Communications Server z/OS® V1R5 and V1R6 Technical Update

TN3270 Server

Topics

➢z/OS V1R5

- ►IPv6 Support
- ►Generic Connection Takeover
- ►Unlock Keyboard Control
- ►IP Range Specification
- ►Network Access Control
- ►Performance monitoring

➢z/OS V1R6

- ►TN3270 server in a separate address space
- ►SCS-mode formatted USS table support

TN3270 Server in CS z/OS V1R5

IBM ®

TN3270 server IPv6 enabled

V1R5 e™

- ➢ Enhanced TN3270 Telnet for IPv6
  - ▪ Profiles will accept IPv6 format addresses.
  - ▪ Commands will accept IPv6 format addresses.
  - ▪ Displays will accommodate IPv6 format addresses.
    - ► IP address now can use up to 39 characters.
    - ► Tabular displays, if IPv6 format, wrap data to second line.
      - – EZZ6064I Summary Connection Display.
      - – EZZ6081I CLientID Display.
      - – EZZ6082I CLientID List Display.
      - – EZZ6083I OBJect Display.
      - – EZZ6065I Detail Connection Display.
    - ► To see wrap format in IPv4, use FORMAT LONG option on the IPCONFIG statement
    - ► Make sure to review any console message automation logic that depends on non-IPv6 format
  - ▪ USSMSG10 IP Substitution
    - ► IPv4 - @@@@@@@@@IPADDR
    - ► IPv6 - @@..@@IPADDR (33 total @'s)

- ➢ IPv6 based on TCP/IP environment

  - ▪ If TCP/IP is IPv6 enabled, Telnet is IPv6 enabled.
  - ▪ If TCP/IP is IPv4 only, Telnet also is IPv4 only.

Display examples IPv6 enabled TB3270 server - notes

V1R5

NOTES

➤ **IPv6 - Allow the IP address to take up the entire line. For consistency, all Client Identifiers will take up the remainder of the line.**
➤ **Summary Connection Display**
   ➤ D TCPIP,,T,CONN

```
EZZ6064I TELNET CONNECTION DISPLAY
           EN                                          TSP
CONN     TY IPADDR..PORT          LUNAME   APPLID   PTR LOGMODE
-------- -- -------------------- -------- --------  --- --------
00000026 4S ::FFFF:9.27.11.202..3408
                                 TCPM1022          TPE SNX32702
00000026 4S ::FFFF:9.27.11.202..3407
                                 TCPM1021          TPE SNX32702
----- PORT:    23  ACTIVE             PROF: CURR CONNS:      2
------------------------------------------------------------
4 OF 4 RECORDS DISPLAYED
```

➤ **OBJect Display**
   ➤ D TCPIP,,OBJ,TYPE=LUGRP

```
EZZ6083I TELNET OBJECT DISPLAY
OBJECT      CONNS  CLIENT ID CLIENT ID              DEFAPPL/
NAME        USING  TYPE      NAME          OPTIONS  ASSOC
----------  ------ --------- ------------- -------- --------
LUGRP
  LUGRP1         0 IPADDR    FEC0:1218:3333::2222
                                          --G-----C-
  LUGRP1         0 LINKNAME  CTCLNK6
                                          ALSD-F--C- APPL2
  LUGRP2         0 HNGRP     HNGRP1
                                          --G-----C-
----- PORT:    23  ACTIVE             PROF: CURR CONNS:      0
------------------------------------------------------------
9 OF 9 RECORDS DISPLAYED
```

TN3270 server reconnect - specific LU requests supported since OS/390 V2R10

Specific LU name request - supported since OS/390 V2R10
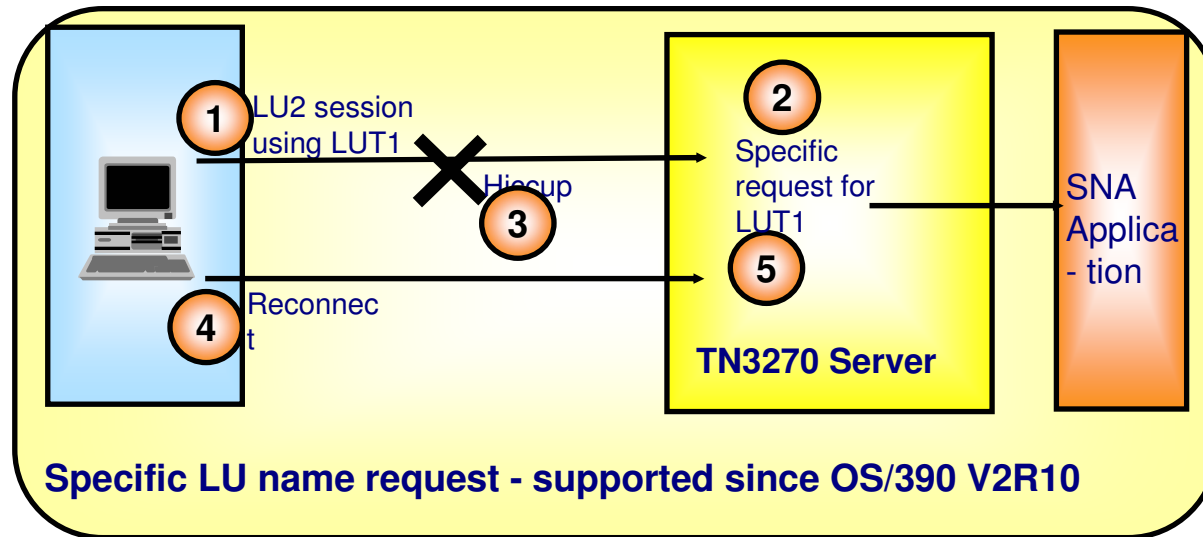
1 Initiate connection for establishing an LU2 session using LU LUT1.

2 TN3270E Server allows LU name LUT1 and user connects to SNA application.

3 Network has a hiccup and client to server IP connection is broken

4 Client sends a new connection (reconnect) request

5 Reconnect logic kicks in and reconnects the user with the SNA application.

- 5a. Telnet suspends new request
- 5b. Sends TimeMark to original client
- 5c. If response, rejects new request
- 5d. If no response, new request continues setup with original LU and copies all relevent session info.

TN3270 server reconnect - generic LU requests now also supported (V1R5)

V1R5 *e*™

Generic LU name request - support added in z/OS V1R5
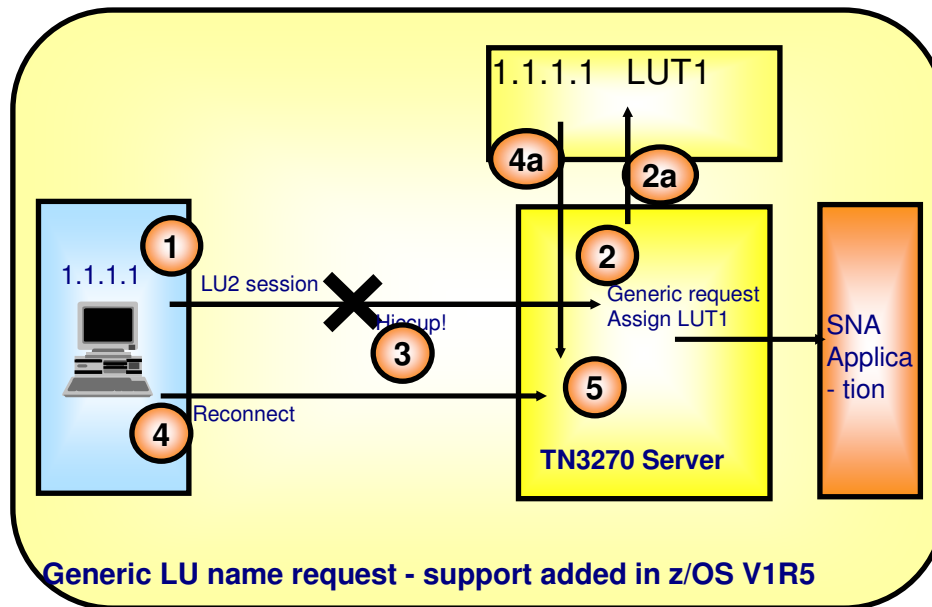
1 Initiate connection without specifying an LU name.

2 TN3270E Server assigns LU name LUT1 and user connects to SNA application.
- 2a. Telnet adds Client ID/LU name to master table.

3 Network has a hiccup and client to server IP connection is broken

4 Client sends a new connection (reconnect) request
- 4a. Request from IP addr 1.1.1.1, so Telnet assigns LUT1 to connection request to simulate a Specific LU request.

5 Reconnect logic kicks in and reconnects the user with the SNA application.
- 5a. Telnet suspends new request
- 5b. Sends TimeMark to orignal client
- 5c. If response, rejects new and next available Generic LU is assigned.
- 5d. If no response, new request continues setup with original LU by copying all relevent session info.

6 At disconnect time, Telnet removes the Client ID - LuName entry from the table.

Generic takeover - notes

NOTES

➢Generic Takeover - Telnet Saves LU Name by Client Identifier.

➢Creates a table that can be searched quickly by Client Identifier.
- ►Userid based on Client Certificate.
- ►Hostname of the client host.
- ►Source IP address of the client host.

➢When a connection is accepted, check the table based on highest priority Client Identifier.
- ►If not found (1st connection), add an entry based on the highest priority Client Identifier and save the assigned LU name with that Client Identifier.
- ►If found (not 1st connection), temporarily assign the LU name in the table to the new connection.
  - ▪If the LU name is in-use, begin the takeover process.
  - ▪If the original connection responds, takeover will fail. Telnet will then treat this connection as an ordinary Generic LU request and search for an unused LU name.
  - ▪If no response from the original connection, Telnet will continue the takeover process by ending the original connection and resuming the new connection with the LU name assigned to the new connection.

➢When an LU name is no longer assigned to a connection, its entry in the ClientID/LUname table is removed.

➢Generic Takeover is based on saving an LU name at assignment time. Therefore, any connection type can use this takeover function.
- ►TN3270E - Save LU name during connection negotiation.
- ►TN3270 - Save LU name at application selection time.
- ►Linemode - Save LU name at application selection time.

Generic Takeover - considerations and configuration

V1R5 *e*

- Additional connections slower
  - Additional connections must always try takeover first.
  - After Takeover failure, a new LU name assigned.
- One LU name per Client Identifier
  - The first LU name assigned is saved.
  - Additional connections can not be taken over.
- Two New Statements:
  - TKOGENLU sec
    - Takeover using a Generic LU connection request.
    - The original SNA session is ended when the connection is taken over.
  - TKOGENLURECON sec [keepontmreset]
    - Takeover using a Generic LU connection request.
    - The original SNA session is saved and transferred to the new connection.
    - keeponTMreset indicates that Telnet should keep the session when a reset is received from the original client after TIMEMARK has been sent. Telnet normally interprets a reset as a client disconnect and will drop the session. Sometimes, when a TIMEMARK is sent to a client host that no longer has the socket specified, the client host will send a reset back to Telnet. In this case, the session should be retained.
      - Specifying KeeponTMreset does create a slight security exposure. An end user may disconnect just after another user attempts takeover. The disconnect reset will be perceived by Telnet as a response to the TIMEMARK sent for takeover and the session will not be dropped.

Generic takeover - notes

V1R5

NOTES

➢The first connection will not find a Client Identifier. An LU name will be found and assigned, and an entry will be added to the ClientID/LUname table.

➢Additional connections will find the Client Identifier in the table.
- ►The LU name from the first connection will be temporarily assigned to the connection and takeover will be attempted.
- ►The original connection will respond indicating takeover failure.
- ►Regular Generic lookup will find an available LU name.
- ►The connection time delay is equal to the takeover time value.

➢Only one LU name per Client Identifier is saved for takeover attempts.
- ►The first connection from a Client Identifier that is assigned an LU name is the ClientID/LUname entry saved in the ClientID/LUname table.
- ►Additional connections from the same Client Identifier will not be eligible for takeover. Their LU names will not be saved.
- ►(If they were saved...
  - •Each additional connection would have to try all current LU names before getting a new LU name.
  - •Telnet would not know how to match takeover requests with emulators. Different emulator characteristics could get switched to different LU names.)

➢sec is the number of seconds Telnet will wait for a response from the original connection.
- ►Valid values are 0-99999999.
- ►0 is a special case indicating Telnet should always takeover, whether or not the original connection is active. This is a useful setting during initial testing.
- ►5 seconds is a typical value.

Generic Takeover - further considerations

V1R5

➢Code at three levels of granularity

- ▪TelnetGlobals
- ▪TelnetParms
- ▪ParmsGroup

➢TKOSPECLU and TKOGENLU can coexist

➢Existing NOTKO turns off ALL takeover

- ▪TKOSPECLU / TKOSPECLURECON
- ▪TKOGENLU / TKOGENLURECON

➢Best use of TKOGENLU / TKOGENLURECON

- ▪One LU name used per unique Client ID.
- ▪Individual LUMAP statements **NOT** needed.

"Stubborn" clients that don't know when to unlock the keyboard

Current TN3270 server process that works for (almost) all TN3270(E) clients:

1 F5C2 (Only in chain, no CDI, no EB). Application sends unlock keyboard, but no CDI or EB, so TN3270 server turns off unlock keyboard and remembers that the application sent it.

2 F5C0 (Unlock keyboard turned off).

3 F6 (Only in chain, CDI). Read buffer, read modified, or read partition query from SNA application.

4 TN3270 server first sends an unlock keyboard to properly finish the previously sent data

5 TN3270 server then sends the read modified
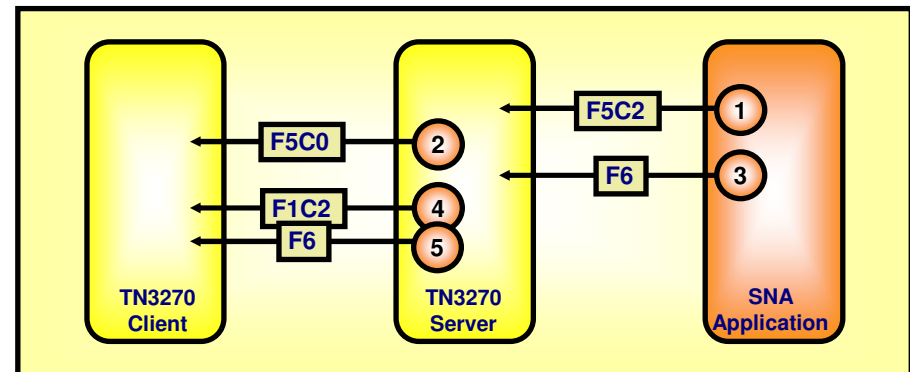
➢ In some cases, type-ahead has buffered data and the unlock keyboard (4) allows the client to send the data to Telnet which forwards it to the application. The application assumes this is the response to the read modified and issues errors. In this case, the unlock keyboard should have been sent AFTER the read modified was sent.

➢ Some applications do not send data to the client first. They expect data from the client after sending the BIND.

  ► TN3270E connections send the Bind to the client alerting it to unlock the keyboard.

  ► Telnet can not send a BIND to the client over a TN3270 connection. In this case the client keyboard remains locked and the end user can not send data to the application. Because the application is waiting for data, the session is essentially hung.

Two new sets of options in z/OS V1R5:

1 Send unlock keyboard before or after a READ command has been received from the SNA application

  ► READ Buffer, READ Modified, READ partition query

  ► Does not apply if SNA extensions have been negotiated on a TN3270E connection (the TN3270E commands for keyboard restore (KRI) and start data indicator (SDI) are used instead in that case)

2 Send unlock keyboard after BIND

  ► Only applies to TN3270 connections (not TN3270E)

If you have problems with specific clients that occasionally hang, you may want to experiment with these options in a PARMSGROUP that is mapped to those specific client identifiers. APARs for OS/390 V2R10 - PQ63027, z/OS V1R2 - PQ63027 & PQ67798, and z/OS V1R4 - PQ63027 & PQ67798

```
UNLOCKKEYBOARD

  BEFOREREAD|AFTERREAD

  TN3270BIND|NOTN3270BIND
```

IP address range definitions
More flexibility in z/OS V1R5

V1R5 *e*

➢ Before z/OS V1R5, IP address ranges could be specified via subnet mask values only:
- 255.255.255.0:1.1.1.0
  - (255 addresses)

➢ An IP address range isn't always a full or partial subnet:
- 1.1.1.4, 1.1.1.5, 1.1.1.6, 1.1.1.7, 1.1.1.8, 1.1.1.9

➢ The above does not fit a subnet.
- 4 - 0100
- 5 - 0101
- 6 - 0110
- 7 - 0111
- 8 - 1000
- 9 - 1001

➢ To allow 4-9 would require allowing 1-15:
- 255.255.255.240:1.1.1.0

➢ IP range format similar to LU range format.

> ► *IP_low_addr..IP_high_addr*

➢ Examples:
- 1.1.1.4..1.1.1.9
- FEC0::3A92:1211..FEC0::3A92:2399
- ::FFFF:1.1.1.3..::FFFF:1.1.3.B

➢ Telnet will create individual IP addresses
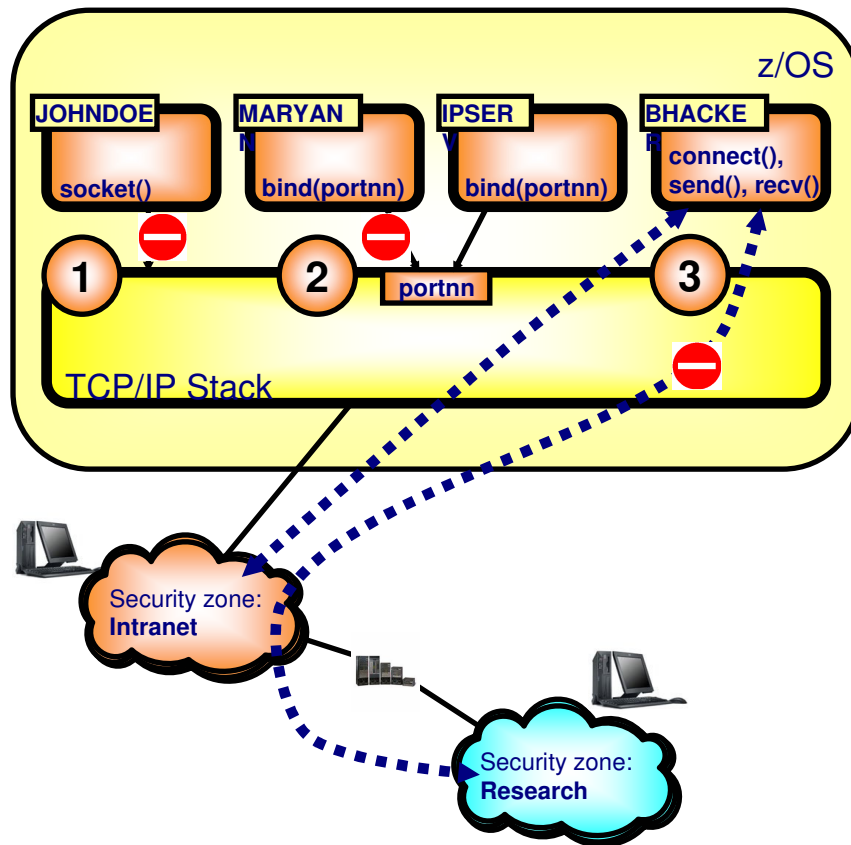
➢ Displays will show ranges as coded

➢ Internal processes treat as individual IP addresses

➢ Considered exact IPs in a group in the client ID hierarchy

➢ Large ranges may affect performance
- The range is treated as individual IP entries
- If a large range is needed, try to use a subnet mask

Protecting TCP/IP services, server port numbers, and network segments

V1R5

z/OS

JOHNDOE
socket()

MARYAN
bind(portnn)

IPSER
bind(portnn)

BHACKE
connect(), send(), recv()

1   2   portnn   3

TCP/IP Stack

Security zone:
Intranet

Security zone:
Research

SAF resources in the SERVAUTH resource class

```
EZB.STACKACCESS.sysname.tcpname
EZB.PORTACCESS.sysname.tcpname.SAFkeywor
d
EZB.NETACCESS.sysname.tcpname.zonename
```

1 Stack Access Control
  - Controls user ability to open socket (use of TCP/IP services)
    - z/OS CS TCP/IP stack is considered a resource
    - Granularity is per stack in a multi-stack environment
  - Access to stack via sockets allowed if user permitted to SAF resource (SERVAUTH class: STACKACCESS)

2 Local Port Access Control
  - Controls user access to a local TCP or UDP port
    - Port is considered a resource
  - Function enabled
    - Via SAF Keyword on PORT or PORTRANGE
  - Access to port allowed if user permitted to SAF resource (SERVAUTH class: PORTACCESS)
  - Access to port not permitted for any user
    - Via RESERVED Keyword On PORT Or PORTRANGE

3 Network Access Control
  - Controls local user access to network resources
    - Network considered a resource - Network/Subnet/Specific host
  - Allows management of security zones
    - Via NETACCESS statement In TCP/IP Profile - NETACCESS statement allows grouping of network resources
  - Access to security zone allowed if user permitted to SAF resource (SERVAUTH class: NETACCESS)

Network access control and TN3270

V1R5 e ™

➢ Prior to z/OS V1R5, it wasn't possible to use NETACCESS control for Telnet

- The TCP/IP system address space is exempt as a user and has access to all security zones.
- Telnet runs in the TCP/IP address space. Therefore, all of its processes are considered part of TCP/IP and are exempt from Network Access Control.

➢ Without NETACCESS control, telnet breaks end-to-end Multilevel security
- Security label check for equivalent security level between:
  - The host VTAM SNA application
  - The Telnet LU representing the client
- No check of the Client.
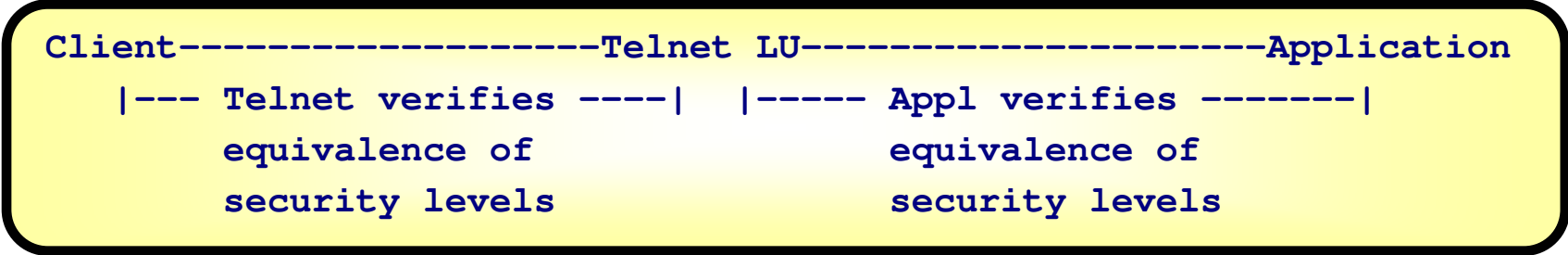
```
Client------------------Telnet LU---------------------Application
    |----- no equivalence ---| |----- Appl can verify ------|
          checking of                  equivalence of
          security levels              security levels
```
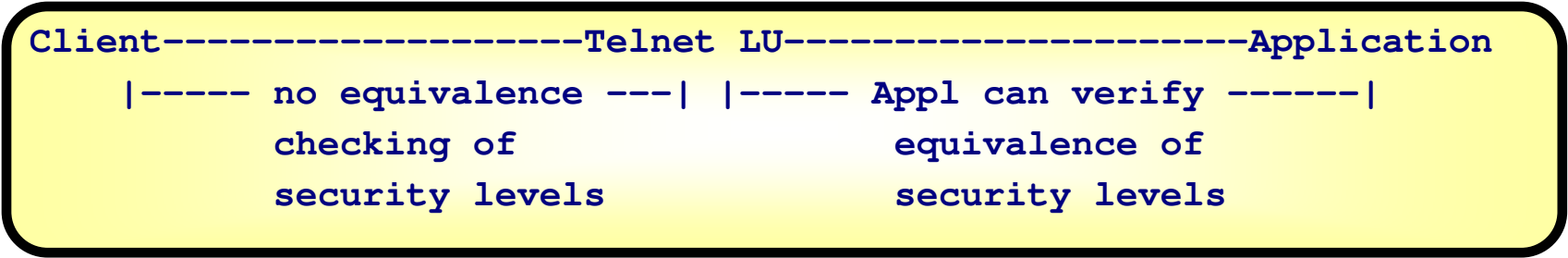
Network access control and TN3270 server in z/OS V1R5

V1R5 *e* ™

➢ Differentiate between TCP/IP & Telnet

- Give Telnet a unique security userid.
- Use the unique identifier during network access.
  - ► Send data
  - ► Receive data

➢ Obtain Security Label of client & LU name

- Compare Security levels of client & LU name.
- Client must be equivalent security level.

```
Client------------------Telnet LU-------------------Application
   |--- Telnet verifies ----|   |----- Appl verifies -------|
         equivalence of                equivalence of
         security levels               security levels
```

TN3270 network access control configuration

➢Enable Network Access Control by Port

```
NACUSERID nac_name  |  NONACUSERID
```

➢Can be coded at two levels of granularity
  ►TelnetGlobals
  ►TelnetParms

➢NACUSERID can not be changed while port active
  ►The nac_name is a userid defined in the system security product.
  ►NONACUSERID will turn off Network Access Control for a port if it was specified in the TELNETGLOBALS block.
  ►The NACUSERID affects the entire port. If several qualified ports are defined, each must have the same NACUSERID value. If there is a mismatch (either no NACUSERID or a different value), the first TELNETPARMS is considered correct. Any TELNETPARMS blocks that differ from the first are not accepted.
  ►The port must be stopped to change the NACUSERID. The port can then be restarted with the new NACUSERID.

➢Example:

```
TELNETPARMS  PORT 23  NACUSERID  TNUSER1  ENDTELNETPARMS
```

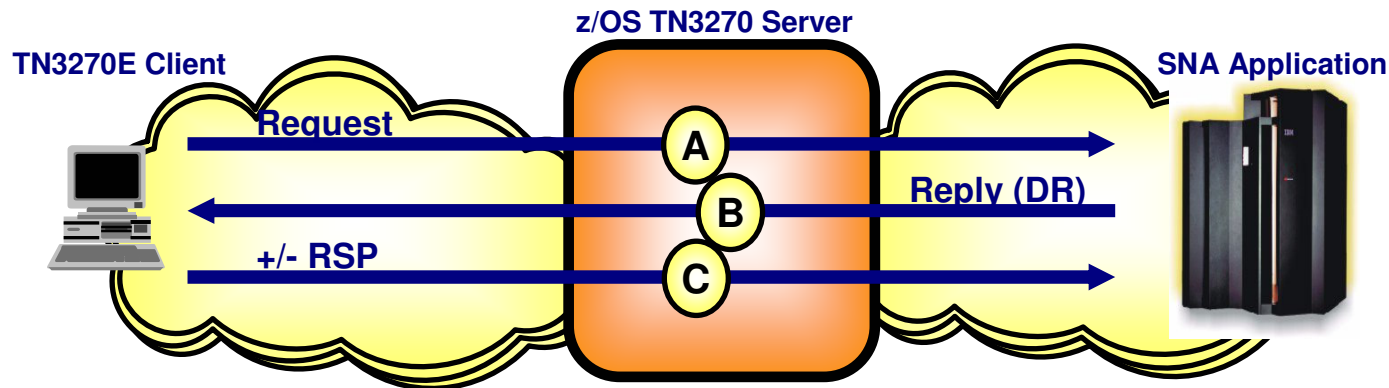# TN3270 response time monitoring basics

V1R5 *e* ™

➢ The TN3270 server in z/OS V1R5 implements a built-in TN3270 round-trip response time monitor function.

- **Time A** - when request is sent to the SNA application
- **Time B** - when reply is sent to the TN3270E client
- **Time C** - when response is received from TN3270E client

```
Round-trip response time = Time C - Time A
IP response time         = Time C - Time B
SNA response time        = Round trip response time - IP response time
```

z/OS TN3270 Server

TN3270E Client

SNA Application

Request — A

Reply (DR) — B

+/- RSP — C
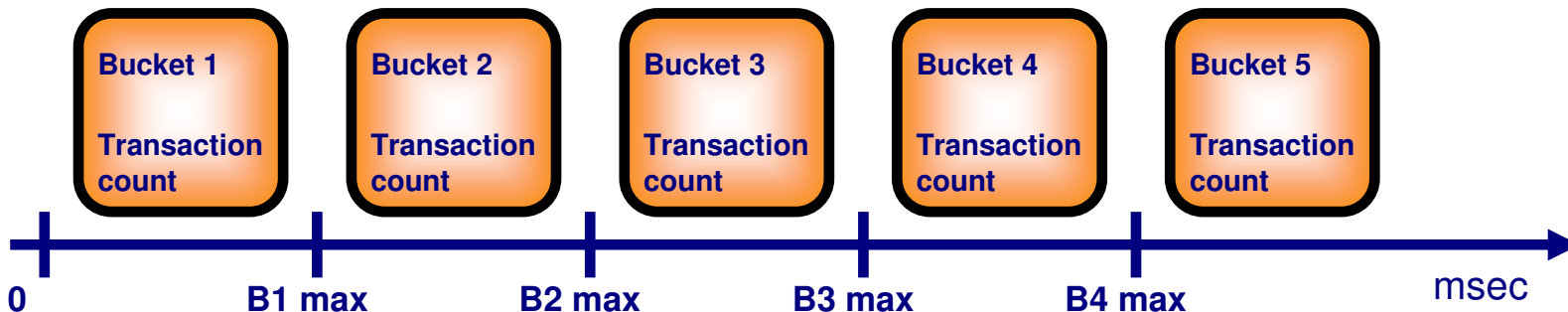
TN3270 response time monitoring - notes

NOTES

➢The performance data can be accessed via SNMP requests

➢The enterprise-specific TN3270 MIB is closely based on the MIB objects defined in RFC 2562. That RFC can be referenced for a more detailed explanation about the data collected and methods used to calculate averages. The z/OS CS SNMP agent and subagents support for nonstandard MIB variables is defined in several files shipped with the product. These files are installed into the HFS in the /usr/lpp/tcpip/samples directory. mvstn3270.mi2 contains the SNMPv2 syntax (SMI) for the IBM MVS Enterprise-Specific TN3270 MIB.

➢RFC 2561, Base Definitions of Managed Objects for TN3270E using SMIv2, is a companion RFC which defines objects for configuring and managing a TN3270E Server. This RFC is not implemented. Profile-based configuration and management is more robust and flexible. It will remain the only method available for TN3270 Server configuration and management.

➢If the application does not request Definite Response and the connection is a TN3270E connection, DR will be set by Telnet. The response is not forwarded to the application.

➢If the connection is not TN3270E, append a TIMEMARK to the data. Telnet uses the TIMEMARK to approximate the IP response time. TIMEMARK acts as an "are you there" for almost all clients. Timestamps B and C are set based on when the TIMEMARK request is sent and when a TIMEMARK response is received.

➢IP measurements can be turned off if they are not wanted.

➢Round trip response time does not include the time data may be queued in Telnet waiting to be sent to the application. If the Telnet server does not have permission to send data to the application it must hold the data until it can be sent. When it is sent, time A is recorded.

TN3270 performance data that is collected

V1R5 *e* ™

- Life-of-Connection data for Life-of-Connection averages
  - Transaction count
  - Round Trip & IP Response Time totals
  - Averages for round trip, IP, and SNA response times
- Sliding-Window data for Sliding-Window averages
  - Period Transaction count
  - Period Round Trip & IP Response Time totals
  - Sliding-Window Transaction count
  - Sliding-Window Round Trip & IP Response Time totals
- Sum of Squares for variance and standard deviation
  - Round Trip, IP, and SNA Sum of Squares
- Round trip response Time counts by Time Bucket

You configure the bucket maximum values in milli seconds.

Bucket 1	Bucket 2	Bucket 3	Bucket 4	Bucket 5
Transaction count	Transaction count	Transaction count	Transaction count	Transaction count

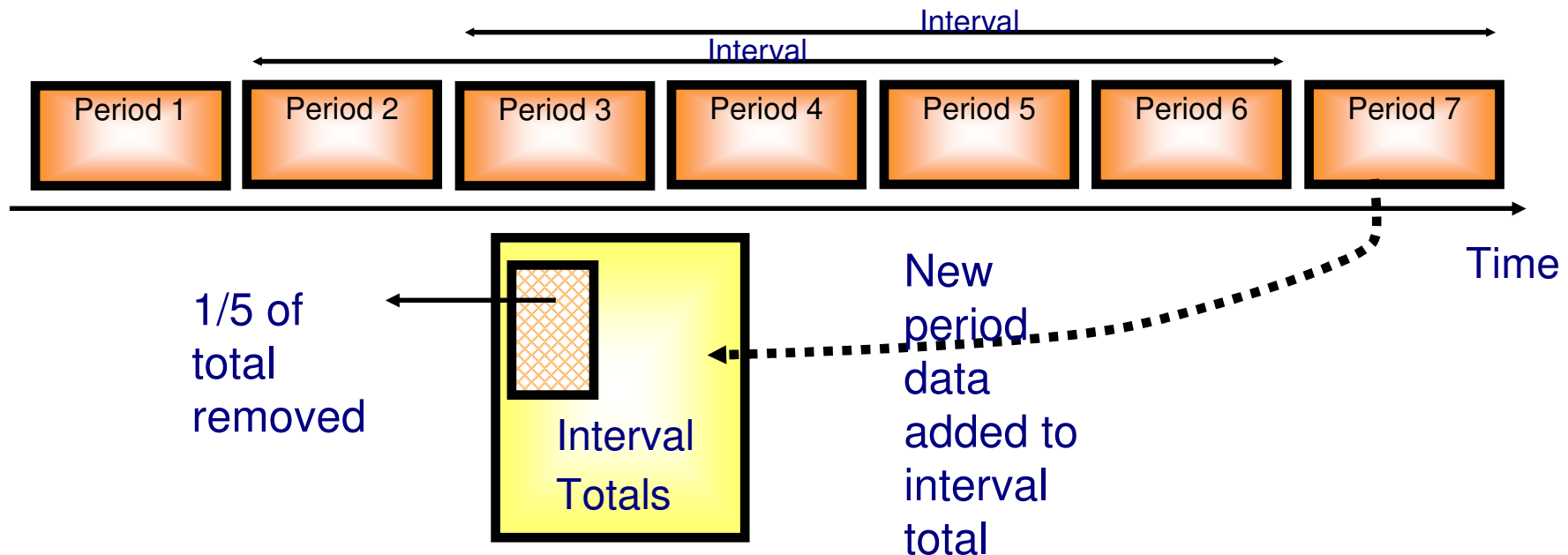0   B1 max   B2 max   B3 max   B4 max   msec

The sliding window - basic principles

Sliding-Window

- ➤A defined interval of time
- ➤The Interval is made up of AVGSAMPMULTIPLIER equal periods of AVGSAMPPERIOD seconds
- ➤Data is ollected by each period
- ➤For an interval of 5 periods... At each period end
  - −1/5 of total interval data removed
  - −New period data added to interval total

Interval

Interval

| Period 1 | Period 2 | Period 3 | Period 4 | Period 5 | Period 6 | Period 7 |

Time

1/5 of total removed

Interval Totals

New period data added to interval total

Sliding window - notes

NOTES

- The data collection process is as follows:
  - During Period 1 time, transaction count and response time data is collected.
  - At the end of Period 1, the Period 1 totals are added to the Sliding-Window totals.
  - The Period totals are reset to zero.

- The cycle repeats itself every period.

- Before new Period data is added to the Sliding-Window totals, the current Sliding-Window totals must be adjusted.

- Calculation method
  - An average period amount is a hypothetical average based on the Sliding-Window total.
  - An average period amount is:

    - (SW total) * (1/n periods)

  - Subtract an average period amount and add the new period actual amount

    - $(SW\ total)_{new} = (SW\ total)_{old} - (Period\ total)_{avg} + (Period\ total)_{new}$
    - $SWtot_{new} = SWtot_{old} - (SWtot_{old}*1/n) + PERtot_{new}$

- Calculations are done at the end of every Period for
  - SW transaction counts
  - SW Round Trip Response Time totals
  - SW IP Response Time totals
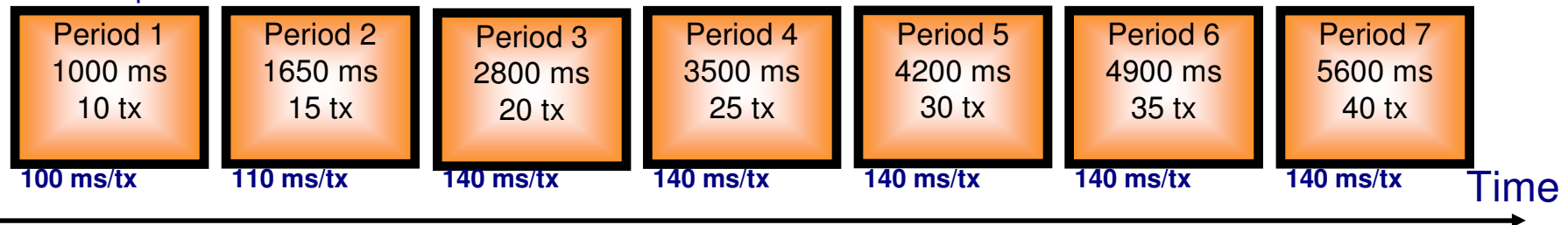
Number of periods per sliding window interval

➢Old period data affects current results

- ►More periods, more impact on current averages
- ►Fewer periods, less impact on current averages
  - –swTotnew = swTotold - (swTotold*1/n) + PerTotnew

- ►Average response time results after 7 periods using different interval sizes
  - – 2 period interval - 139.7 ms/tx
  - – 5 period interval - 137.9 ms/tx
  - –10 period interval - 136.6 ms/tx

Period 1 1000 ms 10 tx	Period 2 1650 ms 15 tx	Period 3 2800 ms 20 tx	Period 4 3500 ms 25 tx	Period 5 4200 ms 30 tx	Period 6 4900 ms 35 tx	Period 7 5600 ms 40 tx
100 ms/tx	**110 ms/tx**	**140 ms/tx**	**140 ms/tx**	**140 ms/tx**	**140 ms/tx**	**140 ms/tx**

Time

➢With few periods, the average period amount removed is larger and the new period data added has a greater impact.

➢Special case Interval definitions.

- ►1 period in an Interval.
  - –100% of the existing interval data is subtracted before the new period data is added. The result is an average for just that interval and the effect of older data is completely ignored.
- ►0 periods in an Interval.
  - –0 indicates that Telnet should include all data equally. The result is a life-of-connection average that is already available. A very large multiplier will have a similar effect.

MONITORGROUP and MONITORMAP

➢ You define one or more monitoring groups to which you map client identifiers via a MONITORMAP statement.

➢ Response time data is collected and maintained per connection

  ► D TCPIP,,TELNET commands for single connections will display results for that single connection

```
BEGINVTAM Block

    MONITORMAP   mongrp_name   client_id


MONITORGROUP   mongrp_name
    AVERAGE/NOAVERAGE
    AVGSAMPMULTIPLIER n
    AVGSAMPPERIOD sec
    BOUNDARY1,BOUNDARY2,BOUNDARY3,BOUNDARY4   msec
    BUCKETS/NOBUCKETS
    DYNAMICDR/NODYNAMICDR
    INCLUDEIP/NOINCLUDEIP
ENDMONITORGROUP
```

```
    MONGROUP:   IG IPGRP1
                    MONGRP1
    PERIOD:        60 MULT:          5
         S/W AVG TOT AVG  SUM R/T     SSQ R/T  ST DEV

         ======= ======= ======== ============ =======
    SNA:     387     567     8501     37955479    1538
    IP:       83      34      521        45917      45
    TOTAL:   470     601     9022     38803058    1544
    COUNT:     3      15
    BUCKET1    BUCKET2    BUCKET3    BUCKET4    BUCKET5
        50        100        200        500     NO LMT
         9          0          1          2          3
```

➢ The response time data can be monitored via D TCPIP,,TELNET commands or via SNMP GET commands that are served by a new TN3270 server SNMP subagent.

**N
O
T
E
S**

➢ **AVERAGE/NOAVERAGE**
➤ Indicates whether or not sliding averages should be calculated.

➢ **AVGSAMPMULTIPLIER n**
➤ Specifies the averaging period multiplier. Default value is 5. The valid range is 0-99999999.

➢ **AVGSAMPPERIOD sec**
➤ Specifies the sampling period for a sliding-window average. Default value of 120 seconds. The valid range is 1-99999999.

➢ **BOUNDARY1, BOUNDARY2, BOUNDARY3, BOUNDARY4 msec**
➤ Defines the upper boundary, in milliseconds, for the bucket. The default values are 50, 75, 100, and 150 milliseconds. The valid range is 0-99999999.

➢ **BUCKETS/NOBUCKETS**
➤ Indicates whether or not time buckets are being used.

➢ **DYNAMICDR/NODYNAMICDR**
➤ Indicates whether or not Telnet should add the Definite Response (DR) request to the outbound TN3270E header if it was not set on by the application. If this option is not chosen, or the client does not support DR, Telnet will use a TIMEMARK to approximate the IP transit time.

➢ **INCLUDEIP/NOINCLUDEIP**
➤ Indicates whether or not Telnet should measure the transit time on the IP side of the connection.

➢ Example:

```
MONITORGROUP   MONGRP1
   DYNAMICDR   INCLUDEIP   AVERAGE BUCKETS
   AVGSAMPPERIOD        60
   AVGSAMPMULTIPLIER    5
   BOUNDARY1    50      BOUNDARY2    75
   BOUNDARY3   100      BOUNDARY4  150
ENDMONITORGROUP

MONITORMAP   MONGRP1   IPGRP1
```

TN3270 response time SNMP subagent

V1R5 *e*

- ➤ Telnet SNMP subagent
  - ► Telnet SNMP subagent runs as a separate task within Telnet

- ➤ TNSACONFIG in TelnetGlobals Block starts the Subagent
  - ► Must be disabled to change any parameter values

- ➤ Network Management Application (SNMP monitor) requests data through SNMP GET requests
  - ► Request goes to z/OS CS SNMP Agent
  - ► Request routed to TN3270 Subagent
  - ► Raw data, by connection, returned
  - ► Data includes unique index to MonitorGroup
- ➤ /usr/lpp/tcpip/samples - mvstn3270.mi2
  - ► Contains SNMPv2 syntax (SMI) for the TN3270 MIB

- ➤ The network management application is responsible for calculating averages, standard deviations, or any other information that can be derived from the MIB data.
  - ► The TN3270 subagent provides data at a connection level. It does not provide any summary data. However, part of the data returned is an index indicating which MONITORGROUP is mapped to the connection. With this information, a network management application could develop summary information by MONITORGROUP.

Configuring the TN3270 SNMP subagent

V1R5 *e*

➤ Statement in TelnetGlobals Block

TNSACONFIG
- **AGENT port_num**
- **CACHETIME cache_time**
- **COMMUNITY comm_string**
- **ENABLED/DISABLED**
- **TNSATRACE/NOTNSATRACE**

➤ Example

```
TELNETGLOBALS
    TNSACONFIG
        AGENT 161
        COMMUNITY public
        CACHETIME 120
        ENABLED
ENDTELNETGLOBALS
```

Telnet subagent - notes

N O T E S

➢AGENT port_num

▶A port number in the range of 1 and 65535 used in establishing communication with the SNMP agent. The default value is 161. For the Telnet SNMP subagent to communicate with the z/OS CS SNMP agent, the port number specified must match the port number specified (or defaulted) on the -p parameter when the SNMP agent is started. See "OSNMPD parameters" in the SNMP chapter for a description of how to specify the port when the SNMP agent is started.

➢CACHETIME cache_time

▶Amount of time in seconds to elapse before rebuilding the MIB object tables. The default value is 30 seconds. The valid range is 0-99999999.

➢COMMUNITY comm_string

▶A character string of 1 to 32 characters used as the community name (or password) in establishing contact with the SNMP agent. The default value is "public". It is not converted to uppercase by profile processing. It cannot contain any imbedded white space or control characters (such as blank, tab, end of line, or end of file) and cannot contain any imbedded semicolons (semicolons are treated as comment delimiters). For the Telnet SNMP subagent to communicate with the z/OS CS SNMP agent, the community name specified (or defaulted) on the COMMUNITY keyword must match one that is defined in the PW.SRC or SNMPD.CONF data set used by the SNMP agent or specified (or defaulted) on the -c parameter when the SNMP agent is started.

➢ENABLED/**DISABLED**

▶DISABLED specifies that you do not require any of the SNMP MIB data supported by the Telnet subagent. By default, the Telnet SNMP subagent is not started during Telnet initialization. If specified using OBEYFILE, this statement indicates that the currently active Telnet subagent task should be terminated.

➢TNSATRACE/**NOTNSATRACE**

▶TNSATRACE will generate trace points throughout Telnet subagent processing in addition to tracing data passed between the Telnet subagent and the agent, Telnet, and TCP/IP stack. The trace data is written to the syslog daemon.

TN3270 Server in CS z/OS V1R6

IBM ®

TN3270 Server in its own address space in z/OS V1R6 for improved management

V1R6 e ™

Remote terminal access

➢ Currently TN3270 Server runs as a subtask of the IBM TCPIP stack address space

➢ In z/OS V1R6, you will have a choice:
  ► Run the TN3270 server as a separately started address space from TCPIP
  ► Continue to run TN3270 server as a subtask of the TCPIP address space

➢ Reasons why an installation may want to run the TN3270 server in a separate address space:
  ► Allows for prioritzation of TCPIP address space vs TN3270 server
  ► Much less likely for TN3270 server failure to cause a total TCPIP failure
  ► Allow for easier problem diagnosis for both TCPIP and TN3270
  ► Easier controls for starting and stopping the server

➢ Considerations
  ► Profile statements are the same (minor considerations) and must be in a file separate from TCPIP
  ► Commands are the same but must be directed to the intended TN3270 procedure name
  ► Multiple TCPIP stacks supported
    – One server per stack (affinity)
    – One server associated with all stacks (Generic Server)
  ► Multiple TN3270 server address spaces supported
    – Max 8 TN3270 server address spaces per LPAR
    – Only one can activate the TN3270 response time SNMP subagent in a stack
      ◆ Must have stack affinity to that stack
      ◆ The first one started with stack affinity and TNSACONFIG enabled activates the SNMP subagent
  ► Must run TN3270 server with affinity for the following functions
    – TN3270 response time SNMP subagent
    – WLM function
  ► Requirements
    – Separate start up JCL. Sample is provided.

z/OS LPAR

TN3270 server | SNA appli-cation

TCP/IP address space | VTAM address space

Multiple TN3270 server address spaces

V1R6
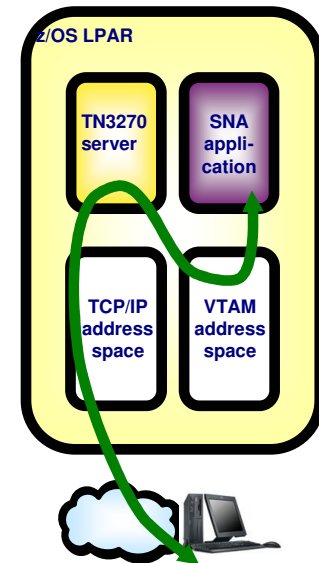
Per TN3270 server address space:
- ▸ Define JCL procedure - sample in hlq.SEZAINST(EZBTNPRC)
- ▸ Define started task RACF profile (assign started task user ID)
  - ▪ Started task userID must be UID 0 or permitted to BPX.SUPERUSER and have OMVS segment
- ▸ Define TN3270 server definitions
  - ▪ Same as prior to z/OS V1R6
  - ▪ One new global option: TCPIPJOBNAME for stack-affinity
  - ▪ Each server has its own set of definitions
    - ◆ Different key ring files per server address space
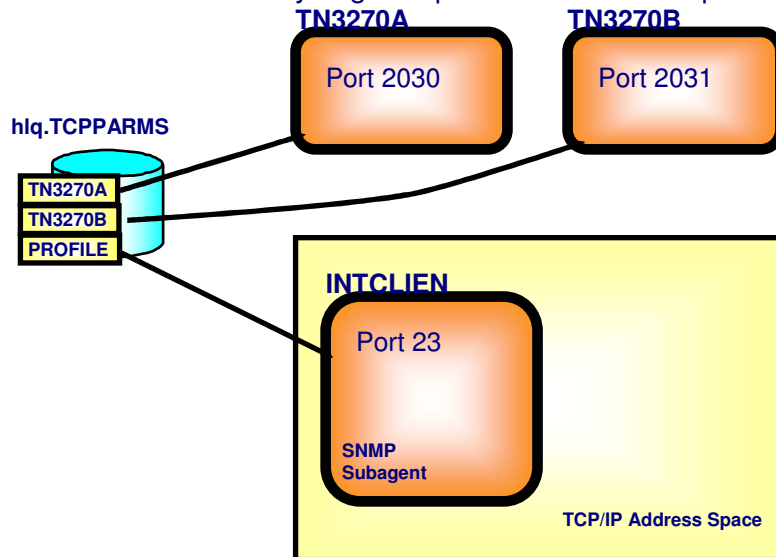
```
//TN3270A  PROC PARMS='CTRACE(CTIEZBTN)'
//TN3270   EXEC PGM=EZBTNINI,REGION=0M,PARM='&PARMS'
//*
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//*
//*TNDBCSCN DD DISP=SHR,DSN=TCPIP.SEZAINST(TNDBCSCN)
//*TNDBCSXL DD DISP=SHR,DSN=TCPIP.SEZAXLD2
//*TNDBCSER DD SYSOUT=*
//*
//PROFILE  DD DSN=USER1.TCPCS.TCPPARMS(TN3270A),DISP=SHR
//SYSTCPD  DD DSN=USER1.TCPCS.TCPPARMS(TCPDATA),DISP=SHR
```

TN3270A **TN3270B**

Port 2030 Port 2031

hlq.TCPPARMS

TN3270A
TN3270B
PROFILE

INTCLIEN

Port 23

SNMP Subagent

TCP/IP Address Space

Normal MVS console TN3270 display commands - directing them to selected server address space name:

```
D TCPIP,TN3270A,T,CONN,CONN=24D
EZZ6065I TELNET CONNECTION DISPLAY 531
  CONNECTED: 12:31:28  06/28/2004  STATUS: SESSION PENDING
  CLIENT IDENTIFIER FOR CONN: 0000024D   SECLABEL: **N/A**
    CLIENTAUTH USERID: **N/A**
    HOSTNAME: NO HOSTNAME
    CLNTIP..PORT: ::FFFF:9.65.211.157..1484
    DESTIP..PORT: ::FFFF:9.42.105.45..2030
    LINKNAME: QDIO4
  PORT:  2030 QUAL: NONE
    AFFINITY: TCPCS
    STATUS: ACTIVE  BASIC        ACCESS: NON-SECURE
  PROTOCOL: TN3270E            DEVICETYPE: IBM-3278-3-E
    TYPE: TERMINAL GENERIC
    OPTIONS: ETET----   3270E FUNCTIONS: BSR----
                        NEWENV FUNCTIONS: --
  LUNAME: TCPABC50
[lines deleted]
```

PPT entries and trace considerations

V1R6

> The latest default MVS Program Property Table (PPT) contains the Telnet procedure. If not using the latest PPT, add a PPT entry into your own table.

```
PPT PGMNAME(EZBTNINI)     PPT Program Name
    NOCANCEL              Non-Cancellable
    KEY(6)                KEY(6)
    NOSWAP                Non-Swappable
    PRIV                  Privileged
    SYST                  System Task (not timed)
```

> These settings are the same as the TCP/IP stack.

> PRIV and SYST each cause the started job to be assigned to the SYSSTC service class. The priority can be changed by assigning the job name to another service class within the STC subsystem.

> Trace functions similar to stack component trace.
> - The trace component is SYSTCPIP. The same as the stack.
> - Tracing can be specified for common services and Telnet.

> Changes to component trace in Telnet.
> - New component trace options dataset sample for Telnet - CTIEZBTN.
> - The default trace options dataset is CTIEZB00
> - Trace data stored in Telnet private storage, not a dataspace.

General considerations

> TCP/IP affinity is required to obtain stack Jobname & Hostname for the following functions.
>> Telnet SNMP Subagent activation - Must direct registration by stack jobname.
>> WLM Registration - Must specify stack hostname during registration.
>> SMF Hostname - Stack hostname used.

> Command processing - The procedure name must be specified to route commands to Telnet. Otherwise the command is routed to the default TCPIP stack.
>> D TCPIP,TELNET1,T,PROFILE

> In a CINET environment, Telnet connections can be supported by different stacks.
>> Netstat Telnet displays show only connections on the stack where the command was issued.

> SNMP Subagent Limitation - Agent/subagent connection requires a one-to-one matchup.
>> Any particular agent can support only one Telnet subagent, including Telnet as part of the stack.

> SMF address space name - Will be the name of the Telnet procedure, not the stack.
>> SMF 118 Started Task name (SMFTNTST)
>> SMF 119 Address Space Name of the Writer (SMF119TI_ASName)

> Can not change IPv4/IPv6 or INET/CINET Environments while running - Unpredictable results.
>> New port activations will fail if environment change is detected.
>> Recommend stop Telnet, change environment, restart Telnet.
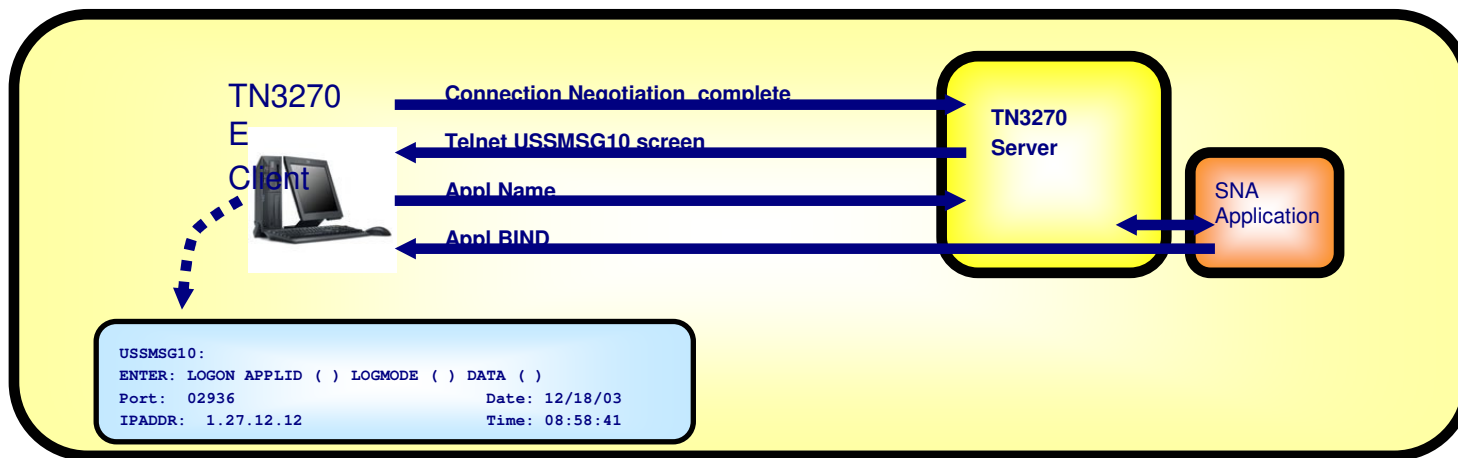
> INTCLIEN Port Reservation - Valid only for Telnet as part of the stack.
>> If Telnet is running as its own procedure and tries to listen on a reserved port, the BIND will fail.
>> Specify the Telnet jobname instead.

> Multilevel Security compliance - Telnet is not compliant when running as its own procedure.
>> You must run Telnet as part of the stack for Multilevel Security compliance.

SCS-mode USS table support

V1R6 🅴™

> Support for USSMSG10 screen in SNA Character Stream (SCS) format
>> - VTAM Unformatted System Services supports two formats of a USSMSG10 screens:
>>> ► 3270 Data format
>>> ► SNA Character Stream (SCS) format
>>
>> - The TCP/IP TN3270 server has sofar only supported USSMSG10 screens in 3270 data stream format
>>
>> - This release adds support for USSMSG10 screens in SCS format
>>> ► Only TN3270E clients support SCS format
>>>> – SCS data flows as SSCP-LU data
>>> ► TN3270 connections continue to use 3270 Data format

TN3270 E Client

Connection Negotiation complete

Telnet USSMSG10 screen

Appl Name

Appl BIND

TN3270 Server

SNA Application

```
USSMSG10:
ENTER: LOGON APPLID ( ) LOGMODE ( ) DATA ( )
Port:  02936                    Date: 12/18/03
IPADDR:  1.27.12.12             Time: 08:58:41
```

128 000 TN3270 connections per port

V1R6

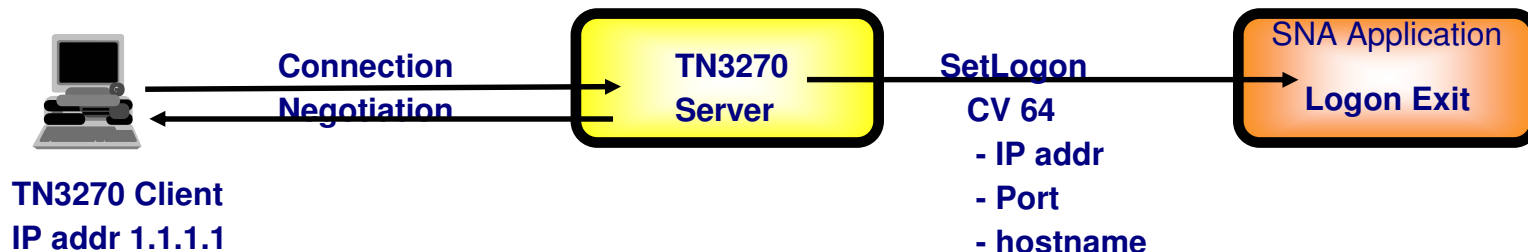➢Support for up to 128 000 connections per TN3270 server port

➢Background
- Unix System Services allows 64K sockets per task.
- Telnet starts one task per port.
- Maximum number of Telnet connections is 64K per port.

➢Solution
- Unix System Services has raised the limit to 128K.
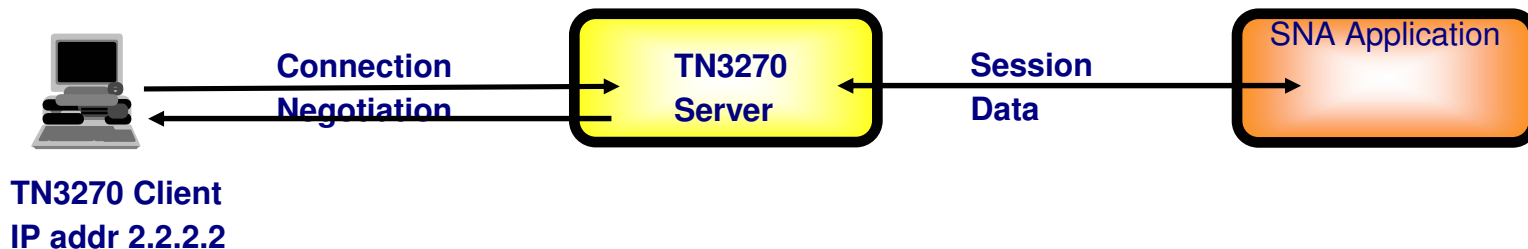- Telnet was changed to use this limit for each port.

Connection takeover when client IP address changes

V1R6 *e* ™

➢ Telnet session initiation uses SetLogon to pass client information to VTAM and the APPL
  - ► VTAM displays include the client's IP address.
  - ► Some applications use the client's IP address for billing or other uses.

```
┌─────────┐   Connection    ┌──────────┐   SetLogon     ┌─────────────────┐
│ [image] │ ──────────────► │ TN3270   │ ─────────────► │ SNA Application │
│         │   Negotiation   │ Server   │   CV 64        │                 │
└─────────┘ ◄────────────── └──────────┘                │   Logon Exit    │
                                          - IP addr      └─────────────────┘
  TN3270 Client                           - Port
  IP addr 1.1.1.1                         - hostname
```

➢ Connection Takeover can be from a different IP address.

```
┌─────────┐   Connection    ┌──────────┐   Session      ┌─────────────────┐
│ [image] │ ──────────────► │ TN3270   │ ◄────────────  │ SNA Application │
│         │   Negotiation   │ Server   │   Data    ───► │                 │
└─────────┘ ◄────────────── └──────────┘                └─────────────────┘
  TN3270 Client
  IP addr 2.2.2.2
```

➢ VTAM and the Application Logon exit can accept only one SetLogon.
  - ► VTAM display is wrong.
  - ► Application has wrong IP address.

Control if change of IP address is allowed during takeover processing

V1R6

- Allow multiple SetLogon macro calls from Telnet to VTAM.
  - At each takeover Telnet will send a new SetLogon with updated CV64 information.
    - Client IP address, Port, Hostname

- Local VTAM display is always correct.

- The Application logon exit still receives only one SetLogon per session.
  - Indicate the session can potentially be taken over
    - CV64 subvector 81 flag '80'x
  - Require the takeover client to have the same IP address
    - Control with a new parameter on TKOSPECLURECON/TKOGENLURECON statements

- SAMEIPADDR requires the taker to have the same IP address as the target.
  - If not same IP addr - "102A Takeover attempted with a different IP address."

```
                         |--NOKEEPONTMRESET--|    |--NOSAMEIPADDR--|
>>---TKOSPECLURECON---sec-+-----------------+--+---------------+----->><
                         |--KEEPONTMRESET----|    |--SAMEIPADDR----|


                         |--NOKEEPONTMRESET--|    |--NOSAMEIPADDR--|
>>---TKOGENLURECON----sec-+-----------------+--+---------------+----->><
                         |--KEEPONTMRESET----|    |--SAMEIPADDR----|
```

SAMEIPADDR - notes

NOTES

- ➢Minor migration issue.
  - ►The local VTAM displays will now always show the correct IP information.

- ➢All other features must be specified or accessed to make a difference.
  - ►SAMEIPADDR
  - ►Takeover capable flag in the CV64

- ➢SAMEIPADDR function was added as an APAR in V1R4.
  - ►PQ73390
- ➢Function is already part of V1R5.

Trademarks, Copyrights, and Disclaimers

e-business

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	CICS	IMS	MQSeries	Tivoli
IBM(logo)	Cloudscape	Informix	OS/390	WebSphere
e(logo)business	DB2	iSeries	OS/400	xSeries
AIX	DB2 Universal Database	Lotus	pSeries	zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

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

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

© Copyright International Business Machines Corporation 2005. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.