定要添加的 Include 子目录路径。

有效值: a-z, A-Z, 0-9, ., _, --, /

缺省值: 无

include all subdirectories under this directory

指定是否包括指定附加子目录中的所有嵌套子目录。

有效值:

- 否

  TSF 将预加载指定目录中的所有文件。

- 是

  TSF 不预加载指定目录中的文件。TSF 而是按需要加载目录及其子目录下的文件。

缺省值是: 否

nfs-nt 当 TSF 与 Windows-NT 连接时使用。

file server IP address

有效值: 任何有效的 IP 地址

缺省值: 无

tftp packet timeout

有效值: 5 - 10 秒

缺省值: 5

tftp maximum retry limit

有效值: 1 - 10

缺省值: 1

maximum segment size

指定最大信息包分段的大小。

有效值: 512, 1024, 2048, 4096, 8192 (字节)

缺省值: 8192

additional Include subdirectories

指定是否添加附加的 Included 子目录。

有效值: 是或否

缺省值: 是

additional Include subdirectory path

指定要添加的 Include 子目录路径。

有效值: a-z, A-Z, 0-9, ., _, --, /

缺省值: 无

include all subdirectories under this directory

指定是否包括指定附加子目录中的所有嵌套子目录。

有效值:

- 否

  TSF 将预加载指定目录中的所有文件。

- 是

  TSF 不预加载指定目录中的文件。TSF 而是按需要加载目录及其子目录下的文件。

缺省值是: 否

nfs-aix

当 TSF 与 AIX 连接时使用。

file server IP address

有效值: 任何有效的 IP 地址

缺省值: 无

tftp packet timeout

有效值: 5 - 10 秒

缺省值: 5

tftp maximum retry limit

有效值: 1 - 10

缺省值: 1

maximum segment size

指定最大信息包分段的大小。

有效值: 512, 1024, 2048, 4096, 8192 (字节)

缺省值: 8192

additional Include subdirectories

指定是否添加附加的 Include 子目录。

有效值: 是或否

缺省值: 是

additional Include subdirectory path

指定要添加的 Include 子目录路径。

有效值: a-z, A-Z, 0-9, ., _, --, /

缺省值: 无

include all subdirectories under this directory

指定是否包括指定附加子目录中的所有嵌套子目录。

有效值:

- 否

  TSF 将预加载指定目录中的所有文件。

- 是

  TSF 不预加载指定目录中的文件。TSF 而是按需要加载目录及其子目录下的文件。

缺省值是: 否

nfs-other

打算手动指定所有子目录时使用。

file server IP address

有效值: 任何有效的 IP 地址

缺省值: 无

tftp packet timeout

有效值: 5 - 10 seconds

缺省值: 5

tftp maximum retry limit

有效值: 1 - 10

缺省值: 1

maximum segment size

指定最大信息包分段的大小。

有效值: 512, 1024, 2048, 4096, 8192 (字节)

缺省值: 8192

additional Include subdirectories

指定是否添加附加的 Included 子目录。

有效值: 是或否

缺省值: 是

additional Include subdirectory path

指定要添加的 Include 子目录路径。

有效值: a-z, A-Z, 0-9, ., _, --, /

缺省值: 无

include all subdirectories under this directory

指定是否包括指定附加子目录中的所有嵌套子目录。

有效值:

- 否

  TSF 将预加载指定目录中的所有文件。

- 是

  TSF 不预加载指定目录中的文件。TSF 而是按需要加载目录及其子目录下的文件。

缺省值是: 否

rfs-as400

当 TSF 与 AS/400 连接时使用。

file server IP address

有效值: 任何有效的 IP 地址

缺省值: 无

tftp packet timeout

有效值: 5 - 10 秒

缺省值: 5

tftp maximum retry limit

有效值: 1 - 10

缺省值: 1

maximum segment size

指定最大信息包分段的大小。

有效值: 512, 1024, 2048, 4096, 8192 (字节)

缺省值: 8192

pre-load file name

指定预加载文件的文件名和路径。

有效值: a-z, A-Z, 0-9, ., _, --, /缺省值: /QIBM/ProdData/OS400/NetStationRmtController/LoadList.file

NFS 的配置实例:

```
Thin server config> add master-file-server nfs
 File Server IP address [0.0.0.0]? 10.22.55.94
 TFTP Packet Timeout in seconds (5 - 10) [5]?6
 TFTP Max Retry Limit (1 - 10) [1]? 7
 TFTP Max Segment Size in bytes (有效值 are 512, 1024, 2048, 4096, 8192) [8192]?
512

Default Include Directories:

    Include Directory List Follows:

    Include
      all
    Subdirs?   Directory Names
    --------   ----------------------------------
       N       /hfs/usr/lpp/nstation/standard
       Y       /hfs/usr/lpp/nstation/standard/mods
       Y       /hfs/usr/lpp/nstation/standard/nls
       Y       /hfs/usr/lpp/nstation/standard/fonts
       Y       /hfs/usr/lpp/nstation/standard/java
       Y       /hfs/usr/lpp/nstation/standard/keyboards
       Y       /hfs/usr/lpp/nstation/standard/proms
       Y       /hfs/usr/lpp/nstation/standard/X11
       Y       /hfs/usr/lpp/nstation/standard/configs
       Y       /hfs/usr/lpp/nstation/standard/SysDef
       Y       /hfs/usr/lpp/nstation/standard/zoneinfo
   Do you want additional Include Subdirectories (Y)es (N)o? [y]

Include Subdirectory [   ]? /usr/lpp/nstation/standard/whatever
Include all subdirectories under this directory (Y)es or (N)o? [n]

Do you want additional Include Subdirectories (Y)es (N)o? []
```

配置 RSF 的实例:

```
Thin server config> add master-file-server rfs
 File Server IP address [0.0.0.0]? 01.01.01.98
 TFTP Packet Timeout in seconds (5-10) [5]? 6
 TFTP Max Retry Limit (1-10) [1]? 7
 TFTP Max Segment Size in bytes (有效值 are 512, 1024, 2048, 4096, 8192) [8192]?
512

 Pre-Load File name
 [/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Delete

使用 **delete** 命令删除一个主文件服务器配置。

语法:

delete nfs

rfs

nfs 配置 NFS 主文件服务器时使用。

rfs 为 RFS 主文件服务器配置 TSF 时使用。

List

使用 **list** 命令显示 TSF 配置。

语法:

list all

例:

```
Thin server config> list all

Thin Server Feature:
     Enabled
     Interval to refresh cache in day(s):  2
     Time of day (military time) to refresh cache: 0800
     Megabytes used for Thin Server RAM cache:  4
     Use Hard File:  YES

Master Thin Server list:
     Server IP Address: 9.37.111.12
     Server Protocol: NFS
     TFTP Packet Timeout in seconds:  10
     TFTP Retry Limit              :  6
     TFTP Max Segment Size in bytes:  512


     Initial directories setup for server type: NFS-AIX

  NFS Include Directory List Follows:

     Include
       all
     subdirs?    Directory Names
     --------    ------------------------------------------

        N        /usr/netstation
        Y        /usr/netstation/mods
        Y        /usr/netstation/nls
        Y        /usr/netstation/fonts
        Y        /usr/netstation/java
        Y        /usr/netstation/keyboards
        Y        /usr/netstation/proms
        Y        /usr/netstation/X11
        Y        /usr/netstation/configs
        Y        /usr/netstation/SysDef
        Y        /usr/netstation/zoneinfo
```

Modify

使用 **modify** 命令修改一个主文件服务器配置。

语法:

modify master-file-server nfs

rfs

nfs 配置了 NFS 主文件服务器时使用。

rfs 为 RFS 主文件服务器配置 TSF 时使用。

NFS 的配置实例:

TSF 配置命令 (Talk 6)

```
Thin server config> modify master-file-server nfs
 File Server IP address [         ]? 10.22.55.94
 TFTP Packet Timeout in seconds (5 - 10) [5 ]? 10
 TFTP Max Retry Limit (1 - 10) [1]? 6
 TFTP Max Segment Size in bytes 有效值 are 512, 1024, 2048, 4096,
 8192) [8192]? 1024

 Include subdirectory [/usr/lpp/tcpip/nstation/standard, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?

 Include subdirectory [/usr/lpp/tcpip/nstation/standard/mods], (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?

 Include subdirectory [/usr/lpp/tcpip/nstation/standard/nls], (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?

 Include subdirectory [/usr/lpp/tcpip/nstation/standard/fonts], (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?

 Include subdirectory [/usr/lpp/tcpip/nstation/standard/java], (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?

 Include subdirectory [/usr/lpp/tcpip/nstation/standard/keyboards], (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?

 Do you want additional Include Subdirectories (Y)es or (N)o? n
```

配置 RSF 的实例:

```
Thin server config> modify master-file-server rfs
 File Server IP address [09.09.255.253 ]? 01.01.01.98
 TFTP Packet Timeout in seconds [5 ]? 10
 TFTP Retry Limit [5 ]? 6
 TFTP Max Segment Size in bytes [8192]? 512

 Pre-Load File name
 [/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Set

使用 **set** 命令设置 TSF 配置参数。

语法:

set mode
interval-pre-load-list
time-to-refresh-pre-load-list
memory-cache
hard-file

mode 指定 TSF 模式。

有效值:

- 启用

  启用模式表示 TSF 完全可运行，将为网络工作站提供高速缓存文件。
- 禁用

  禁用模式表示 TSF 不活动，将不应答网络工作站。网络工作站应配置成直接与服务器通信。

- passthru

  passthru 模式只在 RFS 中用到。Passthru 允许网络工作站与 TSF 联系，但一直从主文件服务器获取文件。

缺省值:

interval-pre-load-list

指定时间间隔(天数)，刷新预加载列表。

有效值: 00 - 365

缺省值: 01

time-to-refresh-pre-load-list

指定刷新高速缓存的军用时刻 (24 小时)。

有效值: 0001 - 2400

缺省值: 0100

memory-cache

指定 Thin Server RAM 高速缓存的内存量(兆字节数)。使用硬文件时，应选择该值，以平衡 TSF 性能与 IBM 2212 中的其它功能。如果不使用硬文件，该值应足够大，以容纳所有高速缓存文件。详细信息，请参阅第251页的『配置建议』。

有效值: 8 - 64 兆字节

缺省值: 16

hard-file

指定是否使用该硬文件。

有效值: 是或否

缺省值: 是

例:

```
Thin server config> set mode passthru
This server feature (TSF) is passthru
Thin server config> set interval-pre-load-list
Interval to refresh the Pre-Load list in days (00-365) [01]? 1
Thin server config> set time-to-refresh-pre-load-list
Time of day to refresh cache in military time (0001-2400) [0100]
0800
Thin server config> set memory-cache
Amount of memory in megabytes for Thin Server RAM cache (8-64MB) [8]
Thin server config> set hard-file
Use the Hard File  (Y)ex N(o) [Y]? yes
```

进入 TSF 监控环境

按以下步骤使用 TSF 监控命令。该进程使您进入 TSF *监控*进程。

1. 在 OPCON 提示符下，输入 **talk 5**。 (有关该命令的详细说明，请参阅Access Integration Services 软件用户指南.中的*OPCON 进程和命令*。)例:

```
* talk 5
+
```

输入 **talk 5** 命令后，终端上将显示 GWCON 提示符 (+)。如果首次输入配置，提示符将不出现，这时请再次按 **Return**。

2. 在 + 提示符下，输入 < **f tsf** 命令，进入 Thin-Server> 提示状态。

   例:

```
+ f tsf
Thin-Server>
```

TSF 监控命令

本章说明 TSF 监控命令。

表 44. TSF 监控命令摘要

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Delete	从 Thin Server 功能部件文件高速缓存中删除文件。
Flush	清除 Thin Server 功能部件文件的高速缓存。
List	显示 Thin Server 设置和参数值
Refresh	刷新高速缓存。
Reset	复位计数器。
Restart	重启 Thin Server 进程。
Set	更改 Thin Server 功能部件的设置。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Delete

使用 **delete** 命令从 Thin Server 功能部件文件高速缓存中删除文件。

语法:

delete *filename*

filename

指定从文件高速缓存中待删除的文件的名称。

有效值:

缺省值: 无

例如:

```
Thin-Server> delete
Enter filename to delete from the File Cache: /ibm/prod/ns/5494.dat
Are you sure that you want to delete this file? (Y/ [N]): y
File successfully deleted
```

Flush

使用 **flush** 命令清除 TSF 内存和硬盘高速缓存空间。**flush** 命令将删除所有的高速缓存文件。 Thin Server 高速缓存将在下次刷新时从主服务器上更新。网络工作站可能遇到延迟，直到刷新结束。

语法:

flush

例:

```
Thin-Server> flush
The FLUSH command will erase all cached files.
  The Thin Server cache will be updated on the next refresh
  from the Master Server.  Network Stations may experience
  delays until the refresh is completed.
Are you sure you really want to do this? (Y/ [N]: y
All Thin Server cached files have been flushed
```

List

使用 **list** 命令显示 TSF 参数设置。

语法:

list cached-files
config
file-access-counters
file-refresh-counters
pre-load-list
tftp-counters
ts-counters

例:

```
Thin-Server> list cached-files

Cached
File Name     File Size  Time Stamp         Flags  Host File Name
------------  ---------  -----------------  -----  ----------------
00000026.DAT      2729   04/08/98 13:35:07   RYY   /QIBM/ProdData/OS400/Netstat
ionRmtController/Loadlist.file
00000002.DAT   2049220   09/16/97 08:55:39   RYU   /QIBM/PRODDATA/NETWORKSTATIO
N/KERNEL
                 10060   03/04/97 16:12:44   RY-   /QIBM/PRODDATA/NETWORKSTATIO
N/FONTS/PCF/MISC/7X14B.PCF
    List is Complete
```

标志的含义有:

- WhereFrom
  - R = RFS 客户机
  - N = NFS 客户机
  - - = 无
- InTable
  - - = 不在表中
  - u (or m) = 待更新
  - Y = 在表中
- FileState
  - - = 不在磁盘上
  - D = 污染

– A = 放弃更新
– u = 待更新
– U = 正在更新
– Y = 在磁盘上，且可用

最后两个标志的公共组合(为了表示清楚，显示所有三个标志)是:

- RYY - 有效文件
- RuY - 在进程中全部刷新，该文件尚未验证
- RYU - 该文件正在更新

配置 RSF 的实例:

```
Thin-Server> list config

Thin Server Configuration:
    Thin Server function is:                          Enabled
    Interval to refresh Pre-Load List (#days):        3
    Time of day (Military) to refresh Pre-Load List: 23:59:00
    Memory (KB) currently using for RAM cache:        14
    Maximum memory (KB) configured for RAM cache:     32
    Use Hardfile?:                                    Yes
    Hard File storage defined for Thin Server:        20
    Hard File storage being used for Thin Server:     14
    Number of Files Cached:                           8
    Master Server IP address:                         9.67.43.69
    TFTP Packet Timeout Value:                        10
    TFTP Max Retries:                                 4
    TFTP Max Segment Size:                            1024

    Thin Server Sync Protocol:                        RFS
    Name of Pre-Load List file:
        /QIBM/ProdData/OS400/NetstationRmtController/Loadlist.file
```

NFS 的配置实例:

```
Thin-Server> list config

Configuration:
    Thin Server function is:                          Enabled
    Interval to refresh Pre-Load List (#days):        7
    Time of day (Military) to refresh Pre-Load List: 23:59:00
    Memory (KB) currently using for RAM cache:        14
    Maximum memory (KB) configured for RAM cache:     32
    Use Hardfile?:                                    Yes
    Hard File storage defined for Thin Server:        64
    Hard File storage being used for Thin Server:     20
    Number of Files Cached:                           12
    Master Server IP address:                         9.67.43.34
    TFTP Packet Timeout Value:                        5
    TFTP Max Retries:                                 6
    TFTP Max Segment Size:                            512

    Thin Server Sync Protocol:                        NFS
    Include Directory List Follows:

    Include
      all
    subdirs?   Directory Name(s)
    --------   ------------------------------------------------
       N       /ibm/mount/point/include/
       N       /ibm/mount/point/include/sub1
       Y       /ibm/mount/point/include/sub2
```

例:

```
Thin-Server> list file-access-counters

Disk Statistics/Counters:
    Number of files currently open:                20
    Number of Total File Opens:                    23
    Number of Open Fails when File is Locked:       1
    Number of Read misses - Version Mismatch:       4
    Number of Read misses - File Not Present:       3
    Number of Write misses - Hard File Full:        4
```

例:

```
Thin-Server> list file-refresh-counters

File Refresh Statistics/Counters:
    Number of Refreshes:             6
    Number of Refresh Failures:      2
    Number of Files Refreshed:      14
    Date/Time of Last File Update:  11/11/97 22:21:11
```

例:

```
Thin-Server> list pre-load-list
 <display of pre-load list raw file>
List of Pre-Load List File is Complete
```

例:

```
Thin-Server> list tftp-counters

TFTP Statistics/Counters
    Number of Total TFTP Clients:                          3
    Number of Current TFTP Clients:                        2
    Number of Files Served:                               22
    Number of Files Served by Master Server:              22
```

配置 RSF 的实例:

```
Thin-Server> list ts-counters

Thin Server Statistics/Counters
    Number of Total RFS Clients:                           3
    Number of Current RFS Clients:                         2
    Number of Files Served:                               22
    Number of Files Served by Master Server:              22
    Number of NS Port Mapper socket accepts:               7
    Number of NS Port Mapper sockets currently active/open:   4
    Number of NS Server socket accepts:                    2
    Number of NS 8473 sockets currently active/open:       1
    Number of NS Login socket accepts:                     3
    Number of NS 8476 sockets currently active/open:       1
    Number of RFS writes to a Thin Server cached file:     0
```

NFS 的配置实例:

```
Thin-Server> list ts-counters

Thin Server Statistics/Counters
    Number of NFS Server Reads:                           13
    Number of NFS Server Read Directories:                 8
    Number of Unsupported NFS Requests:                    2
    Number of total NFS Mounts:                           22
```

```
Number of current NFS Mounts:                    7
Number of total NFS clients:                    15
Number of current NFS Clients:                   4
```

Refresh

使用 **refresh** 命令强行刷新高速缓存。

语法:

refresh

例:

```
Thin-Server> refresh

Force a refresh of the cache ? (Y/ [N]): y

Thin Server cache has been refreshed
```

Reset

使用 **reset** 命令动态复位计数器。

语法:

reset all | file-access-counters | file-refresh | tftp-counters | ts-counters

例:

```
Thin-Server> reset all

All Thin Server feature counters have been reset
```

Restart

使用 **restart** 命令重启 TSF 进程。

语法:

restart

例:

```
Thin-Server> restart

Restart Thin Server? (Y/ [N]): y

Thin Server has been restarted
```

Set

使用 **set** 命令设置 TSF 高速缓存模式。

语法:

set mode

mode 指定 TSF 模式。请参阅第266页的『Set』。

有效值:

- enable
- disable
- passthru

例:

```
Thin-Server> set mode ?

DISABLED
ENABLED
PASSTHRU

Thin-Server> set mode disable

Thin Server caching is now disabled
```

第25章 配置和监控 VCRM

虚拟电路资源管理程序 (VCRM) 是支持资源保留协议 (RSVP) 的功能部件，在 *Protocol Configuration and Monitoring Reference Volume 1* 中的 『使用 RSVP』 和『配置和监控 RSVP』 部分，有对 RSVP 的说明。基于 RSVP 的保留请求，VCRM 为在物理接口上的数据流创建连接。为此，VCRM 首先必须确定是否有足够的带宽以容纳保留。

注: 如果您使用的是 WAN 接口，如帧中继或 X.25，则您必须设置线路速度，以使 VCRM 知道有多少带宽可用。有关线路速度的设置过程，在*Access Integration Services 软件用户指南*中的帧中继和 X.25 接口配置和监控章节中有说明。

如果接口是 PPP 链路、LAN 或 WAN，则 VCRM 使用 QoS 和最佳信息包软件排队技术，以使出网链路上的信息包成为优先级。

本章节包括以下部分:

- 『访问 VCRM 配置环境』
- 『访问 VCRM 监控环境』
- 第276页的『VCRM 监控命令』

访问 VCRM 配置环境

为访问 VCRM 配置环境，请在 Config> 提示符下输入下列命令:

```
Config> feature vcrm
VC & Resource Management config console
  --Currently no configurable objects.
Config>
```

所显示的消息旨在说明不能单独配置 VCRM。启用 RSVP 则启用了 VCRM，VCRM 需从 RSVP 的配置中获取其本身所需的参数。

访问 VCRM 监控环境

为存取 VCRM 监控环境，请输入:

```
   *
t 5
```

然后请在 **+** 提示符下输入下列命令:

```
   + feature VCRM
   VCRM console
   VCRM Console>
```

显示出 VCRM Console> 提示符。

VCRM 监控命令

此节说明 VCRM 的监控命令。请在 VCRM Console> 提示符下输入这些命令。

表 45. VCRM 监控命令

命令	功能
? (帮助)	显示该命令级可用的所有命令并列示特定命令的选项(如果有的话)。请参阅第xxvi页的『获得帮助』。
Clear	重置队列统计信息。
Queue	显示软件排队技术的统计信息。
Exit	返回到上一个命令级。请参阅第xxvi页的『退出较低级别的环境』。

Clear

使用 **clear** 命令，重置软件队列的统计信息。

语法:

clear

请参阅 **queue** 命令中的 **clear** 命令实例。

Queue

使用 **queue** 命令，显示 通信流的软件排队情况。

语法:

queue

下面的列表定义了显示 软件队列中所使用的术语:

Quota 保留的带宽量。开始时，”最佳信息包”(B.E.) 拥有全部定额的带宽量。当设置保留时，所保留的带宽 (b/w) 从 B.E. 定额转移到 QoS 定额。

Max-q 最大队列长度，已在信息包中指定。

Curr-q
当前队列长度，已在信息包中指定。

In quota
在指定带宽内发送的信息包或千字节。

Outside quota
出现空闲带宽时，在指定带宽之外发送的信息包或千字节。

Packets/bytes dropped
软件队列丢弃的信息包或千字节。

DLC packets/bytes dropped
通过软件队列后，由 DLC 丢弃的信息包或千字节。

实例:

```
*t 5

+feature vcrm
VCRM console
```

```
VCRM Console>?
CLEAR
QUEUE
EXIT
VCRM Console>queue
Flow-control Queues at sys-clock 346781 Second:
---------
Intf    B.E. Quota:       10000 Kbps            QoS Quota:        0     Kbps
0/Eth   B.E. Max-q        0                     QoS Max-q         0
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:        54169/   3926          in quota:            0/      0
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2048  Kbps            QoS Quota:        0     Kbps
2/PPP   B.E. Max-q        0                     QoS Max-q         0
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:           62/      6          in quota:            0/      0
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2032  Kbps            QoS Quota:        16    Kbps
3/FR    B.E. Max-q        1                     QoS Max-q         1
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:        53160/   4920          in quota:       346596/  31886
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2048  Kbps            QoS Quota:        0     Kbps
4/PPP   B.E. Max-q        1                     QoS Max-q         1
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:           66/      6          in quota:          109/     1
        outside quota:       0/      0          outside quota:       0/
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0

Max total queue length=1;  current total length=0
VCRM Console>clear
Flow-control Queues cleared at sys-clock 346786 Second:
-------
VCRM Console>
```

监控 VCRM (Talk 5)

附录. 远程 AAA 属性

本章包括 Radius、TACACS 和 TACACS+ 服务器使用的远程 AAA 属性。

Radius

IBM 供应商 ID: 211

授权属性

初步标准

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

values

TUNNEL_TYPE		integer
3	L2TP	
TUNNEL_MEDIUM_TYPE		integer
1	IP	
TUNNEL_SERVER_EP		string
	ip address	

IBM 供应商指定

NAS_TUNNEL_PASSWORD	101
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
SUBNETMASK	215
PRIVILEGE	216

密钥字

密钥字用于 Radius 服务器，该服务器允许使用供应商指定的字段 `<keyword>=<value>` 项。

KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_SUBNETMASK	SNM
KWD_PRIVELGE	PRV

Values

PRIVILEGE:
ADMIN
OPER
MONITOR

CALLBACKFLAGS

REQ	required callback
ROAM	roaming callback

TACACS+

认证

授权

PPP service=ppp protocol=ip
LOGIN service=shell cmd=null pri_lvl*0

Standard TACACS+ Attributes
service
protocol
cmd
addr
timeout
priv_lvl
callback-dialstring

IBM Specific Attributes

encryption_key	16 hex characters
dial_out	TRUE FALSE ONLY

记帐

task_id
start_time
stop_time
elasped_time
timezone
event
reason
bytes
bytes_in
bytes_out
paks
paks_in

paks_out
status
err_msg

缩写词表

ARP AppleTalk 地址识别协议

ABR 区域边界路由器

ack 确认

AIX 高级交互式执行操作系统

AMA MAC 随机寻址

AMP 当前的活动监视器

ANSI 美国国家标准学会

AP2 AppleTalk 可执行程序段 2

APPN 高级对等联网

ARE 全路由浏览器

ARI/FCI
地址识别指示符/帧复制指示符

ARP 地址识别协议

AS 独立系统

ASBR 独立系统边界路由器

ASCII 美国信息交换标准代码

ASN.1 抽象语法表示法 1

ASRT 自适应源路由透明选择

ASYNC
异步

ATCP AppleTalk 控制协议

ATP AppleTalk 事务处理协议

AUI 连接单元接口

ayt 您在吗

BAN 边界访问节点

BBCM 桥接广播管理器

BECN 反向拥塞显式通知

BGP 边界网关协议

BNC bayonet Niell-Concelman

BNCP 桥接网络控制协议

BOOTP
BOOT 协议

BPDU 桥接器协议数据单元

bps 位/秒

BR 桥接/路由

BRS 带宽保留

BSD Berkeley 软件发布

BTP BOOTP 中继代理

BTU 基本传输单元

CAM 相联存储器

CCITT 国际电报电话顾问委员会

CD 冲突检测

CGWCON
网关控制台

CIDR 无级别域间路由选择

CIP 传统 IP

CIR 信息提交率

CLNP 无连接模式网络协议

CPU 中央处理器

CRC 循环冗余校验

CRS 配置报告服务器

CTS 清除发送

CUD 调用用户数据

DAF 目的地地址过滤

DB 数据库

DBsum
数据库摘要

DCD 数据信道接受线路信号检测器

DCE 数据电路端接设备

DCS 直接连接的服务器

DDLC 双数据链路控制器

DDN 国防数据网

DDP 数据报传送协议

DDT 动态调试工具

DHCP 动态主机配置协议

dir 直接连接

DL 数据链路

DLC 数据链路控制

DLCI 数据链路连接标识符

DLS 数据链路交换

DLSw 数据链路交换

DMA 直接访问存储器

DNA 数字式网络体系结构

DNCP DECnet 协议控制协议

DNIC 数据网络标识符代码

DoD 国防部

DOS 磁盘操作系统

DR 指定的路由器

DRAM 动态随机存取内存

DSAP 目的地服务访问点

DSE 数据交换设备

DSE 数据交换机

DSR 数据集就绪

DSU 数据服务单元

DTE 数据终端设备

DTR 数据终端就绪

Dtype 目的地类型

DVMRP
远程向量多址发送路由选择协议

E1 2.048 Mbps 的传输速率

EDEL 终止定界符

EDI 出错指示符

EGP 外部网关协议

EIA 电子工业协会

ELAN 仿真 LAN

ELAP EtherTalk 链路访问协议

ELS 事件记录系统

ELSCon
次级 ELS 控制台

ESI 结尾系统定界符

EST 东部标准时间

Eth 以太网

fa-ga 功能地址-组地址

FCS 帧校验序列

FECN 前向转发拥塞显式通告

FIFO 先进先出

FLT 过滤程序库

FR 帧中继

FRL 帧中继

FTP 文件传输协议

GMT 格林威治标准时间

GOSIP
官方开放式系统互连概要

GTE 通用电话公司

GWCON
网关控制台

HDLC 高级数据链路控制协议

HEX 十六进制

HPR 高性能路由选择

HST TCP/IP 主机服务

HTF 主机表格格式

IBD 集成引导设备

ICMP Internet 报文控制协议

ICP Internet 控制协议

ID 标识

IDP 初始域部分

IDP Internet 数据报协议

IEEE 电气电子工程师协会

Ifc# 接口号

IGP 内部网关协议

InARP 反向地址识别协议

IP Internet 协议

IPCP IP 控制协议

IPPN IP 协议网络

IPX 网间包交换

IPXCP IPX 控制协议

ISDN 综合业务数字网

ISO 国际标准协会

Kbps 千比/秒

LAN 局域网

LAPB 平衡型链路接入协议

LAT 局域传送

LCS LAN 信道工作站

LCP 链路控制协议

LED 发光二极管

LF 最大帧; 换行

LIS 逻辑 IP 子网

LLC 逻辑链路控制

LLC2 逻辑链路控制 2

LMI 局部管理接口

LRM LAN 报表机制

LS 链路状态

LSA 链路状态通告

LSA 链路服务体系结构

LSB 最无关紧要的位

LSI LAN 快捷接口

LSreq 链路状态请求

LSrxl 链路状态再发送列表

LU 逻辑单元

MAC 介质访问控制

Mb 兆比特

MB 兆字节

Mbps 兆比特/秒

MBps 兆字节/秒

MC 多址发送

MCF MAC 过滤

MIB 管理信息库

MIB II 管理信息库 II

MILNET
军用网络

MOS Micro 操作系统

MOSDBG
Micro 操作系统调试工具

MOSPF
使用多址发送扩充设备时最短路径优先

MPC 多路径信道

MPC+ 高性能数据传送多路径 (HPDT) 信道

MSB 最重要的位

MSDU MAC 服务数据单元

MRU 最大接受单元

MTU 最大传送单元

nak 未确认

NAS Nways 交换管理站

NBMA 非广播多路访问

NBP 名字绑定协议

NBR 邻居

NCP 网络控制协议

NCP 网络核心协议

NDPS 非击穿路径交换

NetBIOS
网络基本输入输出系统

NHRP 下一驿站识别协议

NIST 国家标准与技术协会

NPDU 网络协议数据单元

NRZ 不归零

NRZI 不归零倒置

NSAP 网络服务访问点

NSF 国家科学基金会

NSFNET
国家科学基金会网络

NVCNFG
非易失配置

OPCON
操作员控制台

OSI 开放式系统互连

OSICP
OSI 控制协议

OSPF 最短路径优先(OSPF)

OUI 编制唯一标识符

PC 个人计算机

PCR 峰端单元速率

PDN 公用数据网

PING 报文包网间探索指令

PDU 协议数据单元

PID 进程标识

P-P 点到点

PPP 点对点协议

PROM 可编程只读存储器

PU 物理单元

PVC 永久虚拟电路

RAM 随机存取存储器

RD 路由描述符

REM 环错误监控器

REV 接收

RFC 请求说明

RI 环形指示器；路由选择信息

RIF 路由选择信息字段

RII 路由选择信息指示器

RIP 路由选择信息协议

RISC 精简指令集计算机

RNR 接收未就绪

ROM 只读存储器

ROpcon 远程操作员主控制台

RPS 环参数服务器

RTMP 路由选择表维护协议

RTP 路由选择更新协议

RTS 请求发送

Rtype 路由类型

rxmits 再传输

rxmt 再传输

s 二次

SAF 报源地址过滤

SAP 服务访问点

SAP 服务广告协议

SCR 持续的信元速率

SCSP 服务器高速缓冲存储器同步协议

sdel 起始定界符

SDLC SDLC 中继、同步数据链路控制

seqno 序列号

SGID 服务器组 id

SGMP 简单网关监视协议

SL 串行线路

SMP 当前的备用监视器

SMTP 简易邮件传输协议

SNA 系统网络体系结构

SNAP 子网访问协议

SNMP 简易网络管理协议

SNPA 子网连接点

SPF OSPF 区域内路由

SPE1 1OSPF 外部路由类型 1

SPE2 OSPF 外部路由类型 2

SPIA OSPF 区域间路由类型

SPID 服务概要 ID

SPX 编序包交换

SQE 信号品质错误

SRAM 静态随机存取内存

SRB 报源路由网桥

SRF 特别路由的帧

SRLY SDLC 中继

SRT 报源透明路由选择

SR-TB
报源透明路由网桥

STA 静态

STB 跨越树网桥

STE 跨越树浏览器

STP 屏蔽双绞线; 跨越树协议

SVC 交换虚拟电路

TB 透明桥接

TCN 拓扑结构变换通告

TCP 传输控制协议

TCP/IP
传输控制协议/Internet 协议

TEI 终端点标识符

TFTP 日常文件传输协议

TKR 令牌环

TMO 超时

TOS 服务类型

TSF 透明跨越帧

TTL 活动时间

TTY 电传打字机

TX 传送

UA 无序号的确认

UDP 用户数据报协议

UI 无序号的信息

UTP 无屏蔽双绞线

VCC 虚拟信道连接

VINES 虚拟联网系统

VIR 可变信息速率

VL 虚拟链路

VNI 虚拟网络接口

VR 虚拟路由

WAN 广域网

WRS WAN 恢复/重新路由

X.25 包交换网络

X.251 X.25 物理层

X.252 X.25 帧层

X.253 X.25 包层

XID 交换标识

XNS Xerox 网络系统

XSUM 校验和

ZIP AppleTalk 区域信息协议

ZIP2 AppleTalk 区域信息协议 2

ZIT 区域信息表

词汇表

本词汇表的词汇及定义来自:

- *American National Standard Dictionary for Information Systems* , ANSI X3.172-1990, copyright 1990, American National Standards Institute (ANSI)。其副本可向 American National Standards Institute, 11 West 42nd Street, New York, New York 10036 订购。其中的定义在本文档中以定义后面的符号 (A) 标识。
- ANSI/EIA Standard--440-A, *Fiber Optic Terminology*。其副本可向 Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006 订购。其中的定义在本文档中以定义后面的符号 (E) 标识。
- *Information Technology Vocabulary*, 由国际标准化组织和国际电工技术委员会 (ISO/IEC) 下设的 Joint Technical Committee 1 和 Subcommittee 1共同编写。在本文档中, 该词汇表的公开部分以定义后面的符号 (I) 标识; 而从 ISO/IEC JTC1/SC1 开发的国际标准草本、委员会草本和工作笔记中摘取的定义则以定义后面的符号 (T) 标识, 表明这些定义尚未获得 SCI 所有参与国家或地区的共同确认。
- *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*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines* , Carmel, Indiana: Que, 1992.

本词汇表采用了下列交叉引用:

对比: 此选项可使用户参考意义相反或明显不同的词汇。

同义词: 表明该词与词汇表中其它位置上定义的特定词汇具有相同的含义。

与...同义: 从已定义的词汇到所有含义相同词汇的逆向参考。

见: 引导读者参考以相同单词结尾的多词汇词组。

另见: 引导读者参考意义相关, 但并不相同的词汇。

A

abstract syntax (语法摘要). 一种数据规范。包括数据传送时需要的所有特征, 但忽略(抽取)其它细节, 如依赖于特定计算机体系结构的信息。另见 *abstract syntax notation 1 (ASN.1) (语法符号摘要 1)(ASN.1)* 和 *basic encoding rules (BER)(基本编码规则)(BER)*。

abstract syntax notation 1 (ASN.1)(语法符号摘要 1). 以下列标准指定的语法摘要的开放式系统互连 (OSI):

- ITU-T Recommendation X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994

另见 *basic encoding rules (BER) 基本编码规则*。

ACCESS. 在简单网络管理协议 (SNMP) 中, 管理信息库 (MIB) 模块中的一个子句。该子句定义了受管节点可以向对象提供的最小支持级别。

acknowledgment (确认). (1) 接收方将确认字符作为肯定响应回送给发送方的传送过程。 (T) (2) 表明已经接收到发送的对象。

active (激活). (1) 可操作。 (2) 节点或设备所处的一种状态。表明该节点或设备已经连接, 或者, 已经准备好与另一节点或设备进行连接。

active monitor (活动监控程序). 令牌环网络中, 某一特定环站可以执行的一种功能, 该环站应为最初传送令牌并提供令牌错误恢复帮助的环站。如果当前的活动监控程序出现故障, 则环上的任何活动的适配器均可代其提供活动监控程序功能。

address (地址). 数据通信中, 分配给与网络相连的各个设备、工作站或用户的唯一编码。

address mapping table (AMT)(地址映射表). AppleTalk 路由器中保存的一张表, 该表提供了节点地址到硬件地址的当前映射。

address mask (地址掩码). 在互连网子网中, 用以在 IP 地址的主机部分标识子网地址位的 32 位掩码。与 *subnet mask* 和 *subnetwork mask* 同义。

address resolution (地址转换). (1) 将网络层地址映射到介质专用地址的一种方法。 (2) 另见 *Address Resolution*

*Protocol (ARP)(地址转换协议)*和 *AppleTalk Address Resolution Protocol (AARP)(AppleTalk 地址转换协议)*。

Address Resolution Protocol (ARP)(地址转换协议). (1) 在 Internet 协议组中，用以将 IP 地址动态映射至网络所用地址的协议---- 该网络应支持全球区域或局部区域，如以太网或令牌环网。 (2) 另见 *Reverse Address Resolution Protocol (RARP)(反向地址转换协议)*。

addressing (寻址). 数据通信中，某一站点选择数据发送的目的地站点的方法。

adjacent nodes (相邻节点). 至少有一条路径相连的两个节点，并且，该路径(或所有路径)不与其它节点相连。 (T)

Administrative Domain (管理域). 由单独的管理权限管理的主机、路由器和互连的网络的集合。

Advanced Peer-to-Peer Networking (APPN)(高级对等联网). SNA 的一项扩展功能，其特点为: (a) 分布网络控制功能更为强大，能够避免严重的分层依赖性，进而隔离因单一点上的故障而造成的影响; (b) 动态交换网络拓扑信息，这使连接、再配置和适配路由选择更为方便快捷; (c) 网络资源的动态定义; (d) 自动资源注册和目录查找。APPN 将 LU 6.2 的最终用户服务对等定向扩展至网络控制，同时它还支持多个 LU 类型，其中包括 LU 2、 LU 3 和 LU 6.2。

Advanced Peer-to-Peer Networking (APPN) end node (高级对等联网终端节点). 提供大范围的最终用户服务，并且，支持其本地控制点 (CP) 和相邻网络节点 CP 间会话能力的节点。利用这些会话，该节点可以动态方式向相邻 CP (它的网络节点服务器)注册资源、接发搜索请求和获取管理服务。APPN 终端节点也可作为外围节点连至子区网络或连至其它终端节点。

Advanced Peer-to-Peer Networking (APPN)(高级对等联网网络). 互连的网络节点及其客户机终端节点的集合。

Advanced Peer-to-Peer Networking (APPN) network node (高级对等联网网络节点). 提供大范围的最终用户服务及以下服务的节点:

- 分布式目录服务，包括其域资源到中央目录服务器的注册
- 与其它 APPN 网络节点间进行拓扑结构数据库交换，支持网络中的所有节点在进行 LU-LU 会话时，以请求的服务类为基础，选择最佳路由。
- 本地 LU 和客户机终端节点的会话服务
- APPN 网络内的中间路由服务

Advanced Peer-to-Peer Networking (APPN) node (高级对等联网节点). APPN 网络节点或 APPN 终端节点。

agent (代理). 担任代理角色的系统。

alert (警告). 网络中发送到管理服务焦点的消息，用以表明出现了故障或可能出现的故障。

all-stations address (全站地址). 在网络通信中，是 *broadcast address (广播地址)*的同义词。

American National Standards Institute (ANSI)(美国国家标准协会). 由生产者、消费者和共同利益团体组成的组织，主要制定鉴定后的组织的创建手续，并维护美国国内的自主行业标准。 (A)

analog (模拟). (1) 通过物理量的连续变化实现数据传送的一种方式。 (A) (2) 对比: *digital (数字)*。

AppleTalk. Apple Computer, Inc.开发的一种网络协议。主要用于互连网络设备，但互连的设备既可以是 Apple 产品，也可以是非 Apple 产品。

AppleTalk Address Resolution Protocol (AARP)(AppleTalk 地址转换协议). AppleTalk 网络中的一种协议，可 (a) 将 AppleTalk 节点地址转换为硬件地址，并 (b) 消除支持多组协议的网络在寻址时的差异。

AppleTalk Transaction Protocol (ATP)(AppleTalk 事务处理协议). AppleTalk 网络中的一种协议，可为访问区域信息协议 (ZIP) 以获得区域信息的主机提供客户机/服务器请求和响应功能。

APPN network (APPN 网络). 见 *Advanced Peer-to-Peer Networking (APPN) network (高级对等联网网络)*。

APPN network node (APPN 网络节点). 见 *Advanced Peer-to-Peer Networking (APPN) network (高级对等联网网络节点)*,

arbitrary MAC addressing (AMA)(MAC 随机寻址). DECnet 结构中，由支持通用管理地址和局部管理地址的 DECnet Phase IV-Prime 使用的寻址方案。

area (区域). 在 Internet 和 DECnet 路由协议中，按网络管理员定义组合在一起的网络或网关子集。每个区域均为自包含类型，对于其它区域而言，该区域的拓扑结构为隐藏信息。

asynchronous (ASYNC)(异步). 不依特定事件，如公共计时信号，而存在的两个或两个以上的进程。 (T)

attachment unit interface (AUI)(连接设备接口). 局域网环境下，数据站内媒体连接设备和数据终端设备间的接口。 (I) (A)

authentication failure (认证失败). 简单网络管理协议 (SNMP) 中，当请求客户机为非 SNMP 团体成员时，认证实体可能创建的一种陷阱。

autonomous system (自主系统). TCP/IP 中，某一管理权限下的一组网络和路由器。这些网络和路由器彼此密切合作，并且使用它们的内部网关协议互相传播网络穿透性(和路由)信息。

autonomous system number (自主系统编号). 在 TCP/IP 中，由分配 IP 地址的中央授权系统分配给自主系统的号码。利用这一号码，自动路由算法可识别自主系统。

B

backbone (干线). (1) 局域网多桥环配置中的一种高速链路，网中的各个环可通过网桥或路由器与其连接。干线可配置为总线或环。 (2) 在广域网中，与节点或数据交换机(DSE)相连的一种高速链路。

backbone network (干线网络). 与小网络(通常速度较低)相连的一种中央网络。干线网络通常较其帮助连接的网络容量更大，或者，也可能是一个广域网(WAN)，如公用包交换数据报网络。

backbone router (干线路由器). (1) 用以在不同区域间传输数据的路由器。 (2) 系列路由器中的一个，用于将网络互联为更大的互连网。

Bandwidth (带宽). 光纤链路的带宽。用于确定链路的信息携带能力，并与光纤链路可以支持的最大位速相关。

basic transmission unit (BTU)(基本传输单元). 在 SNA 中，经过路径控制部件的数据单元和控制信息。一个 BTU 可以包含一个或多个路径信息单元 (PIU)。

baud (波特). 异步传输中的调制速率单位，与每秒单元间隔时间对应。也就是说，如果单元间隔时间为 20 毫秒，则其调制速率为 50 波特。 (A)

bootstrap (引导程序). (1) 一系列系统指令，其执行的结果是装入并执行附加指令，直至存储了所有的计算机程序。 (T) (2) 一种技术或设备。用于通过内部操作将其自身转入需要的状态。例如，一个机器例程，它的前几项指令即可以将其自身的其余部分从输入设备转入计算机内。(A)

Border Gateway Protocol (BGP)(边界网关协议). 一种 Internet 协议 (IP)。用于路由在域和自主系统间使用的协议。

border router (边界路由器). Internet 通信中的一种路由器。位于自主系统的一边，与其它自主系统边缘的另一路由器通信。

bridge (网桥). 互联多个 LAN (本地或远程)的一种功能部件。这些 LAN 必须使用统一的逻辑链路控制协议，但可以使用不同的介质访问控制协议。基于介质访问控制 (MAC) 地址，网桥可将帧转发到另一个网桥。

bridge identifier (网桥标识符). 跨越树协议中使用的一种 8 位字段。该字段内容由 MAC 端口地址、最低端口标识符和一个用户定义值组成。

bridging (桥接). 在 LAN 中，从一个 LAN 段至另一个 LAN 段的帧转发。其目的地由介质访问控制 (MAC) 子层地址指定，此地址编码在帧头部目的地地址字段内。

broadcast (广播). (1) 将相同数据传输到所有目的地。(T) (2) 同时将数据传输到一个以上的目的地。 (3) 对比: *multicast*。

broadcast address (广播地址). 通信中的一个保留的网站地址 (8 个 1)。它是链路上所有站点的共知地址。与 *all-stations address (全站地址)*同义。

C

cache (高速缓冲存储器). (1) 具有专门用途的一种缓冲存储器。与主存储器相比，该存储器容量小但速度快，主要用于存储指令副本及从主存储器获得，但马上即可能由处理器使用的数据。 (T) (2) 一种存储常用指令和数据的缓冲存储器，主要用于降低存取时间。 (3) 网络节点中目录数据库的任选部分。可用于存储常用目录信息以提高目录搜索速度。 (4) 在高速缓冲存储器中放置、隐藏或存储。

call request packet (呼叫请求包). (1) 数据终端设备 (DTE) 传输的一种呼叫管理包。用于请求在整个网络中建立呼叫连接。 (2) X.25 通信中的一种呼叫管理包。该包由 DTE 传输，用于请求在整个网络中建立呼叫连接。

canonical address (标准地址). LAN 中用于传输令牌环和以太网适配器介质访问控制 (MAC) 地址的 IEEE 802.1 格式。在标准格式中，每个地址字节的最无关紧要(最右边)的位首先传输。对比: *noncanonical address (非标准地址)*。

carrier (载波). 电波、磁波或脉冲序列的一种。经信号调制后，它们可以将信息携带传送过通信系统。 (T)

carrier detect (载波检测). 同义词: *received line signal detector (RLSD)(接收到的线路信号检测器)*.

carrier sense (载波监听). 局域网中数据站的一种持续进行的活动，用于监听是否有另一站点正在传输数据。 (T)

carrier sense multiple access with collision detection (CSMA/CD)(载波监听多路访问冲突检测). 要求载波监听的一种协议。在此协议下，数据站在传送的时候如果检测到了其它信号，则停止传送并发出干扰信号，然后，在重试发送前，它会等待一段时间，时间长短视情况而定。(T) (A)

CCITT. 国际电报电话咨询委员会。它是国际电信联盟 (ITU) 的一个组织。1993 年 3 月 1 日， ITU 进行了重组，重组后标准化任务由名为国际电信联盟远程通信标准化分部这样一个附属组织承担。重组前通过的推荐标准中，『CCITT』 一词仍在继续使用。

channel (信道). (1) 信号可以沿其发送的路径，如数据信道、输出信道。 (A) (2) 由处理器控制的功能部件。该部件可控制处理器存储设备和本地外围设备间的数据传送。

channel service unit (CSU)(信道服务部件). 为数字网络提供接口的一种部件。CSU 提供线路调整(或均衡)功能，该功能可使信号在通过信道带宽时保持性能稳定；另外，CSU 还提供信号整形功能，该功能可形成二进制脉冲流；除此之外，CSU 还提供了回送测试功能，其中包括 CSU 和网络载波的局信道部件间的测试信号传输。另见 *data service unit (DSU) (数据服务部件)*。

channelization (信道化). 将通信线路上的带宽划分为多个信道的过程，这些信道可以具有不同的大小。信道化也称为 ***time division multiplexing*** (TDM)(时分多路复用)。

checksum (校验和). (1) 一个数据组的数据总量。此数值与该组相关联并用于校验目的。 (T) (2) 在错误检测中，块中所有位的一种功能。如果写入的和与计算出来的和不一致，则表明出错。 (3) 为进行错误检测，在软盘上的某一扇区写入数据；如果计算得出的校验和与写入扇区的数据的校验和不匹配，则表明这是一个坏扇区。为计算校验和，此数据应是数字或可视为数字的其它字符串。

circuit switching (线路交换). (1) 一种进程。在收到请求的时候，该进程可连接两个或多个数据终端设备 (DTE)，并且，允许它们专用某一数据电路，直到连接释放为止。 (I) (A) (2) 与 *line switching (线路交换)*同义。

class A network (A 类网络). Internet 通信中的一种网络。在该网络中，IP 地址的高位(最重要)设为 0，而主机 ID 则占用其它三个低八位位组。

class B network (B 类网络). Internet 通信中的一种网络。在该网络中，IP 地址的两个高位(最重要位和次重要位)分别设为 1 和 0，而主机 ID 则占用其它两个低八位位组。

class of service (COS)(服务类型). 用以在会话方之间构建路由的一组参数(如路由安全、传输优先级和带宽)。服务类型是从会话启动程序指定的模式名称中产生出来的。

Client (客户机). (1) 从服务器接收共享服务的功能部件。 (T) (2) 用户。

client/server (客户机/服务器). 通信中分布式数据处理的一种交互作用模式。在这种模式下，一个站点的程序向另一站点发送请求并等待响应。请求程序称为客户机，应答程序称为服务器。

clocking (时钟同步). (1) 在二进制同步通信中，使用时钟脉冲控制数据同步和字符的一种方法。 (2) 控制给定时间内远程通信线路上可以发送的数据位位数的一种方法。

collision (冲突). 因在同一信道上同时进行多个传输而导致的不利状态。 (T)

collision detection (冲突检测). 在载波检测多路访问/冲突检测中，表明两个或多个站点正在同时传输的一种信号。

Committed information rate (信息提交速率). 网络可以发送的最大数据量(以位为单位)。

community (集合). 简单网络管理协议 (SNMP) 中实体间的管理关系。

community name (集合名称). 简单网络管理协议 (SNMP) 中标识集合的八位位组字符串。

compression (压缩). (1) 删除间隔、空字段、冗余数据以缩短记录或块长度的一种处理。 (2) 用以减少代表给定消息或记录的位的位数的任何编码操作。

configuration (配置). (1) 信息处理系统的硬件或软件的组织和互联方式。 (T) (2) 组成系统、子系统或网络的设备及程序。

configuration database (CDB)(配置数据库). 存储一个或多个设备配置参数的数据库。使用配置程序可构建并更新此数据库。

configuration file (配置文件). 指定系统设备或网络特性的一种文件。

configuration parameter (配置参数). 配置定义中的一种变量。其变量值可定义一个产品和同一网络中其它产品的关系特性，除此之外，它还可以定义产品本身的特性。

configuration report server (CRS)(配置报告服务器). IBM 令牌环网络桥接程序中的一种服务器。该服务器从 LAN 网络管理器 (LNM) 接收命令以获得站点信息、设定站点参数和从环上删除站点。另外，此服务器还负责收集和转发环上站点生成的配置报告。该配置报告包括新活动监视器报告和最邻近活动上游站 (NAUN) 报告。

congestion (拥塞). 见 *network congestion (网络拥塞)*。

connection (连接). 数据通信中用于传送信息的功能部件间建立的一种关联。(I) (A)

control point (CP)(控制点). (1) APPN 或 LEN 节点的一个组成部分，用于管理该节点的资源。在 APPN 节点中，CP 能够与其它 APPN 节点建立并保持 CP-CP 会话状态。在 APPN 网络节点中，CP 也能够向 APPN 网络中的相邻终端节点提供服务。 (2) 节点中的一个部件。主要用于管理该节点的资源，同时也可有选择性地向网络中的其它节点提供服务。具体实例如: 5 类子区节点中的系统服务控制点 (SSCP); APPN 网络节点中的网络节点控制点 (NNCP); APPN 或 LEN 终端节点中的终端节点控制点。其中，SSCP 和 NNCP 可以向其它节点提供服务。

control point management services (CPMS)(控制点管理服务). 控制点的一个组件，由管理服务功能集构成，可以帮助进行问题管理、性能和记帐管理、更改管理及配置管理。CPMS 提供如下功能: 向物理部件管理服务 (PUMS) 发送测试系统资源请求; 从 PUMS 收集系统资源的统计信息(如错误和性能数据); 分析并提交测试结果和收集到的系统资源统计信息。用于性能监控和确定故障原因的分析及提交任务可在多个 CPMS 中分布执行。

control point management services unit (CP-MSU)(控制点管理服务单元). 包含管理服务数据并在管理服务功能集间流动的消息单元。此消息单元采用通用数据流 (GDS) 格式。另见 *management services unit (MSU)(管理服务单元)* 和 *network management vector transport (NMVT)(网络管理向量传输)*。

D

D 位. 发送确认位。在 X.25 通信中，如果需要接收方进行端到端确认(发送确认)，则应将数据包或呼叫请求包中的某一位设为 1，这一位即称为 D 位。

daemon (守护程序). 在无人值守的情况下提供标准服务的一种程序。有些守护程序自动触发执行任务，而其它守护程序则定期执行操作。

data carrier detect (DCD)(数据载波检测). 同义词: *received line signal detector (RLSD)(接收到的线路信号检测器)*.

data circuit (数据电路). (1) 一对关联的传输和接收信道，提供了双工数据通信的方式。 (I) (2) 在 SNA 中，同义词为: *link connection (链路连接)*。 (3) 另见 *physical circuit (物理线路)*和 *virtual circuit (虚拟电路)*。

注:

1. 根据数据交换机处使用的接口类型的不同，数据交换机间的数据电路可以包括数据电路端接设备 (DCE)。
2. 在数据站和数据交换机或数据集中器之间，数据电路包括数据站端的数据电路端接设备，同时，在数据交换机或数据集中器位置，该线路也可以包括与 DCE 类似的设备。

data circuit-terminating equipment (DCE)(数据电路端接设备). 数据站中用于在数据终端设备 (DTE) 和线路间提供信号和代码转换的设备。 (I)

注:

1. DCE 既可以是单独的设备，也可以是 DTE 或中间设备的主要部分。
2. DCE 可以执行一些通常在线路网络终端执行的其它功能。

data link connection identifier (DLCI)(数据链路连接标识符). 帧中继网络中帧中继子端口或 PVC 段的数值标识符。帧中继端口的每个子端口都有一个唯一的 DLCI。下表是从美国国家标准协会 (ANSI) 标准 T1.618 和国际电报电话顾问委员会 (ITU-T/CCITT) 标准 Q.922 中摘取的，该表列出了与特定 DLCI 值关联的功能:

DLCI 值	功能
0	表示位于信道内
1-15	保留
16-991	指定使用帧中继连接过程
992-1007	帧中继载体服务 2 层管理
1008-1022	保留
1023	信道层管理

data link control (DLC)(数据链路控制). 数据链路(如 SDLC 链路或令牌环)上的节点用以完成信息顺序交换的一组规则。

data link control (DLC) layer (数据链路控制层). SNA 中由链路站组成的一层。调度数据在两个节点间的链路上传送并对此链路进行错误控制。具体实例如按位串行连接的 SDLC 和 System/370 信道的数据链路控制。

注: DLC 层通常独立于物理传送装置，可以确保数据到达高层时的完整性。

data link layer (数据链路层). 在开放式系统互连 (OSI) 参考模型中的一层，主要在网络层实体间通过通信链路提供数据传送服务。数据链路层检测并且可能校正物理层中出现的错误。 (T)

data link level (数据链路级别). (1) 在数据站分层结构中，高层逻辑和维护数据链路控制的数据链路间的控制概念级或处理逻辑概念级。数据链路级别执行如下功能: 插入传输位和删除接收位; 解析地址和控制字段; 生成、传输和解释命令及响应; 计算和解析帧校验序列。另见 *packet level (包级别)*和 *physical level (物理级别)*。 (2) 在 X.25 通信中，与*frame level (帧级别)*同义。

data link switching (DLSw)(数据链路转换). 使用 IEEE 802.2 逻辑链路控制 (LLC) 类型 2 的网络协议的一种传送方法。SNA 和 NetBIOS 便是使用 LLC 类型 2 的具体协议实例。另见 *encapsulation (封装)*和 *spoofing (欺骗)*。

data packet (数据包). X.25 通信中通过 DTE/DCE 接口处的虚电路传输用户数据的包。

data service unit (DSU)(数据服务设备). 直接向数据终端设备提供数字数据服务接口的一种设备。DSU 提供环路均衡、远程和本地测试功能及标准 EIA/CCITT 接口。

data set ready (DSR)(数据设备就绪). 同义词: *DCE ready (DCE 就绪)*。

data switching exchange (DSE)(数据交换机). 在某一单独位置安装的一种设备，主要提供交换功能，如电路转换、报文交换及包交换。 (I)

data terminal equipment (DTE)(数据终端设备). 数据站中的一部分，主要作为数据源、数据接收器提供服务，或者，同时作为以上两者提供服务。 (I) (A)

data terminal ready (DTR)(数据终端就绪). 发给使用 EIA 232 协议的调制解调器的一个信号。

data transfer rate (数据传送速率). 数据传输系统中，单位时间内在相应设备间通过的平均位数、字符数或块数。 (I)

注:

1. 此速率以每秒、每分或每小时的位数、字符数或块数表示。
2. 应指明相应的设备，如调制解调器、中间设备或数据源及数据接收器。

datagram (数据报). (1) 包交换中的一种自包含数据包。该包独立于其它数据包，它无需依靠 DTE 和网络间的早期交换便可以凭借自身携带的信息从源数据终端设备 (DTE) 路由至目标 DTE。 (I) (2) TCP/IP 中通过 Internet 环境传送的基本信息单元。数据报中除数据外，还包含源地址和目的地地址。Internet 协议 (IP) 数据报由 IP 头和其后的传输层数据组成。 (3) 另见 *packet (包)*和 *segment (分段)*。

Datagram Delivery Protocol (DDP)(数据报发送协议). AppleTalk 网络中的一种协议。该协议利用网络层上的无连接套接字对套接字发送服务提供网络连接。

DCE ready (DCE 就绪). EIA 232 标准中发给数据终端设备 (DTE) 上的一种信号。该信号表明本地数据电路端接设备 (DCE) 已与通信信道连接，并且已经准备好发送数据。与 *data set ready (DSR)(数据设备就绪)*同义。

DECnet. 定义软件、模块、数据库和硬件部件系列操作的网络体系结构。上述各项通常用于将 Digital Equipment Corporation 的各个系统连接起来以实现资源共享、分布式计算或远程系统配置。DECnet 网络实施方案采用数字网络体系结构 (DNA) 模式。

default (缺省). 一种属性、条件、值或选项。当未明确指定上述各项时，使用缺省设置。 (I)

dependent LU requester (DLUR)(关联 LU 请求程序). 一种 APPN 末端节点或网络节点。该节点拥有关联 LU，但需要关联 LU 服务器为那些关联 LU 提供 SSCP 服务。

designated router (指定的路由器). 将其它路由器的标识及存在情况报告给末端节点的一种路由器。所选的指定路由器应是具有最高优先级的路由器。当几个路由器共享最高优先级时，则选择具有最高站地址的路由器。

destination node (目的地节点). 请求或数据将要发送到的节点。

destination port (目的地端口). 8 端口异步适配器。主要作为与串行服务的连接点使用。

destination service access point (DSAP)(目的地服务访问点). SNA 和 TCP/IP 中的一个逻辑地址。该地址允许系统将数据从远程设备路由至适当的通信支持。对比 *source service access point (SSAP)(源服务访问点)*。

device (设备). 用于特定目的的机械、电子或电磁产品。

digital (数字式). (1) 指由数字组成的数据。 (T) (2) 指以数字形式出现的数据。 (A) (3) 与 *analog (模拟)*对比。

Digital Network Architecture (DNA)(数字网络体系结构). DECnet 所有硬件及软件实施方案的模型。

direct memory access (DMA)(直接存储器访问). 一种系统设施。此设施允许宏信道总线上的设备在没有系统处理器介入的情况下，直接存储系统或总线存储器。

directory (目录). 相应数据项的标识符及标记的表格。 (I) (A)

directory service (DS)(目录服务). 一种应用程序服务元素。它将应用进程使用的符号名转换为 OSI 环境下使用的完整的网络地址。 (T)

directory services (DS)(指导服务). APPN 节点的一种控制点部件。该部件用于维护网络资源位置信息。

disable (禁用). 禁止运行某一功能。

disabled (已禁用). (1) 正在执行处理的部件所处的一种状态。此状态可防止发生某些类型的中断。 (2) 传输控制部件或音频响应部件所处的一种状态。在这种状态下，上述两种部件无法接收在线入网呼叫。

domain (域). (1) 计算机网络的一部分。在这一部分，数据处理资源处于共同控制之下。 (T) (2) 开放式系统互连 (OSI) 中的一部分分布式系统或一组受管对象，这些系统或

对象使用共同的策略。 (3) 见 *Administrative Domain (管理域)*和 *domain name (域名)*。

domain name (域名). Internet 协议系列中的一个主机系统名。域名由以定界符分隔的一系列子名构成。例如，如果主机系统的全限定域名 (FPDN) 为 ralvm7.vnet.ibm.com，则列各项均为域名:

- ralvm7.vnet.ibm.com
- vnet.ibm.com
- ibm.com

domain name server (域名服务器). Internet 协议系列中的一个服务器程序。该程序通过将域名映射为 IP 地址的形式提供名称和地址间的转换。同义词: *name server (名称服务器)*。

Domain Name System (DNS)(域名系统). Internet 协议系列中的一种分布式数据库系统。该数据库用于将域名映射为 IP 地址。

dotted decimal notation (点分十进制表示法). 32 位整数的一种句法表示。这个 32 位整数由 4 个 8 位数字组成，以 10 进制为基准，并且中间以句点分隔。点分十进制用于表示 IP 地址。

dump (转储). (1) 已经转储的数据。 (T) (2) 为收集错误信息而复制虚拟存储器的全部或部分存储内容。

dynamic reconfiguration (DR)(动态重新配置). 更改网络配置(外围 PU 和 LU)的过程。这一过程无需重新创建完整的配置表和停用受影响的主节点。

Dynamic Routing (动态路由). 路由时使用的是学到的路径，而不是初始化时静态配置的路径。

E

echo (响应). 数据通信中通信信道上的一种反射信号。例如，在通信终端上，每个信号都显示两次: 一次是从本地终端进入时，另一次是从通信链路上返回时。这样便可以对信号的准确性进行检查。

EIA 232. 数据通信中电子工业协会 (EIA) 的一种标准。该标准定义了使用串行二进制数据互换的数据终端设备 (DTE) 和数据电路端接设备 (DCE) 间的接口规格。

Electronic Industries Association (EIA)(电子工业协会). 一个电子制造商组织。该组织主要致力于推动电子行业的技术发展，发表会员观点以及开发行业标准等。

EIA 单元. 一种计量单位。由电子工业协会建立，等于 44.45 毫米 (1.75 英寸)。

encapsulation (封装). (1) 通信中分层协议使用的一种技术。通过这种技术，一层将在其上一层传来的协议数据单元 (PDU) 中添加控制信息。 从这方面来讲，可以说是该层封装了来自其所支持的层的数据。例如，在 Internet 协议系列中，信息包中首先包含的是来自物理层的控制信息，然后是来自网络层的控制信息，这之后便是应用协议数据。 (2) 另见 *data link switching (数据链路交换)*。

encode (编码). 以某种方式将数据转换为代码，同时在需要时又可以将其还原为原始状态的。 (T)

end node (EN)(末端节点). (1) 见 *Advanced Peer-to-Peer Networking (APPN) end node (高级对等联网末端节点)*和 *low-entry networking (LEN) end node (低入口联网末端节点)*。 (2) 通信中的一种节点。该节点经常连与单独的数据链路，但不能执行中间路由功能。

entry point (EP)(入口点). SNA 中提供分布式网络管理支持的 2.0 型、2.1 型、4 型或 5 型节点。这些节点将自身及其控制的资源的网络管理数据发送到焦点进行集中式处理，并且，接收执行焦点启动的命令以管理和控制其资源。

Ethernet (以太网). 一种 10-Mbps 的基带局域网。该网络允许多个站点在不进行事先协商的情况下，按自己的意愿访问传输介质。同时，该网络还采用载波监听和延迟措施避免争用，以及一旦发生时使用冲突检测和延迟再传输方式解决争用。Ethernet 使用载波检测多路访问/冲突检测。

exception (异常). 一种非正常状态。如在处理数据集或文件时遇到 I/O 错误。

exception response (ER)(异常响应). SNA 中的一个协议，需要在请求头部的“要求的响应形式”字段中填写。该协议可指示接收程序仅在请求无法接受或无法处理时返回响应；也就是说，可以返回否定响应，而不是肯定响应。对比: *definite response (明确响应)*和 *no response (无响应)*。

exchange identification (XID)(交换标识). 基本链路单元的一种特定类型。该单元用于在相邻节点间传送节点和链路特性信息。链路激活前和激活期间，XID 在链路站间交换可建立并协商链路和节点特性；链路激活后，XID 交换可传达链路站特性的更改。

explicit route (ER)(显式路由). SNA 中连接两个子区节点的一个或多个传输组系列。显式路由由原始子区地址、目的地子区地址、显式路由号和反向显式路由号标识。对比: *virtual route (VR)(虚拟路由)*。

explorer frame (探测帧). 见 *explorer packet (探测包)*。

explorer packet (探测包). LAN 间的一种包。该包由源主机生成，跨越 LAN 的整个源路由部分并收集主机的可能路径信息。

exterior gateway (外部网关). Internet 通信中自主系统上的一种网关。主要用于实现该系统与另一自主系统的通信。对比: *interior gateway (内部网关)*。

Exterior Gateway Protocol (EGP)(外部网关协议). Internet 协议系列中用于域和自主系统间的一种协议。该协议可使网络可到达性信息得以通知和交换。利用 EGP 参与路由器，一个自主系统中的 IP 网络地址可传达到另一自主系统。具体 EGP 实例如边界网关协议 (BGP)。对比: Interior Gateway Protocol (IGP)(内部网关协议)。

F

fax (传真). 从传真机收到的复印件。与 ***telecopy (远程复制)***同义。

File Transfer Protocol (FTP)(文件传送协议). Internet 协议系列中的一个应用层协议。该协议使用 TCP 和 Telnet 服务在机器或主机间传送成批数据。

flash memory (闪速存储器). 一种可编程、可擦除但并不需要不间断电源的数据存储设备。闪速存储器较其它可编程、可擦除的数据存储设备而言，其最大优点在于无需从电路板上拆除即可重新编程。

flow control (流控制). (1) SNA 中管理数据信息在网络部件间流通速率的过程。流控制的目的在于最大可能地提高报文单元的流通速率并使网络拥塞概率降至最低。也就是说，既不使接收端或中间路由节点的缓冲区溢出，也不让接收端等待报文单元。 (2) 另见 *pacing (定步)*。

fragment (段). 见 *fragmentation (分段)*。

fragmentation (分段). (1) 将数据报分成一个个小部分或段，以使其与传送它的物理介质传送能力相匹配的过程。(2) 另见 *segmenting (划分数据段)*。

frame (帧). (1) 开放式系统互连体系结构中的一种数据结构。此数据结构与特定的知识区域相关联，并由可接受指定属性值的多个时隙组成，相应的过程附件可从这些时隙推出信息。 (T) (2) 包括 IBM 令牌环网在内的某些局域网的传输单元。它包括定界符、控制字符、信息和检验字符。 (3) SDLC 中所有命令、响应和使用 SDLC 过程传输的信息的运送工具。

frame level (帧级). 与 *data link level (数据链路级别)*同义。见 *link level (链路级别)*。

frame relay (帧中继). (1) 一种接口标准。此标准描述了用户设备和快速分组网络间的边界。在帧中继系统中，缺陷帧将丢弃；而恢复过程则采用端到端形式，而不是驿站到驿站的形式。 (2) 从综合业务数字网 (ISDN) D 信道标准衍生而来的技术。此技术假定连接可靠，并且在网络中执行错误的检测与控制。

front-end processor (前端处理器). 如 IBM 3745 或 3174 之类的一种处理器，此处理器替主机承担了通信控制任务。

G

gateway (网关). (1) 一种功能部件，能够连接体系结构不同的两个计算机网络。网关主要用于连接体系结构不同的网络或系统。而网桥则用于互连体系结构相似或相同的网络或系统。 (T) (2) IBM 令牌环网内的一种设备及其关联软件。主要用于连接使用不同逻辑链路协议的局域网或局域网和主机。 (3) 在 TCP/IP 中，与 *router (路由器)*同义。

general data stream (GDS)(通用数据流). LU 6.2 会话中用于对话的数据流。

general data stream (GDS) variable (通用数据流变量). RU 子结构中的一种类型。其前面是标识符和长度字段，其内容包括请求数据、用户控制数据或 SNA 定义的控制数据。

H

header (头部). (1) 用户数据前的系统定义的控制信息。(2) 报文的一部分。其中包含报文的控制信息，如一个或多个目的地字段、源站名、输入序列号、指明报文类型的字符串和报文优先级等。

heap memory (堆内存). 用于动态分配数据结构的 RAM 总量。

Hello. 由一组彼此合作、彼此信任的路由器使用的协议。这些路由器使用该协议可查找最小延迟路由。

hello message (hello 协议报文). (1) 一种定期发送的报文。用于建立和检测路由器之间或路由器和主机之间的可到达性。 (2) Internet 协议系列中的一种报文。该报文由 Hello 协议定义为内部网关协议 (IGP)。

heuristic (探试法). 与问题解答探测法相关的一种方法。此方法通过验证趋向最终结果的进程来查找问题解决方案。

high-level data link control (HDLC)(高级数据链路控制). 数据通信中以指定的位系列控制数据链路的一种方法。使用的位系列符合 HDLC 国际标准: ISO 3309 Frame Structure 和 ISO 4335 Elements of Procedures。

high-performance routing (HPR)(高性能路由选择). 高级对等联网 (APPN) 体系结构的一个附加组成部分。此部分增强了数据路由选择性能和可到达性，特别是使用高速链路时，其增强效果更为明显。

hop (驿站). (1) APPN 中某一路由的一部分，此部分没有中间节点。这一部分只有与相邻节点连接的一个单独的传输组。 (2) 对于路由层而言，是网络中两个节点的逻辑距离。

hop count (跳跃计数). (1) 两点间的量度或测量距离。(2) 在 Internet 通信中，指的是数据报抵达目的地前经由的路由器数。 (3) 在 SNA 中，对经沿某一路径到达目的地前需要跨越的链路数目进行的计量。

host (主机). Internet 协议系列中的一个末端系统。此末端系统可以是任何一个工作站，而不一定必须是大型主机。

hub (intelligent)(集线器(智能)). 一种连线集中器，如 IBM 8260。集线器可在使用不同电缆和不同协议的 LAN 之间提供桥接和路由功能。

hysteresis (滞后). 报警临界值设置后，报警条件清除前必须调整的温度额度。

I

I-frame (I 帧). 信息帧。

information (I) frame (信息 (I) 帧). 一种 I 格式帧。主要用于传送已编号信息。

input/output channel (输入/输出信道). 数据处理系统中的一种功能部件。主要负责在内部设备和外部设备间传送数据。 (I) (A)

Integrated Digital Network Exchange (IDNX)(综合数字网交换机). 用于集成声音、数据和图像应用的一种处理器。除此之外，该处理器也负责管理传输资源、连接多路复用器和网络管理支持系统。IDNX 可以接受不同供应商的设备集成。

integrated services digital network (ISDN)(综合业务数字网). 一种端到端数字远程通信网络。此网络支持多种服务，其中包括(但不限于)声音和数据。

注: ISDN 用于分共和专用网络体系结构中。

interface (接口). (1) 两个功能部件间的共享边界。根据需要，该边界由功能特性、信号特性或其它特性定义。此概念包含具有不同功能的两个设备的连接说明。 (T) (2) 链接系统、程序或设备的硬件、软件或硬软件。

interior gateway (内部网关). Internet 通信中仅与自身自主系统联系的网关。对比: *exterior gateway (外部网关)*。

Interior Gateway Protocol (IGP)(内部网关协议). Internet 协议系列中的一个。用于在自主系统中广播网络可到达性和路由信息。IGP 实例如路由信息协议 (RIP) 和最短路径优先 (OSPF)。

intermediate node (中间节点). 位于一个以上支线末端的节点。 (T)

intermediate session routing (ISR)(中间会话路由选择). APPN 网络节点中的一种路由功能类型。此类型路由为所有经过该节点，但其结束点在其它位置的会话提供会话级流控制和中断报告。

International Organization for Standardization (ISO)(国际标准化组织). 由来自不同国家的国家标准团体建立起来一个组织。其主旨在于推动标准研究，促进国际货物与服务交换和推进各国在知识、科学技术和经济领域的合作。

International Telecommunication Union (ITU)(国际电信联盟). 联合国下属的专业电信机构。主要提供标准化通信程序和相关常规工作，其中包括全球范围的频率分配和无线电规程。

internet (互连网). 由多个路由器互联的一组网络。通过路由器，这些网络可作为一个单独的大网络运行。另见 *Internet*。

Internet. 由 Internet 体系结构委员会 (IAB) 管理的互连网。它由世界各地的较大的国家主干网和许多地区网及校园网组成。Internet 使用 Internet 协议系列。

Internet address (Internet 地址). 见 *IP address (IP 地址)*。

Internet Architecture Board (IAB)(Internet 体系结构委员会). 负责监管 Internet 协议系列 (通常称为 TCP/IP) 开发的技术组织。

Internet Control Message Protocol (ICMP)(网际控制报文协议. 用于在 Internet 协议 (IP) 层处理错误和控制报文的一种协议。问题报告和错误的数据报目的地将返回原始数据报源。ICMP 也是 Internet 协议的一部分。

Internet Control Protocol (ICP)(Internet 控制协议). 提供异常通告、量度通告和 PING 支持的虚拟联网系统 (VINES) 协议。另见 *RouTing update Protocol (RTP)(路由更新协议)*。

Internet Engineering Task Force (IETF)(Internet 工程任务部). Internet 结构委员会 (IAB) 的任务部门。主要负责解决 Internet 的短期工程需要。

Internetwork Packet Exchange (IPX)(网际分组交换协议). (1) 一种网络协议。主要用于将 Novell 服务器或其它适用于 IPX 的工作站或路由器连至其它工作站。尽管此协议与 Internet 协议 (IP) 十分相似，但 IPX 使用不同的包格式和术语。 (2) 另见 *Xerox Network Systems (XNS)(施乐网络系统)*。

Internet Protocol (IP)(Internet 协议). 将数据路由过网络或互联网络的一种无连接协议。在高级协议层和物理网络间，IP 作为一种中介起作用。然而，此协议不能提供错误恢复和流控制，也不能确保物理网络的可靠性。

interoperability (互操作性). 用户无须清楚各种功能部件的重要特性便可以在其间通信、执行程序或传送数据的能力。 (T)

intra-area routing (域内路由选择). Internet 通信中某一区域的数据路由选择。

Inverse Address Resolution Protocol (InARP)(反向地址转换协议). Internet 协议系列中的一种。主要作用是通过已知硬件地址查找协议地址。在帧中继上下文中，数据链路连接标识符 (DLCI) 与已知硬件地址同义。

IPPN. 一种接口。其它协议可利用此接口通过 IP 传送数据。

IP address (IP 地址). 由 Internet 协议，标准 5，请求注释 (RFC) 791 定义的 32 位地址。该地址通常以点分十进制方法表示。

IP datagram (IP 数据报). 在 Internet 协议系列中，通过互连网传输的信息的基本单位。其中包含源和目的地地址、用户数据以及其它一此控制信息，如数据报长度、首部校验和用以表明数据报能否分段或是否已经分段的标识。

IP router (IP 路由器). IP 互连网中的一种设备。主要负责确定网络通信流经的路径。这里，路由协议用以获取网络信息并确定最佳路由。确定后，数据报便将按此路由转发，直至抵达最后目的地。数据报以 IP 目的地地址为基础进行路由。

IPXWAN. 一种 Novell 协议。主要用于在交换标准互联网分组交换 (IPX) 路由选择信息前交换路由器对路由器信息并通过广域网 (WAN) 传输数据。

J

jitter (跳动). (1) 数字信号的有效时间距其理想时间位置的短期非积累偏离。 (2) 已传送数字信号的不合要求的偏离。 (3) 网络延迟偏离。

L

LAN bridge server (LBS)(LAN 桥接服务器). IBM 令牌环网络桥接程序中的一种服务器。此服务器主要用于保存两个或多个环之间转发的帧(通过网桥)的统计信息。LBS 通过 LAN 报告装置将这些统计信息发送到适当的 LAN 管理器。

LAN Network Manager (LNM)(LAN 网络管理器). 一种 IBM 授权的程序。主要用于支持用户从中央工作站管理并监视 LAN 资源。

LAN segment (LAN 段). (1) LAN 的一部分(如总线或环)。此部分能够独立操作，但需要通过网桥与网络其它部分相连。 (2) 没有网桥的环或总线网络。

layer (层). (1) 网络体系结构中的一组服务。从概念的角度来看是完整的，它只是按分层排列的多个组中的一个。另外，它还扩展到遵循网络体系结构的所有系统。 (T) (2) 在开放式系统互连 (OSI) 参考模型中，是七个从概念角度考虑十分完整，但又按分层形式安排的服务组、功能组和协议组中的一个。此概念适用于所有的开放式系统。 (T) (3) SNA 中的一个相关功能组。从逻辑上来讲，该组中的功能分离于其它组中的功能。因此，更改某一层中的功能实施状态时，不会影响其它层中的功能。

line switching (线路交换). 与 *circuit switching (线路交换)*同义。

link (链路). 链路连接(传输介质)和两个链路站的组合。这两个链路站分别位于链路连接两端。在多点或令牌环配置中，链路连接可以在多个链路中共享。

link access protocol balanced (LAPB)(均衡式链路访问协议）. 用于以链路级访问 X.25 网络的一种协议。LAPB 是一种双工、异步、对称协议，主要用于点对点通信。

link-attached (链路连接设备). (1) 通过数据链路连与控制部件的设备。 (2) 对比: *channel-attached (信道连接设备)*。 (3) 与 *remote (远程)*同义。

link connection (链路连接). (1) 一种物理设备。主要在一个链路站和另一个或多个链路站之间提供双向通信。具体实例如远程通信线路和数据电路端接设备 (DCE)。 (2) 在 SNA 中，与 *data circuit (数据电路)*同义。

link level (链路级别). (1) Recommendation X.25 的一部分。定义了经由全双工链路从网络中取出或输入数据时使用的链路协议，但此全双工链路应为将用户机器连与网络节点的链路。 LAP 和 LAPB 是由 CCITT 介绍的链路访问协议。 (2) 见 *data link level (数据链路级别)*。

link-state (链路状态). 路由协议中的一中广播信息。主要介绍路由器或网络中的可用接口及可到达邻居。此协议的拓扑数据库是由收集到的链路状态广播内容形成的。

link station (链路站). (1) 某一节点中的硬件或软件部件，此节点代表通过特定链路与相邻节点的连接。例如，如果节点 A 是连与三个相邻节点多点线路的主末端，则节点 A 有三个代表与相邻节点连接的链路站。 (2) 另见 *adjacent link station (ALS)(邻接链路站)*。

local (本地设备). (1) 无需使用远程通信线路即可直接访问的设备。 (2) 对比: *remote (远程)*。 (3) 同义词: *channel-attached (信道连接设备)*。

local area network (LAN)(局域网). (1) 在一定的地理区域内，以用户为前提建立起来的计算机网络。局域网的内部通信可以不依外部规则，但是，跨越 LAN 边界的通信可能会受某种形式规章的限制。 (T) (2) 一种网络，其中一系列设备相互连接进行通信，并能够连接到较大的网络。 (3) 另见 *Ethernet (以太网)*和 *token ring (令牌环)*。 (4) 对比: *metropolitan area network (MAN)(城域网)* 和 *wide area network (WAN)(广域网)*。

local bridging (本地桥接). 桥接程序的一种功能。此功能允许单独的网桥在不使用远程通信链路的情况下，连接多个 LAN 段。对比: *remote bridging (远程桥接)*。

local management interface (LMI)(本地管理接口). 见 *local management interface (LMI) protocol (本地管理接口协议)*。

local management interface (LMI) protocol (本地管理接口协议). NCP 中的一组帧中继网络管理程序和消息。相邻帧中继节点使用这些程序和消息通过 DLCI X'00' 交换线路状态信息。NCP 同时支持 LMI 协议的美国国家标准协会 (ANSI) 和国际电信咨询委员会 (ITU-T/CCITT) 两种版本。在这些标准中，LMI 协议称为*链路完整性验证测试 (LIVT)*。

locally administered address (局部管理地址). 局域网中的一种适配器地址。此地址经分配后可优先于通用管理地址。对比: *universally administered address (通用管理地址)*。

logical channel (逻辑信道). 分组方式运行中的发送信道和接收信道。这两个信道共同用于通过数据链路同时发送和接收数据。通过交叉传送包可在同一个数据链路上建立几个逻辑信道。

logical link (逻辑链路). 一对链路站，两个相邻节点每边一个。其基本链路连接可在两个节点间提供单一的链路层连接。多个逻辑链路在共享连接两个节点的相同物理介质时可以彼此区别。具体实例如局域网 (LAN) 设施上的 802.2 逻辑链路和两个节点间相同点到点物理链路上的 LAP E 逻辑链路。逻辑链路一词还包括多个 X.25 逻辑信道，这些信道共享从 DTE 到 X.25 网络的访问链路。

logical link control (LLC)(逻辑链路控制). 数据链路控制 (DLC) LAN 子层。该层为信息顺序交换提供了两种类型的 DLC 操作。第一种类型是无连接服务，此服务允许在未建立链路的情况下发送和接收信息。对于无连接服务，LLC 子层不执行错误恢复和流控制。第二种类型是面向连接的服务，这种服务要求在交换信息前建立链路。面向连接的服务提供编序信息传送、流控制和错误恢复。

logical link control (LLC) protocol (逻辑链路控制协议). 局域网中的一种协议。该协议独立控制数据站间的传输帧交换，而不计传输介质的共享情况。 (T) LLC 协议由 IEEE 802 委员会开发，并且在所有的 LAN 标准中经常使用。

logical link control (LLC) protocol data unit (逻辑链路控制协议数据单元). 在不同节点的链路站间交换的一种信息单位。LLC 协议数据单元包含目的地服务访问点 (DSAP)、源服务存取点 (SSAP)、控制字段和用户数据。

logical unit (LU)(逻辑单元). 一种网络可存取单元。使用此单元用户可访问网络资源并实现彼此通信。

loopback test (回送测试). 一种测试。在这种测试中，发自测试器的信号在调制解调器或其它网络元素处循环返回该测试器。此信号携带的信息可用于确定或验证通信路径的质量。

low-entry networking (LEN)(低入口联网). 节点使用基本对等网络协议实现彼此直接连接的一种功能。这些节点在连接后可支持逻辑部件间的多个并行会话。

low-entry networking (LEN) end node (低入口联网末端节点). 从相邻 APPN 网络节点接收网络服务的一种 LEN 节点。

low-entry networking (LEN) node (低入口联网节点). 提供多种最终用户服务的一种节点。该节点使用对等协议直接连与其它节点连接，并从相邻 APPN 网络节点隐式衍生网络服务，也就是说，不直接使用 CP-CP 会话而创建服务。

M

Management Information Base (MIB)(管理信息库). (1) 一组可通过网络管理协议访问的对象集合。 (2) 管理信息的一种定义。此信息指定了可从主机或网关获得且得到操作允许的信息。 (3) OSI 中某一开放系统内管理信息的概念储存库。

management station (管理工作站). Internet 通信中负责管理全部或部分网络的系统。管理工作站使用网络管理协议，如简单网络管理协议 (SNMP)，与受管节点内的网络管理代理联系。

mapping (映射). 一种数据转换过程。其内容是将用户以一种格式传输的数据转换为接收方可以接受的数据格式。

mask (掩码). (1) 一种字符模式。此模式可用于控制保留或删除另一种字符模式部分。 (I) (A) (2) 使用一种字符模式控制另一种字符模式部分的保留或删除。 (I) (A)

maximum transmission unit (MTU)(最大传输单位). 在 LAN 中传输数据时，给定物理介质上的一个帧内可以发送的最大数据单位。例如，以太网的 MTU 为 1500 字节。

medium access control (MAC)(介质访问控制). LAN 中数据链路控制层的一个子层。该子层支持介质依赖功能，并且，使用物理层的服务为逻辑链路控制 (LLC) 子层提供服务。MAC 子层包括设备何时可以使用传输介质的判断方法。

medium access control (MAC) protocol (介质访问控制协议). 局域网中的一种协议。此协议控制传输介质访问，具体运作时它也将网络的拓扑结构因素考虑在内，这样便可以支持数据站间的数据交换。 (T)

medium access control (MAC) sublayer (介质访问控制子层). 局域网中应用介质访问方法的数据链路层部分。MAC 子层支持拓扑结构依赖功能，并且，使用物理层的服务为逻辑链路控制子层提供服务。 (T)

metric (量度). Internet 通信中与路由关联的一个值。该值用于鉴别同一自主系统中的多个出口或入口点。具有最低量度值的路由优先选择。

metropolitan area network (MAN)(城域网). 由两个或多个网络互联形成的一个大网络。此网络较其组成网络速度更快，并且可以跨越管理边界和使用多种访问方法。 (T) 对比: *local area network (LAN)(局域网)*和 *wide area network (WAN)(广域网)*。

MIB. (1) MIB 模块。 (2) 管理信息库。

MIB object (MIB 对象). 同义词: *MIB variable (MIB 变量)*。

MIB variable (MIB 变量). 简单网络管理协议 (SNMP) 中 MIB 模块内定义的特定数据实例。与 *MIB object (MIB 对象)*同义。

MIB view (MIB 视图). 简单网络管理协议 (SNMP) 中的一组受管对象集合。这些对象为代理周知对象，可供某一特定群体查看。

MILNET. 军用网络。此网络原是 ARPANET 的一部分，在 1984 年从 ARPANET 中分出。 MILNET 为军用安装提供可靠的网络服务。

modem (modulator/demodulator)(调制解调器). (1) 用于调制和解调信号的一种功能部件。其功能之一是支持数字数据通过模拟传输设施进行传送。 (T) (A) (2) 将计算机的数字数据转换为可在远程通信线路上传送的模拟信号的一种设备。另外，该设备在接收时还可将接收到的模拟信息转换为计算机数据。

module (组件). Nways 交换机中的一种打包的功能硬件设备。其中包括逻辑卡、连接头和指示灯。组件可用于打包适配器、线路接口耦合器、话音服务扩充设备和其它部件。逻辑辅助支架中的所有组件均可***热插拔***。

modulo (模). (1) 模数的一个相关部分。例如，9 以 5 为模等于 4。 (2) 另见 *modulus (模数)*。

modulus (模数). 一个数值，如正整数。此数值将两个相关数值间的差值分成两个值而不留任何余数。例如，9 和 4 共有一个模数 5 (9 - 4 = 5; 4 - 9 = -5; 值 5 分成了 5 和 -5 且不带任何余数)。

monitor (监视器). (1) 用于观查和记录数据处理系统中的选定活动以供分析的一种设备。可能的使用内容如指明与正常状态的显著偏离，或者是确定特定功能部件的利用程度。 (T) (2) 用于观查、监管、控制或验证系统操作的软件或硬件。 (A) (3) 一种功能。在环网上启动令牌传输以及在丢失令牌、循环帧或遇到其它困难时需要使用此功能。该功能存在于所有的环形网站上。

multicast (多址发送). (1) 将相同数据传输到一组选定的目的地的过程。 (T) (2) 广播的一种特殊方式。在这种方式下，包的副本仅分送到所有可能目的地的子集。

multipath channel (MPC)(多路信道). 一种信道协议。此协议将多个单向子信道用于 VTAM-to-VTAM 双向通信。

multiple-domain support (MDS)(多域支持). 一种通过 LU-LU 和 CP-CP 会话在管理服务功能设置间运输管理服务数据的技术。另见 *multiple-domain support message unit (MDS-MU)(多域支持报文单元)*.

multiple-domain support message unit (MDS-MU)(多域支持报文单元). 包含管理服务数据单元的一种报文单元。此单元通过由多域支持使用的 LU-LU 和 CP-CP 会话在管理服务功能设置间流通。此报文单元和其中包含的实际管理服务数据采用通用数据流 (GDS) 格式。另见 *control point management services unit (CP-MSU)(控制点管理服务单元)*、 *management services unit (MSU)(管理服务单元)* 和 *network management vector transport (NMVT)(网络管理向量传输)*。

N

Name Binding Protocol (NBP)(名称绑定协议). AppleTalk 网络中的一种协议。此协议在传输层提供从 AppleTalk 实体(资源)名(字符串)到 AppleTalk IP 地址 (16 位编号)的转换。

name resolution (名称转换). Internet 通信中将机器名映射为相应的 Internet 协议 (IP) 地址的过程。另见 *Domain Name System (DNS)(域名系统)*。

name server (名称服务器). 在 Internet 协议系列中，与 *domain name server (域名服务器)*同义。

nearest active upstream neighbor (NAUN)(最近活动上流站). 在 IBM 令牌环网络中，将数据直接发送到环上给定网站的工作站。

neighbor (邻居). 公共子网上的一种路由器。网络管理员已将其功能专设为接收路由信息。

NetBIOS. 网络基本输入/输出系统。网络、IBM 个人计算机 (PC) 和兼容 PC 机的标准接口，在 LAN 上使用时，主要提供分组、打印服务器和文件服务器功能。使用 NetBIOS 的应用程序不需要处理 LAN 数据链路控制 (DLC) 协议的详细内容。

network (网络). (1) 以某种配置方式连接起来的、可以提供信息交换的一组数据处理设备和软件。 (2) 一组节点和将其互连的链路。

Network Access Server (NAS)(网络访问服务器). 向用户提供临时请求式网络访问服务的一种设备。这种访问是使用 PSTN 或 ISDN 的点到点形式。

network accessible unit (NAU)(网络可访问单元). 一种逻辑单元 (LU)、物理单元 (PU)、控制点 (CP) 或系统服务控制点 (SSCP)。它是由路径控制网传输的信息的源和目的地。同义词: *network addressable unit (网络地址单元)*。

network address (网络地址). 按 ISO 7498-3 规定，网络地址是 OSI 环境中的一种无歧义名称，主要用于标识一系列网络服务访问点。

network addressable unit (NAU)(网络可寻址单元). 同义词: *network accessible unit*。

network architecture (网络体系结构). 计算机网络的逻辑结构和操作原则。 (T)

注: 网络操作原则包括服务、功能和协议原则。

network congestion (网络拥塞). 因通信量超过网络处理能力而产生的不希望的过载状态。

network identifier (网络标识符). (1) 在 TCP/IP 中，是定义网络的 IP 地址部分。网络 ID 长度取决于网络级别类型 (A、B、C、D)。 (2) 标识特定子网的唯一 1-8 字节客户选定名或 8 字节 IBM 注册名。

Network Information Center (NIC)(网络信息中心). Internet 通信中遍布全球的本地、地区和国家组织。这些组织向用户提供支持、培训和其它服务。

network layer (网络层). 开放式系统互连 (OSI) 结构中的一个层次。主要负责 OSI 环境中的路由选择、交换及链路层访问。

network management (网络管理). 面向通信的数据处理或信息系统的计划、组织和控制过程。

network management station (网络管理工作站). 简单网络管理协议 (SNMP) 中的一种工作站。主要负责执行监视和控制网络元素的管理应用程序。

network management vector transport (NMVT)(网络管理向量传输). 一种管理服务请求/响应单元 (RU)。此单元主要在物理单元管理服务和控制点管理服务间的活动会话中使用 (SSCP-PU 会话)。

network manager (网络管理程序). 用于监视、管理和诊断网络问题的一个程序或一组程序。

network node (NN)(网络节点). 见 *Advanced Peer-to-Peer Networking (APPN) network (高级对等联网网络节点)*,

network support station (网络支持工作站). 用于本地运行和服务 Nways 交换机的处理器。此处理器由 Nways 交换机管理员或服务人员使用。

network user address (NUA)(网络用户地址). X.25 通信中最多可包含 15 个二进制代码位的 X.121 地址。

node (节点). (1) 网络中的一个点。在此点上，信道和数据电路由一个或多个功能部件连接。 (I) (2) 任何连于网络的数据传输和接收设备。

noncanonical address (非标准地址). LAN 中用于传输令牌环适配器的介质访问控制 (MAC) 地址的格式。在非标准格式中，每个地址字节的最重要(最左边)的位首先传输。对比: *canonical address (标准地址)*。

Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1)(不归零按“1”变化记录). 一种记录方式。在这种记录方式下，磁化状态改变代表“1”，不改变代表“0”。其中只有“1”类信号明确记录。(以前称为***不归零翻转*** (NRZI) 记录法。)

nonseed router (非种子路由器). AppleTalk 网络中的一种路由器。此路由器需要从连于相同网络的种子路由器获得网络编号范围和区域列表信息。

Nways Switch (Nways 交换机). 与 IBM 2220 Nways 宽带交换机同义。

Nways Switch configuration station (Nways 交换机配置站). 运行 Nways 交换机配置工具 (NCT) 独立版本的专用 OS/2 工作站。此工作站用于创建网络配置数据库，并且，应该作为远程控制台进行安装。

O

Open Shortest Path First (OSPF)(最短路径优先). Internet 协议系列中能够提供域间信息传送的一种功能。作为路由信息协议 (RIP) 的替代物， OSPF 允许最低成本路由选择并可以处理大区域或公司网络的路由选择。

Open Systems Interconnection (OSI)(开放式系统互连). (1) 用于信息交换的开放式系统互联。这种互连遵循国际标准化组织 (ISO) 制定的标准。 (T) (A) (2) 使用标准化程序支持数据处理系统互联。

注: OSI 体系结构建立了一个框架，此框架可用于协调当前和未来计算机系统互联标准的开发。网络功能分为七个层次。每一层次都代表一组相关的数据处理和通信功能，这些功能以标准方式执行后可以支持不同的应用程序。

Open Systems Interconnection (OSI) architecture (开放式系统互连体系结构). 遵守特定开放式系统互连相关 ISO 标准集的网络体系结构。 (T)

Open Systems Interconnection (OSI) reference model (开放式系统互连参考模型). 表明开放式系统互连一般原则的一种模型。除此之外，该模型还展示了七个层次的用途和具体分层方法。 (T)

origin (源). 发出消息或其它数据的外部逻辑单元 (LU) 或应用程序。另见 *destination (目的地)*。

orphan circuit (孤立线路). 一种可以动态获知其可用性的未配置线路。

P

pacing (定步). (1) 接收部件据以控制发送部件的传输速率以防止溢出或拥塞的一种技术。 (2) 另见 *flow control (流控制)*、*receive pacing (接收定步)*、*send pacing (发送定步)*、*session-level pacing (会话级定步)*和 *virtual route (VR) pacing (虚拟路由定步)*。

packet (包). 数据通信中的一系列二进制位，其中包括数据和控制信号。这些内容作为一个复合整体进行传输和交换。数据、控制信号(可能还有错误控制信息)均以特定格式进行安排。 (I)

packet internet groper (PING)(分组互连网搜索程序). (1) Internet 通信中的一个程序。该程序在 TCP/IP 网络中主要用于测试目的地的可到达性。其具体内容为: 向目的地发送 Internet 控制分组协议 (ICMP) 响应请求并等待回答。 (2) 通信中对可到达性的测试。

packet loss ratio (包丢失比率). 包不能到达目的地或者在指定的时间内不能到达目的地的可能性。

packet mode operation (信息包模式作业). 同义词: *packet switching (信息包交换)*。

packet switching (信息包交换). (1) 使用带有目的地地址信息的包路由和传送数据的过程。采用这种方法后，信道只有在包传输时才被占用。传输结束后，此信道便可用于传送其它包。 (I) (2) 与 *packet mode operation (信息包模式作业)*同义。另见 *circuit switching (线路交换)*。

parallel bridges (并行网桥). 连于相同 LAN 段的一对网桥，这对网桥可用于为该段创建冗余路径。

parallel transmission groups (并行传输组). 相邻节点间的多个传输组，每一组均有一个独特的传输编号。

path (路径). (1) 网络中两个任意节点间的路由。这里，一条路径可包括两个或多个分支。 (T) (2) 一系列传输网络组成部分(路径控制和数据链路控制)，这些组成部分通过两个网络可访问设备间的信息交换实现了网络横越。另见 *explicit route (ER)(显式路由)*、 *route extension (路由扩展)*和 *virtual route (VR)(虚拟路由)*。

path control (PC)(路径控制). 网络中的一种功能。使用该功能可在网络中的可访问部件间路由报文单元，并且，在其间提供各种路径。此功能可将传输控制(可能需要将其分段)中的基本信息单元 (BIU) 转换为路径信息单元 (PIU)，并且，与数据链路控制交换含有一个或多个 PIU 的基本传输单元。路径控制因节点类型不同而有所不同: 有些节点(如 APPN 节点)使用本地生成的会话标识符进行路由，而其它节点(子区节点)则使用网络地址进行路由。

path cost (路径费用). 在链接状态路由协议中，两个节点或网络间某条路径上的所有链接费用总和。

path information unit (PIU)(路径信息单元). 一种包单元，此单元仅由传输首部 (TH) 构成，或者，只由 TH 和其后面的基本信息单元 (BIU) 或 BIU 段构成。

pattern-matching character (模式匹配字符). 可用于代表一个或多个字符的一种特殊字符，如星号 (*) 或问号 (?)。任何字符或字符集均可代替模式匹配字符。与 *global character (全局字符)*和 *wildcard character (通配符)*同义。

permanent virtual circuit (PVC)(永久虚拟线路). X.25 和帧中继通信中的一种虚拟电路。此虚拟电路在每个数据终端设备 (DTE) 处均有一个由系统永久分配的逻辑信道。此线路不需要呼叫建立协议。对比: *switched virtual circuit (SVC)(交换虚拟电路)*。

physical circuit (物理线路). 不可多路复用的一种线路。另见 *data circuit (数据电路)*。对比: *virtual circuit (虚拟电路)*。

physical layer (物理层). 在开放式互连参考模型中，通过传输介质，使用机械、电子、功能和过程方式建立、维护和释放物理连接的一层。 (T)

physical unit (PU)(物理单元). (1) 如 SSCP 通过 SSCP-PU 会话请求的那样，管理和监视节点关联资源(如连接的链路和相邻链路站)的部件。SSCP 使用物理单元激活会话，以便通过 PU 间接管理节点资源，如连接的链路。该词仅适用 2.0、4 和 5 型节点。 (2) 另见 *peripheral PU(外设 PU)* 和 *subarea PU (子区 PU)*。

ping command (ping 命令). 发送 Internet 控制分组协议 (ICMP) 响应请求报文至网关、路由器或主机，并且，期待接收到回答的一种命令。

Point-to-Point Protocol (PPP)(点到点协议). 在串行点到点链路上提供包的封装和传输方法的一种协议。

polling (轮询). (1) 在多点连接或点到点连接中，数据站逐个传输的过程。 (I) (2) 为避免争用、确定运作状态或确定数据发送或接收就绪状态而对设备进行的询问过程。 (A)

port (端口). (1) 用于数据输入或输出的存取点。 (2) 设备上的一种连接头。其它设备，如显示站和打印机的电缆便与此连接头相连。 (3) 代表与链路硬件的物理连接。端口有时称为适配器，但是，适配器上却可以有不止一个端口。一个 DLC 进程可以控制一个或多个端口。 (4) Internet 协议系列中的一个 16 位编号。此编号用于在 TCP 或用户数据报协议 (UDP) 和较高级别协议或应用程序间通信。某些协议，如文件传送协议 (FTP) 和简单邮件传送协议 (SMTP)，在所有应用 TCP/IP 的网络中使用共知的端口号。 (5) 一种抽象定义。传送协议使用此定义区分主机中的多个目的地。 (6) 与 *socket (套接字)*同义。

port number (端口号). 在 Internet 通信中，应用实体相对于传送服务的标识。

private branch exchange (PBX)(私人交换分机). 一种私人电话交换机。主要用于传输来往于公用电话网络间的呼叫。

problem determination (问题确定). 确定问题根源的过程。具体原因如: 程序部件、机器故障; 远程通信功能、用户或承包人安装的程序或设备、环境故障，如功率损耗或用户错误。

program temporary fix (PTF)(程序临时性修改). 故障的临时解决方案或临时旁路。此问题由 IBM 在当前尚未修改的程序发行版中诊断确定。

protocol (协议). (1) 一组语义和语法规则。这些规则用于确定实现通信时各种功能部件的运作状况。 (I) (2) 开放式系统互连体系结构中的一组语义和语法规则。这些规则主要用于确定执行通信功能时，同一层实体的运作状况。 (T) (3) SNA 中请求和响应的含义及其编序规则。这些请求和响应主要用于管理网络、传送数据和同步网络部件状态。与 *line control discipline (线路控制规程)*和 *line discipline (线路规程)*同义。见 *bracket protocol (括号协议)* 和 *link protocol (链路协议)*。

protocol data unit (PDU)(协议数据单元). 给定层协议中指定的一种数据单元。此单元由该层的协议控制信息组成，但同时也可能包括该层的用户数据。 (T)

pulse code modulation (PCM)(脉冲代码调制). 模拟声音信号数字化时采用的一种标准。在 PCM 中，声音以 8 kHz 的速率抽样，并且，每个样本都编码在 8 位帧中。

R

Rapid Transport Protocol (RTP) connection (快速传送协议连接). 高性能路由选择 (HPR) 中的一种连接。此连接建立于路由的端点之间，主要用于传送会话信息。

reachability (可到达性). 节点或资源与其它节点或资源通信的能力。

read-only memory (ROM)(只读内存). 一种内存。除某些特殊情况外，用户不能修改此内存中存储的数据。

real-time processing (实时处理). 数据的一种处理过程。这些数据为当某些进程处于运行状态时，该进程要求或生成的内容。通常情况下，当处理进行时，其结果便会用于影响该进程，同时也可能用于影响其它相关进程。

reassembly (重组). 通信过程中，将接收到的分段包重新组合起来的过程。

receive not ready (RNR)(接收未就绪). 通信中的一种数据链路命令或响应。此命令或响应指明无法接收入网帧的临时状态。

receive not ready (RNR) packet (接收未就绪分组). 见 *RNR packet (RNR 分组)*。

received line signal detector (RLSD)(接收线路信号检测器). EIA 232 标准中的一种信号。主要用于向数据终端设备 (DTE) 表明它从远程数据电路端接设备 (DCE) 接收到了信号。与 *carrier detect (载波检测)*和*data carrier detect (DCD)(数据载波检测)*同义。

Recognized Private Operating Agency (RPOA)(经认可的私营电信机构). 除政府部门或业务外，经营远程通信业务的所有其它个人、公司或社团。这些机构均遵守国际电信联盟规程和约定中的条款，如通信公共载波。

reduced instruction-set computer (RISC)(精简指令集计算机). 一种使用小型、简化常用指令的计算机。使用这些指令后，计算机可加快执行速度。

remote (远程设备). (1) 指能够通过远程通信线路访问的系统、程序或设备。 (2) 同义词; *link-attached (链路连接设备)*。 (3) 对比: *local (本地设备)*。

remote bridging (远程桥接). 网桥的一种功能。此功能允许两个网桥使用远程通信链路连接多个 LAN。对比: *local bridging (本地桥接)*。

remote console (远程控制台). 运行 OS/2、TCP/IP 和远程 Nways 交换机资源控制程序的工作站。此工作站可与任何网络支持工作站连接，并对 Nways 交换机进行远程操作或向其提供远程服务。

其连接可以使用:

- 使用调制解调器的交换线路

任何网络支持工作站均可作为另一网络支持工作站的远程控制台使用。

Remote Execution Protocol (REXEC)(远程执行协议). 一种允许在网络的任何主机上执行命令或程序的协议。执行后本地主机接收命令执行结果。

Request for Comments (RFC)(请求注释). Internet 通信中的文件系列。此文件系列描述了部分 Internet 协议系列和相关实验。所有 Internet 标准均作为 RFC 归档。

reset (复位). 虚拟电路上数据流控制的重新初始化过程。复位时，所有转接中的数据都将清除。

reset request packet (复位请求包). X.25 通信中数据终端设备 (DTE) 传输到数据电路端接设备 (DCE) 的一种信息包。此信息包主要用于请求复位虚拟呼叫或永久虚拟电路。另外，包中也可指定请求原因。

resource (资源). 在 Nways 交换机中，由控制程序创建的硬件元素或逻辑实体，例如，适配器、 LIC 和电路均为物理资源; 而控制点和连接均为逻辑资源。

ring (环). 见 *ring network (环形网络)*。

ring network (环形网络). (1) 网络的一种。在这种网络中，每个节点均恰好有两个分支与其相连，并且，任何两个节点间均正好有两条路径。 (T) (2) 一种网络配置。在这种配置中，以单向传输链路连接的设备形成了一个封闭路径。

ring segment (环段). 可与其它部分分离(拔下连接头)的一段环网。见 *LAN segment (LAN 段)*。

rlogin (remote login)(远程注册). rlogin 软件可将用户环境(如终端类型)的相关信息传递到远程机器。

RNR packet (RNR 包). 由数据终端设备 (DTE) 或数据电路端接设备 (DCE) 使用的一种包。此包表明设备暂时无法接受虚拟呼叫或永久虚拟电路的其它包。

root bridge (根网桥). 指作为跨越树根的网桥。此网桥在桥接网络的其它活动网桥间形成。此根网桥产生桥接协议数据单元 (BPDU)，并且，将其传输到其它活动网桥以维护跨越树拓扑结构。在网络中，它是优先级最高的网桥。

route (路由). (1) 一系列编序节点和传输组 (TG)。这些节点和传输组代表因通信交换而在源节点和目的地节点间形成的路径。 (2) 将网络通信从源节点发送到目的地节点时使用的路径。

route bridge (路由桥接). IBM 桥接程序的一种功能。此功能允许两个桥接计算机使用远程通信链路与两个 LAN 相连。每个桥接计算机都直接与一个 LAN 相连，而远程通信链路则将这两个桥接计算机连接起来。

route extension (REX)(路由扩展). SNA 中包括外围链路在内的路径控制网络部件。这些部件组成了子区节点和相邻外围节点的网络可寻址单元 (NAU) 间的路径部分。另见 *explicit route (ER)(显式路由)*、*path (路径)*和 *virtual route (VR)(虚拟路由)*。

Route Selection control vector (RSCV)(路由选择控制向量). 描述 APPN 网络内的路由的控制向量。 RSCV 由一系列编序的控制向量组成，这些向量标识了组成从源节点到目的地节点路径的 TG 和节点。

router (路由器). (1) 用以确定网络通信量流通路径的计算机。路径选择要在几个路径中进行，其选择原则以从以下来源获得的信息为基础: 来自特定协议的信息; 试图标识最短或最优路径的算法规则; 其它标准，如量度或协议专用目的地地址。 (2) 连接两个 LAN 段的连网设备。这两个 LAN 段在参考模型网络层可以使用相似或不同的体系结构。 (3) OSI 术语中的一种功能。此功能主要用于确定到达某一实体的路径。 (4) 在 TCP/IP 中，与 *gateway (网关)* 同义。 (5) 对比: *bridge (网桥)*。

routing (路由选择). (1) 报文到达目的地的路径分配。 (2) 在 SNA 中，沿网络中的特定路径转发报文单元的过程。其具体转发路径由报文单元中携带的参数，如传输首部中的目的地网络地址确定。

routing domain (路由选择域). Internet 通信中的一组中间系统。这些系统使用一个路由协议，这样，每个中间系统中显示的整个网络就都将相同。路由选择域通过外部链路彼此相连。

Routing Information Protocol (RIP)(路由选择信息协议). Internet 协议系列中的一种内部网关协议。此协议主要用于交换域内路由选择信息和确定互连网主机间的最佳路由。确定最佳路由时，RIP 以路由量度值为基础，而不是以链路传输速度为基础。

routing loop (路由选择回路). 当路由器在其间循环信息时产生的一种状态。这种状态要直到会聚发生或相关网络被认定不可到达时才能停止。

routing protocol (路由协议). 路由器使用的一种协议。主要用于查找其它路由器和保留至可到达网络的最近日期最佳路线。

routing table (路由选择表). 用于指导数据报转发或建立连接的一组路由。这些信息在路由器间传递并标识网络拓扑结构和目的地的可到达性。

Routing Table Maintenance Protocol (RTMP)(路由选择表维护协议). AppleTalk 网络中的一种协议。此协议主要用于通过 AppleTalk 路由选择表，在传输层上生成并维护路由选择信息。AppleTalk 路由选择表可以指导互连网上从源端口到目的地端口的包传输。

RouTing update Protocol (RTP)(路由选择更新协议). 一种虚拟网络系统 (VINES) 协议。主要用于维护路由选择数据库和支持 VINES 节点间的路由选择信息交换。另见 *Internet Control Protocol (ICP)(Internet 控制协议)*.

rsh. rlogin 命令的一种变形。主要用于在远程 UNIX 机器上调用命令解释程序，并且，将命令行自变量传送到命令解释程序以完全跳过注册步骤。

S

SAP. 见 service access point (服务访问点)。

seed router (种子路由器). AppleTalk 网络中的一种路由器。此路由器主要用于维护网络的配置数据(如网络序列号和区列表)。每个网络都至少应有一个种子路由器。种子路由器必须以配置程序工具进行初始配置。对比: *nonseed router (非种子路由器)*。

segment (段). (1) 部件或设备间的电缆部分。段可以包括一条临时电缆、几条互连的临时电缆或建筑电缆与互连的临时电缆的组合。 (2) Internet 通信中不同机器的 TCP 功能间的传送单位。每个数据片均包含控制字段和数据字段，当前字节流位置和实际数据字节经校验和识别后可以验证接收到的数据。

segmenting (分段). OSI 中由某一层执行的功能，该层将来自其支持的层次的一个协议数据单元 (PDU) 映射为多个 PDU。

sequence number (顺序号). 通信中分配给特定帧或包的一个号码。此号码主要用于控制传输流和数据的接收。

Serial Line Internet Protocol (SLIP)(串行线路网际协议). 以串行线路连接的两个 IP 主机间使用点到点连接时应用的一种协议。具体串行线路实例如串行电缆或通过电话线连于调制解调器的 RS232。

server (服务器). 一种功能部件。主要用于通过网络向工作站提供共享服务。具体实例如文件服务器、打印服务器和邮件服务器。 (T)

service access point (SAP)(服务访问点). (1) 开放式系统互连 (OSI) 体系结构中的一种点。在此点上，某一层上的实体可将该层的服务提供给上一层实体。 (T) (2) 使用适配器后产生的一个逻辑点。在此点上，信息可以接收和传输。一个服务访问点可以有多个在其内部终止的链路。

Service Advertising Protocol (SAP)(服务广告协议). 网际分组交换 (IPX) 中提供如下内容的一种协议:

- 一种机械装置。此装置允许互连网上的 IPX 服务器按名称和类型对其服务进行广告宣传。使用此协议的服务器可将其名称、服务类型和地址记录在所有运行 NetWare 的文件服务器中。
- 一种机械装置。此装置允许工作站广播查询以找出所有类型的所有服务器、某一特定类型的所有服务器或指定类型的最近服务器。
- 一种机械装置。此装置允许工作站查询运行 NetWare 的所有文件服务器，这样可以找出指定类型的所有服务器的名称和地址。

session (会话). (1) 网络体系结构中，以功能部件间的数据通信为目的，在连接建立、维护和释放期间进行的所有活动。 (T) (2) 两个网络可访问部件 (NAU) 间的逻辑连接。会话经激活、裁剪后可以提供各种协议，并且，也可按要求释放。每次会话在传输首部 (TH) 中都有独特标识，而首部则随附于会话期间交换的所有传输。

Simple Network Management Protocol (SNMP)(简单网络管理协议). Internet 协议系列中的一种网络管理协议。主要用于监视路由器和连接的网络。SNMP 是一种应用层协议。受管设备的信息定义并存储在应用程序的管理信息库 (MIB) 中。

SNA management services (SNA/MS)(SNA 管理服务). 为辅助管理 SNA 网络而提供的服务。

socket (套接字). (1) 进程或应用程序间通信中的终点。(2) 由 University of California's Berkeley Software Distribution (常称为 Berkeley UNIX 或 BSD UNIX) 提供的一种信息摘要，主要作为进程或应用程序间通信的一个终点提供服务。

source route bridging (源路由桥接). LAN 中的一种桥接方法。此方法使用帧内 IEEE 802.5 介质访问控制 (MAC) 首部中的路由选择信息字段确定该帧应转接至哪一环或令牌环段。路由选择信息字段由源节点插入 MAC 首部。路由选择信息字段中的信息是从由源主机生成的探测包中衍生出来的。

source routing (源路由). LAN 中的一种方法。使用这种方法，发送站可确定帧的发送路径，并将路由选择信息包括在帧内。然后，网桥即读取路由选择信息以确定是否应转发该帧。

source service access point (SSAP)(源服务访问点). SNA 和 TCP/IP 中的一种逻辑地址。此逻辑地址允许系统从适当的通信支持将数据发送到远程设备。对比: *destination service access point (DSAP)(目的地服务访问点)*。

spanning tree (跨越树). LAN 上下文中使用的一种方法。使用这种方法后，网桥可自动创建路由表，并且，根据拓扑结构的变化而自动更新该表。这样可以确保桥接网络中任何两个 LAN 间只有一条路径。这种方法可避免分组循环，也就是说，可以避免包经循环路径后又返回发送路由器。

sphere of control (SOC)(控制区域). 由一个管理服务焦点提供服务的控制点域集。

sphere of control (SOC) node (控制区域节点). 直接位于焦点控制范围内的节点。SOC 与其焦点间有交换管理服务能力。如果支持交换管理服务能力功能，则 APPN 终端节点可以是 SOC 节点。

split horizon (划分范围). 最小化时间以获得网络聚拢效果的一种技术。使用这种技术时，路由器记录接收特定路则时使用的接口，但并不通过相同的接口将其自身关于该路径的信息传播回去。

spoofing (欺骗). 数据链路中使用的一种技术。在这种技术中，从终端工作站启动的协议由中间节点代表最终目的地加以确认和处理。例如，在 IBM 6611 数据链路交换过程中， SNA 帧封装为 TCP/IP 包以通过非 SNA 广域网传输，然后，该包再由另一个 IBM 6611 解封并传送至最终目的地。欺骗的益处之一是可以避免端到端会话超时。

standard MIB (标准 MIB). 简单网络管理协议 (SNMP) 中的一种 MIB 模块。此模块位于管理信息结构 (SMI) 的管理分支下，并且已由 Internet 工程任务部 (IETF) 认定为一种标准。

static route (静态路由). 手动输入路由表中的路由，此路由可以是主机间的路由，网络间的路由，也可以既包括主机间路由，也包括网络间路由。

station (工作站). 使用远程通信功能的系统的输入或输出点。例如，在某一特定位置，通过远程线路可以发送或接收数据的一个或多个系统、计算机、终端、设备及关联程序。

StreetTalk. 虚拟联网系统 (VINES) 中一种独特的网络范围的命名和寻址系统。此系统允许用户在不清楚网络拓扑结构的情况下，查找并访问网络上的任何资源。另见 *Internet Control Protocol (ICP)(Internet 控制协议)*和 *RouTing update Protocol (RTP)(路由更新协议)*。

Structure of Management Information (SMI)(管理信息结构). (1) 简单网络管理协议 (SNMP) 中的一组规则。此规则主要用于定义可通过网络管理协议访问的对象。 (2) OSI 中与管理信息相关的一组标准。此组标准包括*管理信息模式*和*受管对象定义指南*。

subarea (子区). SNA 网络中的一部分。由子区节点、附连外围节点和关联资源构成。在子区节点中，子区内所有可寻址的网络可访问部件 (NAU)、链路和相邻链路站(在附连的外围或子区节点中)共享一个公共子区地址，并且，都拥有明确的元素地址。

subnet (子网). (1) 在 TCP/IP 中，以部分 IP 地址标识的一部分网络。 (2) 同义词: *subnetwork (子网)*。

subnet address (子网地址). Internet 通信中，基本 IP 寻址方案的一个扩展部分。这里，主机地址的一部分被解释为本地网络地址。

subnet mask (子网掩码). 同义词: *address mask (地址掩码)*。

subnetwork (子网). (1) 具有共同特点，如相同的网络 ID 的一组节点。 (2) 与 *subnet (子网)*同义。

Subnetwork Access Protocol (SNAP)(子网访问协议). LAN 中的一种 5 字节协议鉴别程序。该程序主要用于识别包所属的非 IEEE标准协议系列。SNAP 值可用来区分使用 $AA 作为其服务访问点 (SAP) 值的各种不同协议。

subnetwork mask (子网掩码). 同义词: *address mask (地址掩码)*。

subsystem (子系统). 一种次级或附属系统。此系统通常能够在独立于控制系统，或与控制系统异步时完成操作。 (T)

switched virtual circuit (SVC)(交换虚拟电路). 一种需要时即可动态建立的 X.25 电路。电路建立后，X.25 等同于交换线路。对比: *permanent virtual circuit (PVC)(永久虚拟线路)*。

synchronous (同步). (1) 与两个或多个进程相关的一种状态。这两个(或多个)进程均依赖于特定事件的发生，如公共计时信号。 (T) (2) 事件的发生与常规的或可预测的时间有一定的关系。

Synchronous Data Link Control (SDLC)(同步数据链路控制). (1) 用于管理通过链路连接传送同步、代码透明、按位串行信息的一种规程。此规程遵循美国国家标准协会 (ANSI) 的高级数据通信控制过程 (ADCCP) 子集和国际标准化组织的高级数据链路控制 (HDLC)。传输交换可以在交换或非交换链路上以双工或半双工方式进行。此链路连接

的配置可以是点到点，也可以是多点或回路。 (I) (2) 对比: *binary synchronous communication (BSC)(二进制同步通信)*。

synchronous optical network (SONET)(同步光纤网络). 使用光纤接口传输数字信息时使用的一种美国标准。此标准与同步数字分级结构 (SDH) 介绍密切相关。

SYNTAX. 简单网络管理协议 (SNMP) 中 MIB 模块里的一个语句。此语句定义了与受管对象对应的摘要数据结构。

system (系统). 数据处理中组织起来的人、机器、方法的集合。此集合可用于完成一系列指定功能。(I) (A)

system configuration (系统配置). 指定构成特定的数据处理系统的设备或程序的过程。

system services control point (SSCP)(系统服务控制点). 子区网络中的一种部件。主要用于管理配置、协调网络操作员和处理问题确定请求，除此之外，该部件还向网络用户提供目录服务及其它会话服务。以对等形式彼此协作的的多个 SSCP 可将网络分为许多控制域，每个 SSCP 与其域内的物理部件和逻辑部件都有分层控制关系。

Systems Network Architecture (SNA)(系统网络体系结构). 用于传输信息单元和控制网络配置及操作的逻辑结构、格式、协议和操作序列的说明信息。SNA 分层结构接受所有可能的信息源和信息目的地，也就是说，接受独立的、不为用于信息交换的特定 SNA 网络服务和功能所影响的用户。

T

TCP/IP. (1) 传输控制协议/网间协议。 (2) 类 UNIX 或以以太网为基础的系统互连协议。此协议最初由美国国防部开发研制。TCP/IP 支持 ARPANET (高级研究项目管理网)，一种分组交换搜索网络。此网络中，4 层为 TCP，3 层为 IP。

Telnet. Internet 协议系列中的一个。主要用于提供远程终端连接服务。此协议使一台主机上的用户在注册到远程主机时，就如同在与同一台主机上的其它用户直接相连一样。

threshold (阈值). (1) IBM 桥接程序中的一个值。主要用于设定『超过阈值』发生并报告给网络管理程序前，允许因错误而没有通过网桥转发的最大帧数目。 (2) 一个初始值，计数器从该值开始逐渐递减为 0: 或是一个差值，计数器以该值为基础从初始值开始逐渐递增或递减。

throughput class (吞吐量级). 分组交换中的一种速度标识。数据终端设备 (DTE) 包以此速度为基础通过分组交换网络。

time division multiplexing (TDM)(时分多路复用). 见 ***channelization (信道化)***。

time to live (TTL)(生存时间). 最优传送协议使用的一种技术。主要用于保存无限循环的包。如果 TTL 计数器达到 0，则废除该包。

timeout (超时). (1) 在预定义的时间周期开始时，某一事件发生，当周期结束时，如果此事件尚未结束，则另一事件立即发生，此种情况即称为超时。 (I) (2) 一种时间间隔，主要用于等待某一操作的发生。例如，系统操作中断并必须重启前的轮询响应或寻址响应。

token (令牌). (1) 局域网中的一种权力符号。此符号由一站至另一站顺序传递，传递到哪一站就表明该站对传输介质有暂时的控制权。每个数据站都只有一次机会获取并使用令牌控制介质。令牌是表明允许传输数据的一条特定消息或位模式。 (T) (2) 在 LAN 中，沿传输介质由一个设备传向另一个设备的一系列位。当令牌上附加了数据后，它就成为了数据帧。

token ring (令牌环). (1) 符合 IEEE 802.5 要求的一种网络技术。此技术主要以在介质连接的工作站间传递令牌(特殊的包或帧)的方式控制介质访问。 (2) IEEE 802.5 网络。在这样的网络中，令牌由一个附连的环站(节点)传到下一个环站。 (3) 另见 *local area network (LAN)(局域网)*。

token-ring network (令牌环网). (1) 一种环网结构。利用令牌传递规程，此网络允许数据站间的单向数据传输，这样，被传输的数据最终还要返回传输站。 (T) (2) 使用环拓扑结构的一种网络。在该网络中，令牌在节点间呈环形传递。准备好发送的节点可以捕捉令牌并将需要传输的数据插入。

topology (拓扑). 在数据通信中，网络内节点的物理或逻辑安排，特别是节点及其间的链路的关系。

topology database update (TDU)(拓扑数据库更新). 新的或更改过的链路及节点的相关消息。此消息在 APPN 网络节点间广播以维护网络拓扑数据库，广播时，此消息将在各个网络节点复制。TDU 中包含的信息可以标识如下内容:

- 发送节点
- 网络中各种资源的节点和链路特性
- 各个所述资源的最近更新序列号

trace (跟踪). (1) 计算机程序的执行记录。此记录展示了指南的执行序列。 (A) (2) 对于数据链路而言，是传输或接收到的帧和字节的记录。

transceiver (transmitter-receiver)(收发器). LAN 中的一种物理设备。此设备将主机接口连接到局域网，如以太网。以太网收发器中既包含能将信号附加到电缆上的电子，也包含能检测冲突的电子。

Transmission Control Protocol (TCP)(传输控制协议). 一种通信协议。主要用于 Internet 和其它符合美国国防部互连网协议标准的网络。在分组交换通信网络和类似网络的互连系统中，TCP 能够在主机间提供可靠的主机到主机协议。另外，它使用 Internet 协议 (IP) 作为基本协议。

Transmission Control Protocol/Internet Protocol (TCP/IP)(传输控制协议/网际协议). 一组通信协议。此组协议同时支持局域网和和广域网的对等联网连接功能。

transmission group (TG)(传输组). (1) 相邻节点间的一种连接，此连接由传输组号标识。(2) 在子区网络中，相邻节点间的一个单独链路或一组链路。当传输组中包含一组链路时，这组链路便被视为一个单独的逻辑链路，而此传输组则称为 *multilink transmission group (MLTG)(多链路传输组)*。*mixed-media multilink transmission group (MMMLTG)(混合介质多路传输组)*是包含多种介质类型(如令牌环、交换 SDLC、非交换 SDLC 和帧中继链路)的传输组。(3) APPN 网络中相邻节点间的单独链路。(4) 另见 *parallel transmission groups (并行传输组)*。

transmission header (TH)(传输头). 控制信息，其后内容可任选基本信息单元 (BIU) 或 BIU 段。此信息由路径控制生成并用以路由报文单元和在网内进行流控制。另见 *path information unit (路径信息单元)*。

transparent bridging (透明桥接). LAN 中使用的一种方法。这种方法可将单个的局域网通过介质访问控制 (MAC) 层连接起来。透明网桥中存有包含 MAC 地址的图表，这样，在该表的指示下，网桥便可以将遇到的帧转发至其它 LAN。

transport layer (传输层). 开放式系统互连参考模型中的一个层次。此层能够提供可靠的端到端数据传输服务。该路径中可能有中继式开放系统。(T) 另见 *Open Systems Interconnection reference model (开放式系统互连参考模型)*。

trap (陷阱). 简单网络管理协议 (SNMP) 中使用的一个消息。此消息由受管节点(代理功能)发送至管理站，其主要功能是报告异常状态。

trunk line (中继线路). 连接两个 Nways 交换机的高速线路。此线路可以有多种选择，如同轴电缆、光纤电缆或无线电波，并且，此线路也可从电信公司租用。

T1. 美国使用的一种 1.544-Mbps 的公共访问线路。此线路 24 小时均可从 64-Kbps 隧道访问。欧洲版本 (E1) 以 2.048 Mbps 传输。

U

universally administered address (通用管理地址). 局域网中使用的一种地址。此地址在制造时便已永久编码在适配器中。所有的通用管理地址都是唯一的。对比: *locally administered address (局部管理地址)*。

User Datagram Protocol (UDP)(用户数据报协议). Internet 协议系列中的一个。此协议提供无可靠性、无连接的数据报服务。它主要负责启用机器或进程上的应用程序，或者，处理并发送数据报至另一机器或进程上的应用程序。UDP 使用网际协议 (IP) 发送数据报。

V

V.24. 数据通信中 CCITT 的一种规范说明。此说明主要定义了数据终端设备 (DTE) 和数据电路端接设备 (DCE) 间交换电路的定义列表。

V.25. 数据通信中 CCITT 的一种规范说明。此说明主要定义了通用交换电话网络上的自动应答设备和并行自动呼叫设备，其中包括响应控制设备的禁用过程，当然，这些设备既可以是用于手动，也可以是用于自动建立的呼叫的设备。

V.34. 一种 ITU-T 推荐标准。主要用于通过可经商业途径获得的标准音频级 33.6-Kbps (或更低) 隧道进行的调制解调器通信。

V.35. 数据通信中 CCITT 的一种规范说明。此说明定义了不同数据速率的数据终端设备 (DTE) 和数据电路端接设备 (DCE) 间交换电路的定义列表。

V.36. 数据通信中 CCITT 的一种规范说明。此说明主要定义了速率为 48、56、64 或 72 千位/秒的数据终端设备 (DTE) 和数据电路端接设备 (DCE) 间交换电路的定义列表。

version (版本). 一个单独许可的程序。该程序通常都有明显不同的新代码或新功能。

VINES. 虚拟联网系统。

virtual circuit (虚拟电路). (1) 分组交换中网络提供的一种功能。此功能给用户一种实际连接的印象。(T) 另见 *data circuit (数据电路)*。对比: *physical circuit (物理电路)*。(2) 两个 DTE 间建立的一种逻辑连接。

virtual connection (虚拟连接）. 帧中继中潜在连接的返回路径。

virtual link (虚拟链路). 最短路径优先 (OSPF) 中的一个点到点接口。此接口主要用于连接被非干路转接区分隔开的边缘路由器。由于区域路由器是 OSPF 干路的一部分，因此虚拟链路连于干路。虚拟链路可确保 OSPF 干路的连续性。

VIrtual NEtworking System (VINES)(虚拟联网系统). Banyan Systems, Inc. 开发的网络操作系统和网络软件。在 VINES 网络中，虚拟链路使所有设备和服务看起来似乎都是直接连接的，但实际上它们之间可能有千里之遥。另见 *StreetTalk*。

virtual route (VR)(虚拟路由). (1) SNA 中的一个 (a) 逻辑连接。此连接位于两个子区节点之间且这两个子区节点从物理意义来讲，已经形成了一个特定的显式路由；或者是一个 (b) 逻辑连接。但此连接完全包含在用于节点间会话的子区节点中。相异子区节点间的虚拟路由负责将传输优先级附加到基本显式路由，通过虚拟路由定步提供流控制和通过对路径信息单元 (PIU) 进行序列编号提供数据集成。 (2) 对比: *explicit route (ER)(显式路由)*。另见 *path (路径)*和 *route extension (REX)(路由扩展)*。

W

wide area network (WAN)(广域网). (1) 网络的一种。从地理区域角度考虑，此网络较局域网或城域网提供的通信服务范围更大，并且该网络还可以使用或提供公共通信设施。 (T) (2) 专为几百英里或几千英里区域设计的一种数据通信网络。例如，公共和私人分组交换网络及国家电话网络。 (3) 对比: *local area network (LAN)(局域网)*和 *metropolitan area network (MAN)(城域网)*。

wildcard character (通配符). 同义词: *pattern-matching character (模式匹配字符)*。

X

X.21. 国际电报电话咨询委员会 (CCITT) 的一种推荐标准。此标准主要用于数据终端设备和数据电路端接设备间的普通接口，以便在公共数据网络上实现同步操作。

X.25. (1) 国际电报电话咨询委员会 (CCITT) 的一种推荐标准。此标准主要用于数据终端设备和分组交换数据网络间的接口。 (2) 另见 *packet switching (分组交换)*。

Xerox Network Systems (XNS)(施乐网络系统). 由施乐公司开发的一套互连网协议。尽管此协议与 TCP/IP 协议近似，但 XNS 使用不同的包格式和术语。另见 *Internetwork Packet Exchange (IPX)(网际分组交换)*。

Z

zone (区域). 在 AppleTalk 网络中，互连网内的一个节点子集。

Zone Information Protocol (ZIP)(区域信息协议). AppleTalk 网络中的一种协议。此协议主要通过在会话层上保留互连网内的区域名和网络号的映射来提供区域管理服务。

zone information table (ZIT)(区域信息表). 网络号及其在互连网中的关联区域名映射的列表。在 AppleTalk 互连网中，此列表由各个互连网路由器维护。

索引

本索引按汉语拼音, 数字, 英文字母和特殊字符顺序排列。

[A]

[B]

[C]

[D]

[F]

[G]

[J]

[L]

[T]

[W]

[X]

[Y]

[Z]

A

C

D

E

F

I

L

M

N

P

Q

R

S

T

U

V

W

读者意见表

Access Integration Services
使用和配置功能部件版本 3.2

SC84-0713-00

姓名

地址

单位及部门

电话号码

读者意见表

SC84-0713-00

请沿此线
撕下或折起

折起并封口　　**请勿使用钉书机**　　折起并封口

在此
贴上
邮票

IBM 公司
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

折起并封口　　**请勿使用钉书机**　　折起并封口

SC84-0713-00

请沿此线
撕下或折起

Printed in China

SC84-0713-00

Spine information:

IBM Access Integration Services AIS V3.2 使用功能部件