IBM Software Group – Enterprise Networking Solutions

What's new with z/OS CS TN3270?

Alfred B Christensen – alfredch@us.ibm.com
Raleigh, NC, US
February 17, 2010

Trademarks, notices, and disclaimers

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

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM (logo)®
- IBM®
- IMS
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x
- System z
- System z9
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

- 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 trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel Inside (logos), MMX and Pentium 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 trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an “as is” basis, without warranty of any kind.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Refer to www.ibm.com/legal/us for further legal information.

Agenda

I use the terms TN3270 server and Telnet server interchangeably throughout this session.

- A few (three) selected TN3270 Server enhancements in z/OS V1R8 CS
- TN3270 Server in z/OS V1R9 CS
  - AT-TLS Enabled TN3270 Server
  - Management of non-Current TN3270 Server Profiles
  - Use of APPLDATA to Provide Netstat Visbility into TN3270 server options
  - TN3270 Server MUST now run in its own Address Space
- TN3270 Server in z/OS V1R10 CS
  - Sysplex LU name server
- TN3270 Server in z/OS V1R11 CS
  - TSO reconnect enhancements
- TN3270 Server in z/OS V1R12 CS
  - Shared ACB support
  - IP management information through a relay-mode session manager

Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an "as is" basis, without warranty of any kind.

z/OS CS TN3270 server release overview

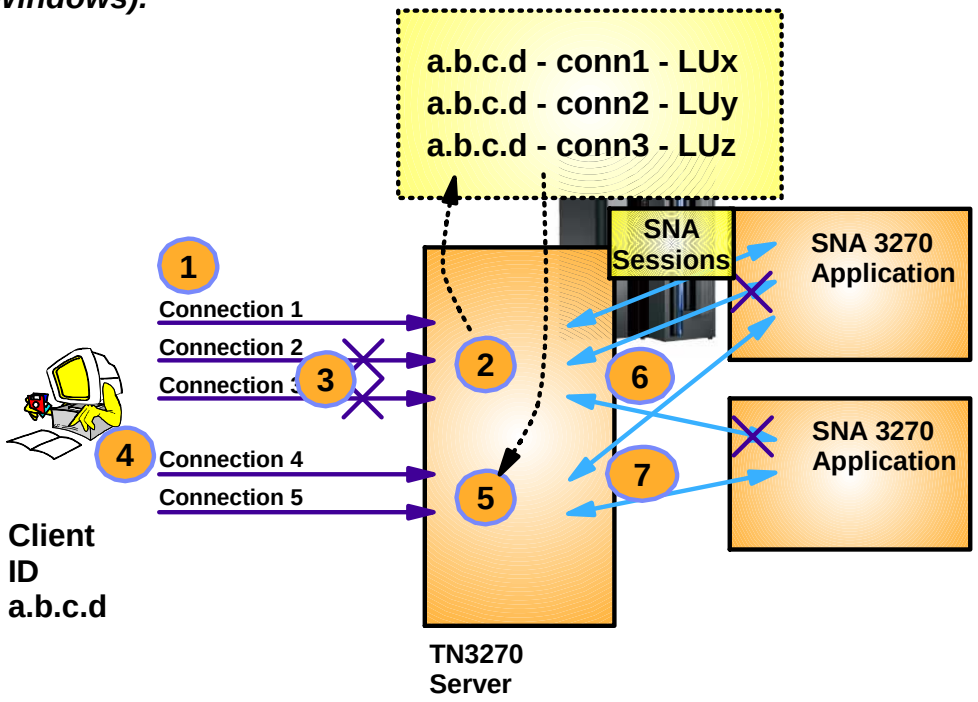
- z/OS V1R5
  - IPv6 Support
  - Generic Connection Takeover
  - Unlock Keyboard Control
  - IP Range Specification
  - Network Access Control
  - Performance monitoring
- z/OS V1R6
  - TN3270 server in a separate address space
  - SCS-mode formatted USS table support
  - Improved control of takeover function
  - 128,000 connections per TN3270 server port support
- z/OS V1R7
  - Option to control use of SSL V2 or not
  - AES encryption support
- z/OS V1R8
  - ✓ Check Client Connection status
  - Use the LU Exit to assign USS tables
  - ✓ Allow System Symbolics in USS tables
  - Add a timer for Queued Sessions
  - ✓ New ways to collect Performance Monitoring Data
  - Obsolete statements
- z/OS V1R9:
  - AT-TLS enable the TN3270 server
  - Add TN3270-specific application data to be included in netstat reports
  - Managing non-current profiles
  - 512,000 connections per TN3270 server port support
- z/OS V1R10:
  - Sysplex LU name server
- z/OS V1R11:
  - Improved TSO LOGON reconnect support
- z/OS V1R12:
  - Shared ACB support for improved performance and reduced ECSA storage use
  - IP management information through a relay-mode session manager

What's New with z/OS Communications Server TN3270?

A few (three) selected TN3270 Server enhancements in z/OS V1R8 CS

CheckClientConn: cleaning up "dead" connections without sending timemarks to the whole world

TN3270 connection clean-up technology if more TN3270 connections are used in parallel from the same source IP address (such as, multiple emulator windows running on Windows).



- "Just-in-time, selected timemark processing"
  - Avoids CPU and network overhead of repetitive timemark processing of all connections
- Cleans up all connections from same workstation when first connection is re-established
  - No SNA session takeover, but all SNA sessions from same source IP address cleaned up
- Be careful not to use this function if you have a large number of connections with the same remote IP address.
  - Use [maxconns] to limit
  - Default is 50
  - Beware of proxy servers !!!

```
CheckClientConn  sec  [maxconns]
```

CheckClientConn is only supported if the TN3270 server runs in a separate address space in z/OS V1R8

MVS system symbols in TN3270 server USS table

- MVS system symbols are defined in your IEASYMnn PARMLIB member
- Specify LUNAME or SCAN on the message as you would for @@ string substitution.
  - **USSMSG10 USSMSG MSG=10,BUFFER=(M1,SCAN)**
- Telnet will now also check for System Symbols in the message string.
  - **&SYSNAME.**
  - **&SYSR1.**
  - **…**

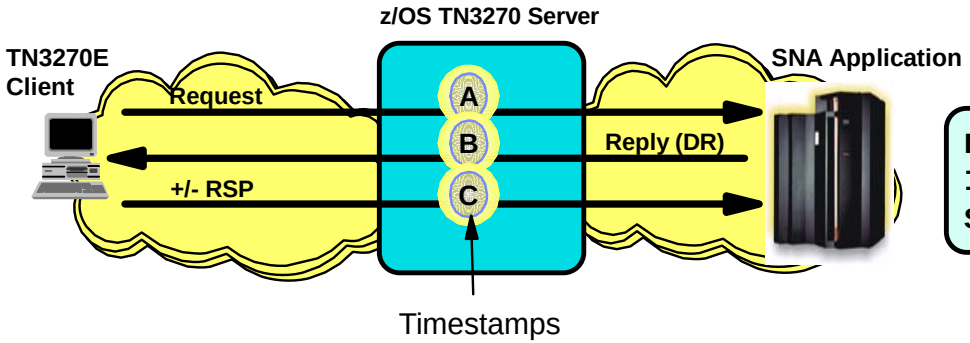
```
USSMSG10: Enter: LOGON APPLID() LOGMODE() DATA()

Port:   52381            Date: 28/07/09    LU:    TCPABC80
IPADDR: 9.65.255.62      Time: 09:20:28    Sense:
USSABC - This is the TCPCS Stack on MVS098 - OS1B0
```

USS Table definition source

```
*
         DC    X'11'                  SET BUFFER ADDRESS ORDER
         DC    X'C5C0'                ROW 5 COLUMN 2
         DC    X'1D'                  START FIELD
         DC    X'F0'                  PROTECT SKIP NORMAL
         DC    C'USSABC - This is the TCPCS Stack on &&SYSNAME.'
         DC    C' - &&SYSR1.'
*
```

Note the extra '&' on the symbol name. This is necessary for the assembler to produce the right substitution.

TN3270 server response time monitoring



Response times

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

- **Two sets of data collected:**
  - Life-of-connection data for life-of-connection averages
  - Life-of-session data for life-of-session averages
- **Data being collected:**
  - Transaction count
  - Round trip & IP response time totals
  - Sum of Squares for round trip, IP, and SNA
  - Transaction counts by time bucket
- **Controlled by means of:**
  - TN3270 server profile statements MONITORGROUP and MONITORMAP

- **For life-of-connection, sliding window data for sliding window averages is also collected**
  - Period transaction count
  - Period round trip & IP response time totals
  - Sliding window transaction count
  - Sliding window round trip & IP response time totals
- **Reporting mechanisms:**
  - SNMP MIBs via a TN3270 server SNMP subagent
  - MVS Console displays
  - NMI (EZBNMIFR) callable management API
  - TN3270 server end-of-session SMF record (SMF119 subtype 21)

An example of using the TN3270 server response time monitor

```
MonitorGroup MONGRP1
             Average              ; Collect sliding averages
             Buckets              ; Use time buckets
             DynamicDR            ; Add DR request if not there
             IncludeIP            ; Include IP response time
             AvgSampPeriod 120    ; Sample every 120 seconds
             AvgSampMultiplier 5  ; Averaging period multiplier
             Boundary1 50         ; Bucket 1: 0 to 50 Msec
             Boundary2 100        ; Bucket 2: 50 to 100 Msec
             Boundary3 200        ; Bucket 3: 100 to 200 Msec
             Boundary4 500        ; Bucket 4: 200 to 500 msec
                                  ; Bucket 5: above 500 msec
EndMonitorGroup
MonitorMap  MONGRP1 IPaddr,9.65.255.62
```

- A Monitor group definition in the TN3270 server profile.
  - This can be created ahead of time.
  - You can have multiple of these with different options.
- When you need to start monitoring, do an OBEYFILE with your TN3270 profile and include a MonitorMap statement that maps the monitor group to one or more client identifiers

```
D TCPIP,TN3270A,TELNET,CONNECTION,PORT=23,LUNAME=TCPABC80,DETAIL
```

```
. . . . .
MONGROUP:   IP ::FFFF:9.65.255.62
                  MONGRP1                        --------
  PERIOD:       120 MULT:         5
        S/W AVG LOC AVG  SUM R/T       SSQ R/T  ST DEV
        ======= ======= ======== ============ =======
  SNA:        59     109     3366            0     227
  IP:         34      33     1050            0       5
  TOTAL:      93     142     4416            0     226
  COUNT:      14      31
  BUCKET1    BUCKET2    BUCKET3    BUCKET4    BUCKET5
       50         100        200        500     NO LMT
       18           4          5          1          3
. . . . .
```

- To view the collected response time data, the simplest way is to issue a console display command as shown in this example
- Various network management products have implemented support for capturing and reporting the TN3270 server response time data

What's New with z/OS Communications Server TN3270?

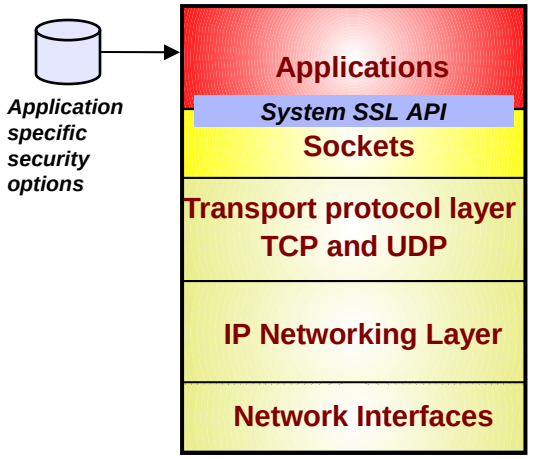
TN3270 Server in z/OS V1R9 CS
AT-TLS Enabled TN3270 Server

SSL/TLS enabling applications on z/OS - technology choices after AT-TLS was introduced in z/OS V1R7

- **SSL/TLS support can since z/OS V1R7 be implemented using one of two methods on z/OS:**

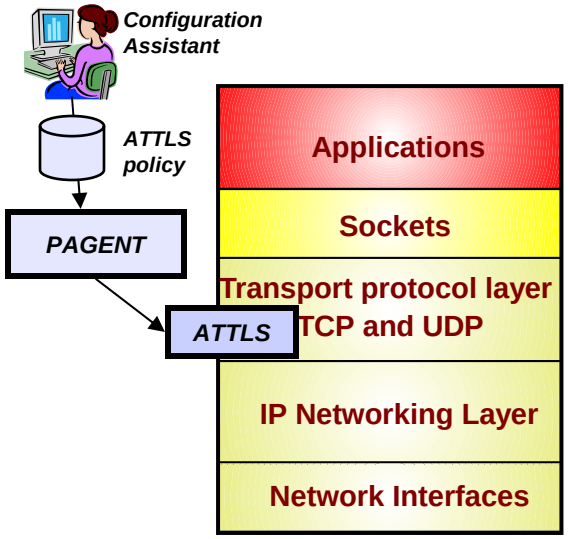
1. *Native System SSL use:*

- Define appropriate application-specific configurations to specify SSL/TLS options, such as key-ring, cipher suites, application-specific security options, etc.
- Replace selected socket calls with calls to system SSL (C/C++/Java only)



2. *AT-TLS:*

- Common SSL/TLS configuration for all applications through an AT-TLS policy (managed by the Policy agent)
- Use optimized SSL/TLS code within the TCP/IP stack that interfaces to system SSL to implement the SSL/TLS functions
- In most cases SSL/TLS support can be added without application changes
- No programming language restrictions (except Pascal)



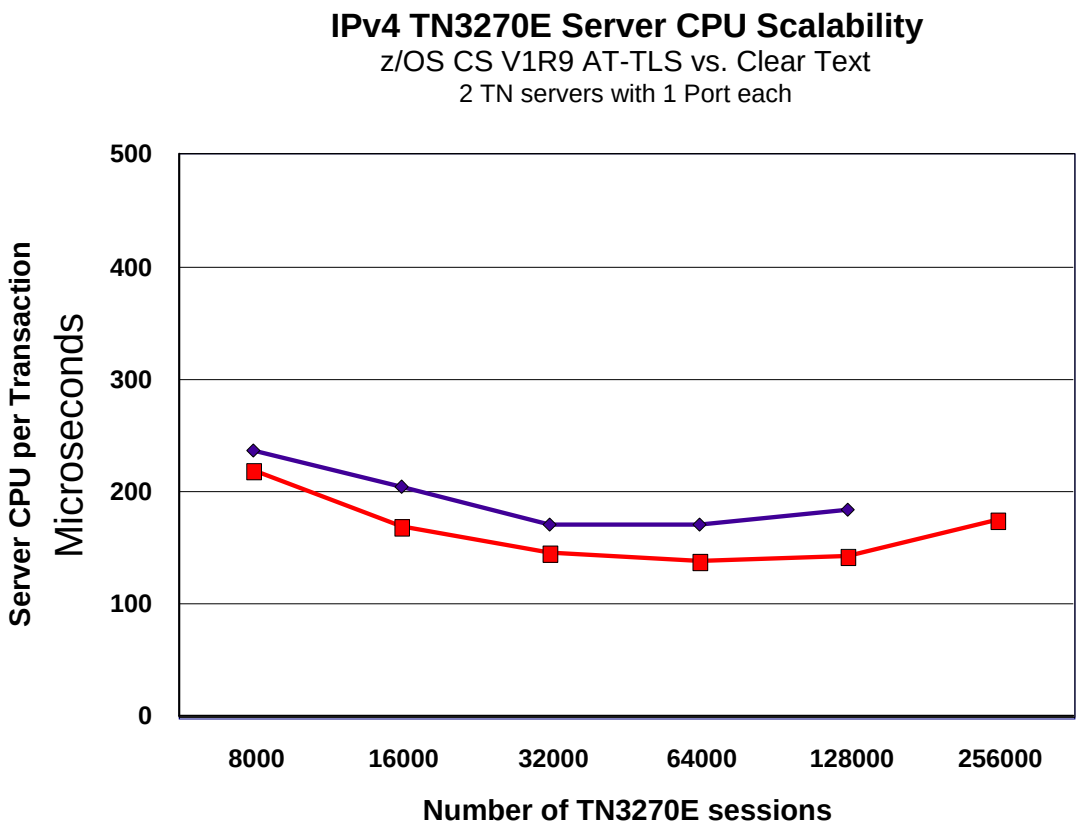
Why use AT-TLS for TN3270?

- **TN3270 can be set up to use native System SSL or AT-TLS**
- **Using AT-TLS has several advantages:**
  - AT-TLS provides SSL/TLS features above and beyond what most SSL/TLS applications choose to support - such as, support for Certificate Revocation Lists (CRLs), multiple key-rings per server, optional use of system SSL cache, etc.
  - AT-TLS uses an optimized SSL/TLS infrastructure that in most cases performs better than when SSL/TLS is implemented directly in the applications
  - Support of new SSL/TLS functions, such as new cipher-suites, can be added without application changes and without changes to application-specific configuration options:
    - New functions are added to AT-TLS in z/OS V1R11 - such as support for TLSv1.1
    - Addressing FIPS 140-2 requirements
  - Allows SSL/TLS-enabling non-C sockets applications on z/OS, such as CICS Sockets, Assembler- and Callable sockets, etc.

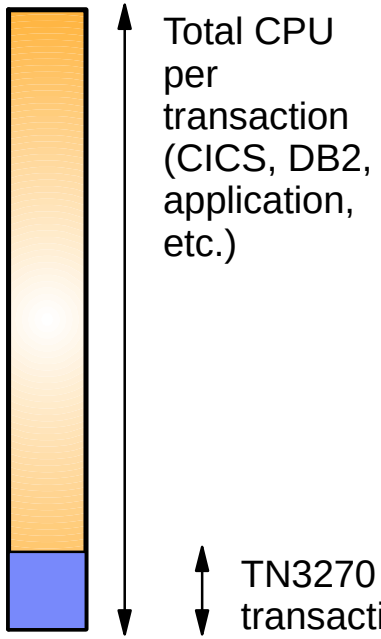
We want you to use AT-TLS !!

Not (just) because Uncle Sam tells you to, but because it is the smart thing to do!

z/OS V1R9 Communications Server TN3270E AT-TLS Security Performance (TN3270 Server, Steady State, CPU per Transaction)



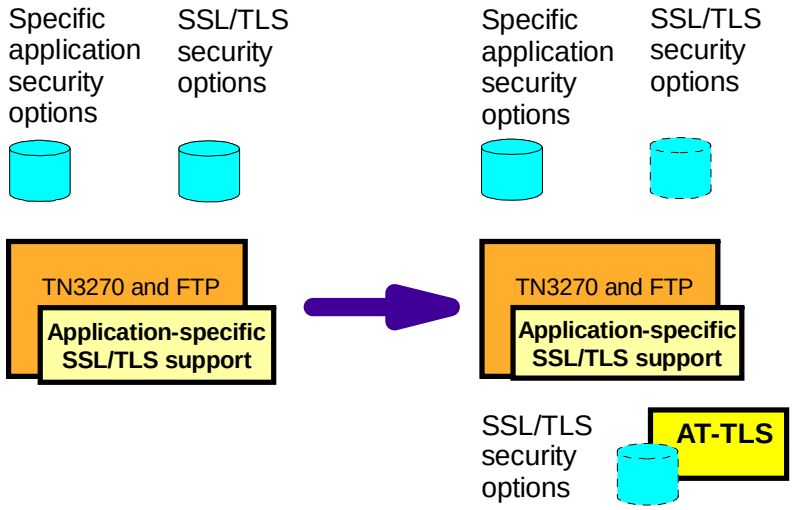
TN3270 server and application server: 4-way 2094-S38



- The TN3270 server CPU portion of the total CPU usage per transaction is very small.
- If you increase the TN3270 server CPU usage with 20%, the total transaction percentage CPU increase is significantly lower.

3DES and SHA
100 bytes in/800 bytes out
Think time 30 seconds

Migrating the TN3270 server to AT-TLS



- **A TN3270 server option to indicate use of AT-TLS instead of the TN3270 server's own system SSL calls is supported:**
  - TTLSPORT
    - CONNTYPE retains its current meaning for a TTLSPORT
- **When TTLSPORT is used for a TN3270 server port:**
  - The TN3270 server becomes an AT-TLS controlling and AT-TLS aware application
  - All the TN3270-specific security options will continue to impact how TN3270 operates
  - Any TN3270 server SSL/TLS security options will be ignored.
    - Matching AT-TLS policies need to be defined before enabling AT-TLS support for the TN3270 server

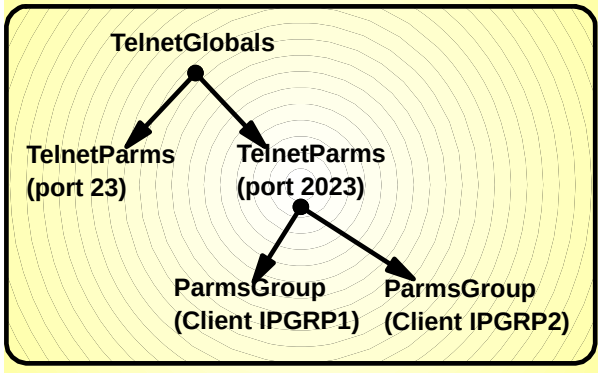
- **TN3270-specific security options:**
  - SECUREPORT (use of this option will indicate to TN3270 that it is to use its existing application-specific SSL/TLS support, and not AT-TLS for the specified port number)
  - CONNTYPE
    - SECURE
    - NEGTSECURE
    - ANY
    - BASIC
  - EXPRESSLOGON
  - RESTRICTAPPL CERTAUTH
- **TN3270 SSL/TLS security options**
  - KEYRING
  - CRLLDAPSERVER
  - CLIENTAUTH
    - SSLCERT
    - SAFCERT
  - ENCRYPTION
  - SSLTIMEOUT
  - SSLV2/SSLNOV2

How to migrate existing TN3270 server SSL/TLS definitions to AT-TLS definitions

TN3270 profile statement	AT-TLS equivalent definition	AT-TLS policy statement
CLIENTAUTH NONE	HandShakeRole Server	TTLSConnectionAction or TTLSEnvironmentAction
CLIENTAUTH SSLCERT	HandshakeRole ServerWithClientAuth and ClientAuthType Required	TTLSConnectionAction or TTLSEnvironmentAction / TTLSEnvironmentAdvancedParms within TTLSEnvironmentAction
CLIENTAUTH SAFCERT	HandshakeRole ServerWithClientAuth and ClientAuthType SAFCHECK	TTLSConnectionAction or TTLSEnvironmentAction / TTLSEnvironmentAdvancedParms within TTLSEnvironmentAction
CRLLDAPSERVER	GSK_LDAP_Server and GSK_LDAP_Server_Port	TTLSGskLdapParms within TTLSEnvironmentAction
ENCRYPTION	TTLSCipherParms	TTLSConnectionAction or TTLSEnvironmentAction
KEYRING	Keyring	TTLSKeyRingParms within TTLSEnvironmentAction
SSLv2	SSLv2	TTLSEnvironmentAdvancedParms within TTLSEnvironmentAction or TTLSConnectionAdvancedParms within TTLSConnectionAction
SSLTIMEOUT	HandshakeTimeout	TTLSEnvironmentAdvancedParms within TTLSEnvironmentAction or TTLSConnectionAdvancedParms within TTLSConnectionAction

AT-TLS enabling TN3270 - mapping of security options to TN3270 client identifiers

TN3270 server configuration options can be specified at multiple levels:



SSL/TLS option	TelnetGlobals	TelnetParms	ParmsGroup
KEYRING	Yes	Yes	
CRLLDAPSERVER	Yes		
CLIENTAUTH	Yes	Yes	**Yes**
ENCRYPTION	Yes	Yes	**Yes**
SSLTIMEOUT	Yes	Yes	**Yes**
SSLV2/NOSSLV2	Yes	Yes	**Yes**

ParmsGroup mapping of SSL/TLS options based on:	TN3270-specific SSL/TLS support	SSL/TLS support through AT-TLS	Comments
User ID or group of user IDs	Only for SSLV2 / NOSSLV2	Not supported	Any impact? Likely not.
Host name or group of host names	Yes	Not supported	Any impact? Assumed to be very low, if any.
Client IP address or group of IP addresses	Yes	Move to an AT-TLS policy rule	AT-TLS will use client IP address/subnet to identify client
Server IP address or group of IP addresses	Yes	Move to an AT-TLS policy rule	AT-TLS will use TN3270 server IP address to identify specific server
Link name or group of link names	Yes	Not supported	Any impact? Assumed to be very low, if any.

Note: Use of PARMSGROUP and PARMSMAP in the TN3270 server configuration for all other configuration options is not impacted by the above discussion.

Use of AT-TLS for TN3270 before and after z/OS V1R9

- **You can use AT-TLS with the TN3270 server in z/OS V1R7 and V1R8**
  - TN3270 server doesn't know anything about AT-TLS
  - Port is defined as a basic port
    - PORT xxx
    - CONNTYPE BASIC
  - Works for implicit mode TN3270 server SSL/TLS
    - AT-TLS can decide based on IP addresses if a connection should be secured or not
  - TN3270 displays do not include any details on SSL/TLS options in use
  - Netstat TTLS report does include details on SSL/TLS options in use

- **Since z/OS V1R9, the TN3270 server has knowledge of AT-TLS**
  - Port is defined as a new TTLSPORT
    - TTLSPort 2025
    - Conntype Any
  - Normal TN3270 server parms mapping can be used to control connection type
  - TN3270 server and netstat displays do include all the details on SSL/TLS options in use

```
TN3270A  0000137C Establsh
  Local Socket:   ::ffff:9.42.105.45..2025
  Foreign Socket: ::ffff:9.65.211.153..2362
  Application Data:  EZBTNSRV TCPABC81          ET TT10A
```

Detailed AT-TLS netstat report for AT-TLS secured TN3270 connection

NETSTAT TTLS CO 000016AF DETAIL TCP TCPCS

```
ConnID: 000016AF
  JobName:       TN3270A
  LocalSocket:   ::ffff:9.42.105.45..2025
  RemoteSocket: ::ffff:9.65.253.59..1266
  SecLevel:      TLS Version 1
  Cipher:        0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
  CertUserID:    N/A
  MapType:       Primary
  FIPS140:       Off
TTLSRule: ABC_TN3270-Server_2025~3
  Priority:        253
  LocalAddr:       All
  LocalPort:       2025
  RemoteAddr:      All
  RemotePortFrom: 1024                RemotePortTo: 65535
  Direction:       Inbound
  TTLSGrpAction:   gAct1
    GroupID:                    00000001
    TTLSEnabled:                On
    Envfile:                    /etc/attls.env
    CtraceClearText:            Off
    Trace:                      6
    SyslogFacility:             Daemon
    SecondaryMap:               Off
    FIPS140:                    Off
```

```
TTLSEnvAction:  eAct1
  EnvironmentUserInstance:    0
  HandshakeRole:              Server
  Keyring:                    TLSRING
  SSLV2:                      Off
  SSLV3:                      On
  TLSV1:                      On
  TLSV1.1:                    On
  ResetCipherTimer:           0
  ApplicationControlled:      Off
  HandshakeTimeout:           10
  TruncatedHMAC:              Off
  ClientMaxSSLFragment:       Off
  ServerMaxSSLFragment:       Off
  ClientHandshakeSNI:         Off
  ServerHandshakeSNI:         Off
  ClientAuthType:             Required
  CertValidationMode:         Any
TTLSConnAction: cAct3~TN3270_2025
  HandshakeRole:              Server
  V3CipherSuites:             2F TLS_RSA_WITH_AES_128_CBC_SHA
                              0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
  CtraceClearText:            Off
  Trace:                      6
  ApplicationControlled:      On
  SecondaryMap:               Off
```

Sample AT-TLS policy for a z/OS TN3270 server on port 2025

```
##
## AT-TLS Policy Agent Configuration file for:
##    Image: MVS098
##    Stack: TCPCS
##
## Created by the IBM Configuration Assistant for z/OS Communications Se
## Version 1 Release 11
## Backing Store = 'USER1.POLICY.BACKSTOR.V1R11.MVS098'
## FTP History:
## 2009-06-19 09:52:56 : user1 to mvs098o.tcp.raleigh.ibm.com
## 2009-05-20 09:50:04 : user1 to mvs098o.tcp.raleigh.ibm.com
##   ATTLS policy rebuilt for R11
##
## TLS default rules: ABC-CICS-Port-3001 (c)| ABC-FTP-server-port-4021 (
##                    ABC-TN3270-Server-2025 (c) |
## End TLS default rules
##
## End of Configuration Assistant information
TTLSRule                          ABC-TN3270-Server-2025~3
{
  LocalAddr                       ALL
  RemoteAddr                      ALL
  LocalPortRangeRef               portR4
  RemotePortRangeRef              portR2
  Direction                       Inbound
  Priority                        253
  TTLSGroupActionRef              gAct1
  TTLSEnvironmentActionRef        eAct1
  TTLSConnectionActionRef         cAct3~ABC-TN3270-2025
}
TTLSGroupAction                   gAct1
{
  TTLSEnabled                     On
}
TTLSEnvironmentAction             eAct1
{
  HandshakeRole                   Server
  EnvironmentUserInstance         0
  TTLSKeyringParmsRef             keyR~MVS098
}
```

```
TTLSConnectionAction              cAct3~ABC-TN3270-2025
{
  HandshakeRole                   Server
  TTLSCipherParmsRef              cipher1~Default_Ciphers
  TTLSConnectionAdvancedParmsRef  cAdv3~ABC-TN3270-2025
  CtraceClearText                 Off
  Trace                           255
}
TTLSConnectionAdvancedParms       cAdv3~ABC-TN3270-2025
{
  ApplicationControlled           On
  SecondaryMap                    Off
}
TTLSKeyringParms                  keyR~MVS098
{
  Keyring                         TLSRING
}
TTLSCipherParms                   cipher1~Default_Ciphers
{
  V3CipherSuites                  TLS_RSA_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DH_DSS_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                  TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                  TLS_RSA_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DH_DSS_WITH_AES_128_CBC_SHA
}
PortRange                         portR2
{
  Port                            1024-65535
}
PortRange                         portR4
{
  Port                            2025
}
```

Use the z/OS CS Configuration Assistant to create this policy !!!!

What's New with z/OS Communications Server TN3270?

TN3270 Server in z/OS V1R9 CS Management of non-Current TN3270 Server Profiles

TN3270 server use of storage for non-current TN3270 server profiles

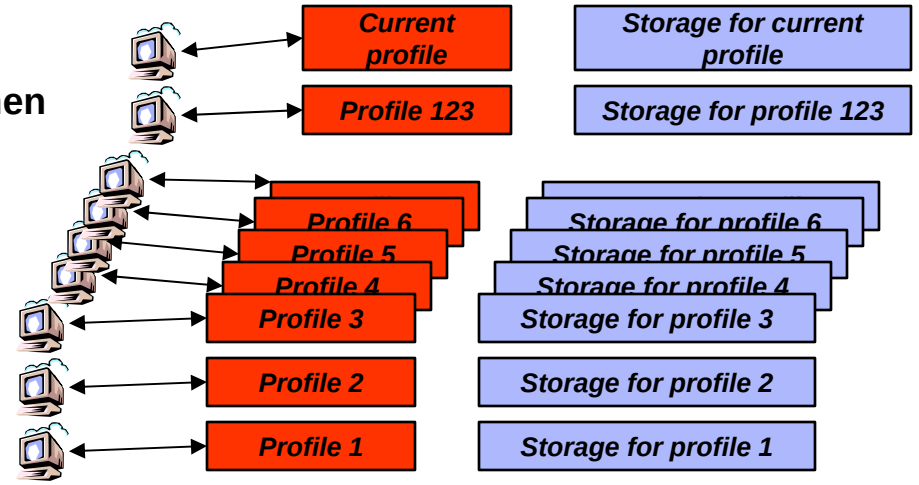
- **V TCPIP,tnproc,OBEYFILE creates a new in-storage TN3270 server profile**
  - New storage for all parameters and mapping statements
  - Existing connections remain associated with same profile

- **Storage for a profile has until z/OS V1R9 been released when:**
  - The profile is no longer the current profile
    - The current profile is the most recently activated profile and the one new connections will be associated with
  - **And** no connections are currently associated with the profile

- **Some installations change their TN3270 server profile frequently**
  - Add new LU names or new mapping statements

- **Connections are associated with a profile even when no SNA session is active**
  - USSMSG10 displayed
  - Solicitor panel displayed

- **Lots of storage may be in-use for old profiles**
  - Storage isn't released until users disconnect their TN3270 connections



TN3270 server PROFILEINACTIVE timer

- **Periodically check connections that are using non-current profiles**
  - ***IF*** there is no SNA session - ***AND*** - there has been no SNA session for at least 'X' amount of time
    - ***THEN***
  - ***DROP*** the connection and by doing so free up storage for a profile if this was the last connection that used that profile
- **More profiles with no connections – storage will be freed**
- **New Telnet parameter statement**
  - ProfileInactive *sec*
    - *Sec* is Time in seconds a connection can stay active without being in an SNA session and is associated with an inactive profile.
    - Telnet is initialized with a value of 1800 (30 minutes) – and this is the default
    - 0 will turn off the function (existing behavior)
  - Set in TelnetGlobals/TelnetParms/Parmsgroup
- **If the default is used, connections using non-current profiles will be dropped after being without an SNA session for at least 30 minutes**
  - To keep your TN3270 server operating as it did before z/OS V1R9, you must specify
    - ProfileInactive 0

What's New with z/OS Communications Server TN3270?

TN3270 Server in z/OS V1R9 CS Use of APPLDATA to Provide Netstat Visibility into TN3270 server options

TN3270 server application data

Bytes	Content	Values
1 to 8	Telnet application identifier	EZBTNSRV
10 to 17	LU name	
19 to 26	SNA application name	
28	Connection mode	E: TN3270E 3: TN3270 L: Line mode D: DBCS
29	Emulator type	T: Terminal P: Printer
31	Security level	B: Basic S: Secure T: AT-TLS
32 to 33	Security protocol	11: TLSv1.1 T1: TLSv1 S3: SSLv3 S2: SSLv2
34 to 35	Cipher	2-digit SSL/TLS cipher code

```
TN3270A  00000553 Establsh
  Local Socket:   ::ffff:9.42.105.45..2025
  Foreign Socket: ::ffff:9.65.255.62..61585
  Application Data:  EZBTNSRV TCPABC81          ET TT135
                     ----+----0----+----0----+----0----+----0
                             1         2         3         4
```

APPLDATA is available through:

- **Netstat**
- **SMF records**
- **NMI interface**

What you can do with the TN3270 server APPLDATA

- APPLDATA can be used as a filter on selected netstat reports
- To get a netstat report of all TN3270 connections with all TN3270 server port numbers:
  - ALLCONN APPLDATA TCP TCPCS (APPLD EZBTNSRV*
- To get a netstat report of all TN3270 connections that are secured with ATTLS:
  - ALLCONN APPLDATA TCP TCPCS (APPLD EZBTNSRV??????????????????????T*
- Based on the APPLDATA information, it is relatively easy to build a TSO/ISPF application to monitor TN3270 server activity

```
*-------------------- MVS TCP/IP NETSTAT CS z/OS V1R11 ------- Row 1 to 4 of 4
Command ===>                                                  Scroll ===> PAGE

TN3270 server overview

Line command: S Connection summary, O TN3270 Profile, T TTLS report for
              secure conn,  P Ping remote IP address, and D Drop connection

          Socket   TN3270                      TN-Conn T Sec   Sec   Cipher
S ConnID  status   ASName   LU-Name  ApplName  Mode    P Type  Level Suite
- ------ -------- -------- -------- -------- ------- - ----- ----- ------------
  000553 Establsh TN3270A  TCPABC81 TSO10002 TN3270E T ATTLS TLSv1 AES256_SHA
  000594 Establsh TN3270A  TCPABC82 N/A      TN3270E T Sport TLSv1 RC4_SHA
  000208 Establsh TN3270A  TCPABC80 TSO10001 TN3270E T Basic
  00059A Establsh TN3270A  TCPABC83 TSO10003 LINE    T Basic
****************************** Bottom of data ******************************
```

What's New with z/OS Communications Server TN3270?

TN3270 Server in z/OS V1R9 CS
TN3270 Server MUST now run in its own Address Space

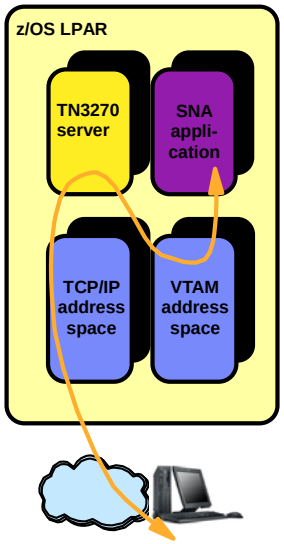
TN3270 Server in its own address space as an option since z/OS V1R6

- **Until z/OS V1R6 the TN3270 Server ran as a subtask of the IBM TCPIP stack address space**
- **In z/OS V1R6 through V1R8, you had a choice:**
  - Run the TN3270 server as a separately started address space from TCPIP stack
  - 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 address spaces
  - 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.

Remote terminal access

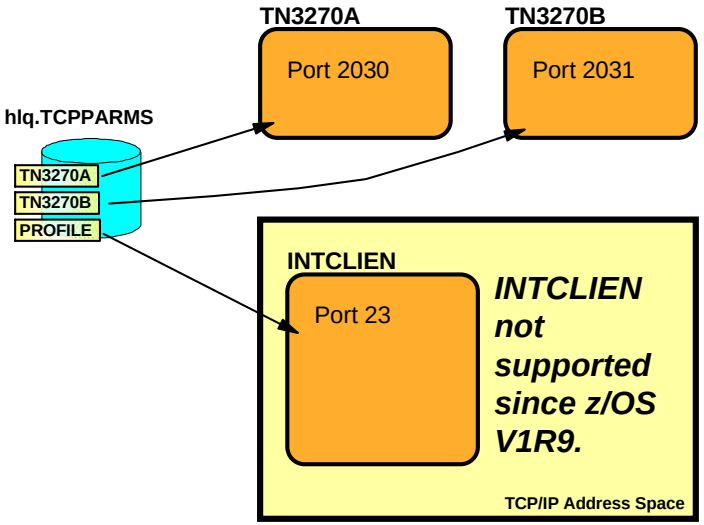
In z/OS V1R9, you can no longer run the TN3270 server in the TCP/IP address space!

Use z/OS V1R6 to V1R8 to migrate.



Multiple TN3270 server address spaces

- **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 optional global option: TCPIPJOBNAME for stack-affinity
  - Each server has its own set of definitions



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

```
D TCPIP,TN3270A,T,CONN,CONN=553
EZZ6065I TELNET CONNECTION DISPLAY 608
  CONNECTED: 13:55:40  07/28/2009  STATUS: SESSION ACTIVE
  CLIENT IDENTIFIER FOR CONN: 00000553   SECLABEL: **N/A**
    CLIENTAUTH USERID: **N/A**
    HOSTNAME: NO HOSTNAME
    CLNTIP..PORT: ::FFFF:9.65.255.62..61585
    DESTIP..PORT: ::FFFF:9.42.105.45..2025
    LINKNAME: QDIO4
  PORT:  2025 QUAL: NONE
    AFFINITY: TCPCS
    STATUS: ACTIVE   TTLSSECURE
    ACCESS: SECURE 35 TLSV1
     TTLSRULE: ABC-TN3270-Server-2025 3
     TTLSGRPACTION: gAct1
     TTLSENVACTION: eAct1
     TTLSCONNACTION: cAct3 ABC-TN3270-2025
  PROTOCOL: TN3270E          DEVICETYPE: IBM-3278-3-E
    TYPE: TERMINAL GENERIC
    OPTIONS: ETET----   3270E FUNCTIONS: BSR--C-
                       NEWENV FUNCTIONS: E-
  LUNAME: TCPABC81
  APPL: TSO10002
    USERIDS   RESTRICTAPPL: **N/A**   EXPRESSLOGON: **N/A**
    LOGMODES  TN REQUESTED: SNX32703  APPL SPECIFIED: SNX32703
```

```
//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)
//PROFILE  DD DSN=USER1.TCPCS.TCPPARMS(TN3270A),DISP=SHR
//SYSTCPD  DD DSN=USER1.TCPCS.TCPPARMS(TCPDATA),DISP=SHR
```

General considerations for standalone TN3270 servers

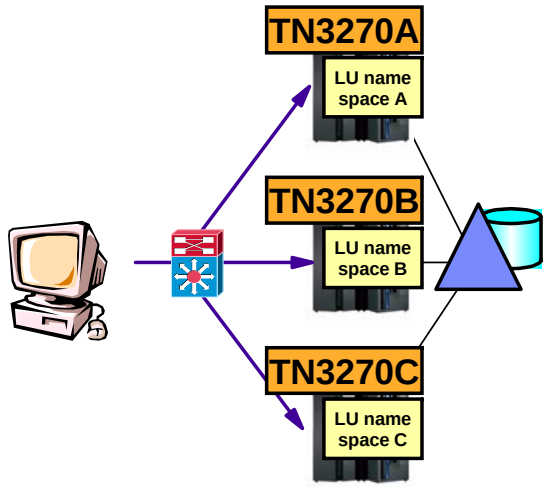
- **TCP/IP affinity is required to obtain stack Jobname & Hostname for the following functions.**
  - Telnet SNMP Subagent activation - Must direct registration by stack jobname.
  - WLM Registration - Must specify stack hostname during registration.
  - SMF Hostname - Stack hostname used.
- **Command 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 netstat command was issued.
- **SNMP Subagent Limitation - Agent/subagent connection requires a one-to-one matchup.**
  - Any particular agent can support only one Telnet subagent
  - You can enable response time monitoring in all servers, but only one can enable the SNMP subagent
- **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)
- **Cannot 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.

What's New with z/OS Communications Server TN3270?

z/OS V1R10 CS Sysplex TN3270 server (LU name server)

TN3270 LU name assignment in a z/OS Sysplex with replicated TN3270 server instances

- **TN3270 connections are often load-balanced across a cluster of TN3270 server instances:**
  - Single system image (one IP address to connect to)
  - High availability (reconnect immediately honored)
  - Scalability (add servers as number of clients increase)
  - Workload management (based on WLM and server health)



- **Such a topology requires careful planning of how LU names are assigned by the individual TN3270 servers in the Sysplex:**
  - Each TN3270 server has its own separately managed LU name space
  - Active LU names must be unique across all LPARs in the Sysplex
    - Unless only local SNA sessions are used (TN3270 server secondary LU in the same LPAR as the primary LU it establishes a session to)
  - Printer association requests must go to the same TN3270 server that was used to select the LU for the associated display session
  - Reconnect processing and SNA session clean up functions only work if clients reconnect to the same server as the original connection

- **For generic LU name assignment implementations (no dependency on specific LU names):**
  - Load balance initial connection from a client IP address
  - Use timed affinity in load balancer for all succeeding connections from same client IP address
    - Necessary to handle reconnect and printer association request processing correctly

- **For specific (nailed) LU name assignment implementations (certain clients need certain LU names):**
  - In most cased, load balancing cannot be done for such connections
  - Use DVIPA takeover to address availability of TN3270 servers

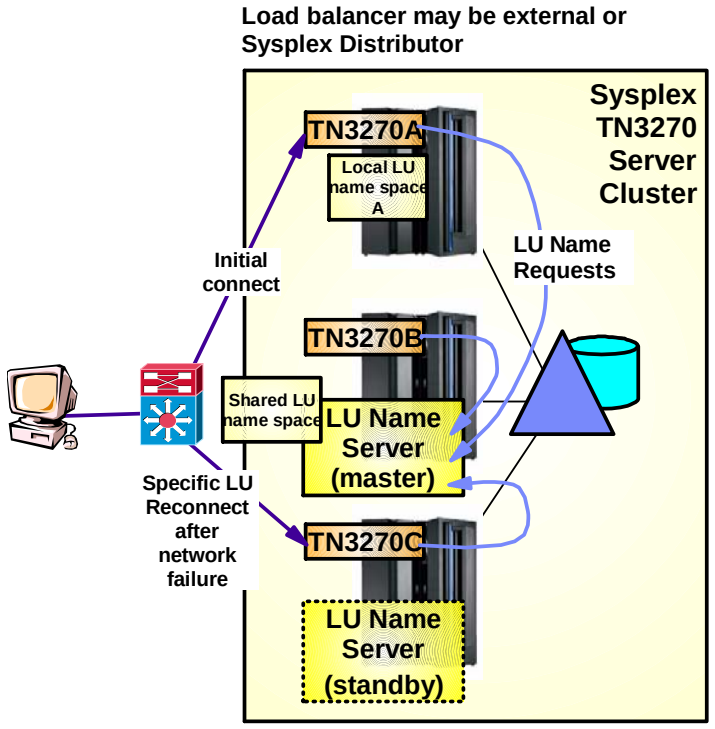
Coordinated TN3270 server LU name management within a Sysplex

- **TN3270 LU name manager for Sysplex-wide LU name management across Sysplexed TN3270 servers**
  - LU name assignment:
    - Generic requests: pick an available LU name in the shared name space
    - Specific request: verify that requested LU is not already in use by one of the Sysplexed TN3270 servers
  - Reconnect with specific LU name requests after temporary network failure:
    - Manage timemark processing on existing connection(s) across sysplexed TN3270 servers:
      - Terminate "stale" TN3270 connections
      - Clean up and terminate associated SNA session
      - Free LU name(s) for terminated connections
      - Process reconnect on any TN3270 server in the Sysplex
  - Some functions will continue to require timed affinity in load balancer:
    - Printer association
    - Generic LU name reconnect processing (TKOGENLU)
    - The check client connection option (CheckClientConn)
    - SNA session reconnect (TKOGENLURECON)
  - A TN3270 server instance may use both a local name space and a shared name space

- **LU name manager functions implemented as extensions to current TN3270 server**
  - A TN3270 server can concurrently act as a normal TN3270 server and as an LU name server
  - A TN3270 server can act as an LU name server only

- **VTAM clone definitions of TN3270 server LUs on all systems**
  - LUs may come active on any system (but not at the same time)

Simplified high-availability and Single System Image design of Sysplexed TN3270 server topologies



TN3270 LU name server in a Sysplex - a few more details

- **New TN3270 profile definition to define**
  - The TN3270 server XCF group name
  - Whether the TN3270 server is an LU name requester or an LU name server
  - For a TN320 server that may be an LU name server
    - Primary (will become the active LU name server if no other LU name server is active when this TN3270 server is started)
    - Backup (with a backup rank - the higher, the more likely to become the active LU name server if the currently active LU name server goes down)

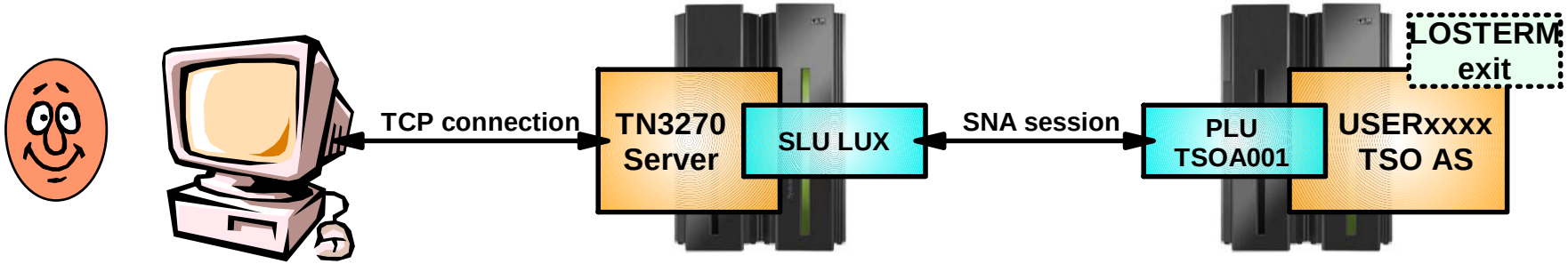
- **Each of the LU mapping statements now has a shared equivalent:**
  - SDEFAULTLUS … ENDSDEFAULTLUS
  - SDEFAULTLUSSPEC … ENDSDEFAULTLUSSPEC
  - SDEFAULTPRT … ENDSDEFAULTPRT
  - SDEFAULTPRTSPEC … ENDSDEFAULTPRTSPEC
  - SLUGROUP … ENDSLUGROUP
  - SPRTGROUP … ENDSPRTGROUP

- **Restrictions:**
  - A profile may have either DEFAULT… or SDEFAULT… defined, but not both.
  - A profile may have both LUGROUP and SLUGROUP definitions, but all LU group names on one profile must be unique.
  - A profile may have both PRTGROUP and SPRTGROUP definitions, but all PRT group names on one profile must be unique.
  - The EXIT parameter is not supported on SLUGROUP and SPRTGROUP statements.

What's New with z/OS Communications Server TN3270?

z/OS V1R11 CS
TSO LOGON Reconnect

Improved TSO LOGON reconnect processing through TN3270



- Combined effort by TSO and CS development
- New LOGONHERE option in IKJTSOxx member to enable new support
  - LOGONHERE(ON) - default
  - LOGONHERE(OFF)
- Enables reconnecting TSO user from a new SNA session
- Helps further reduce number of “USERID already in use” errors
- Make sure you don’t have a RECONLIM=0 in your TSOKEY00 member

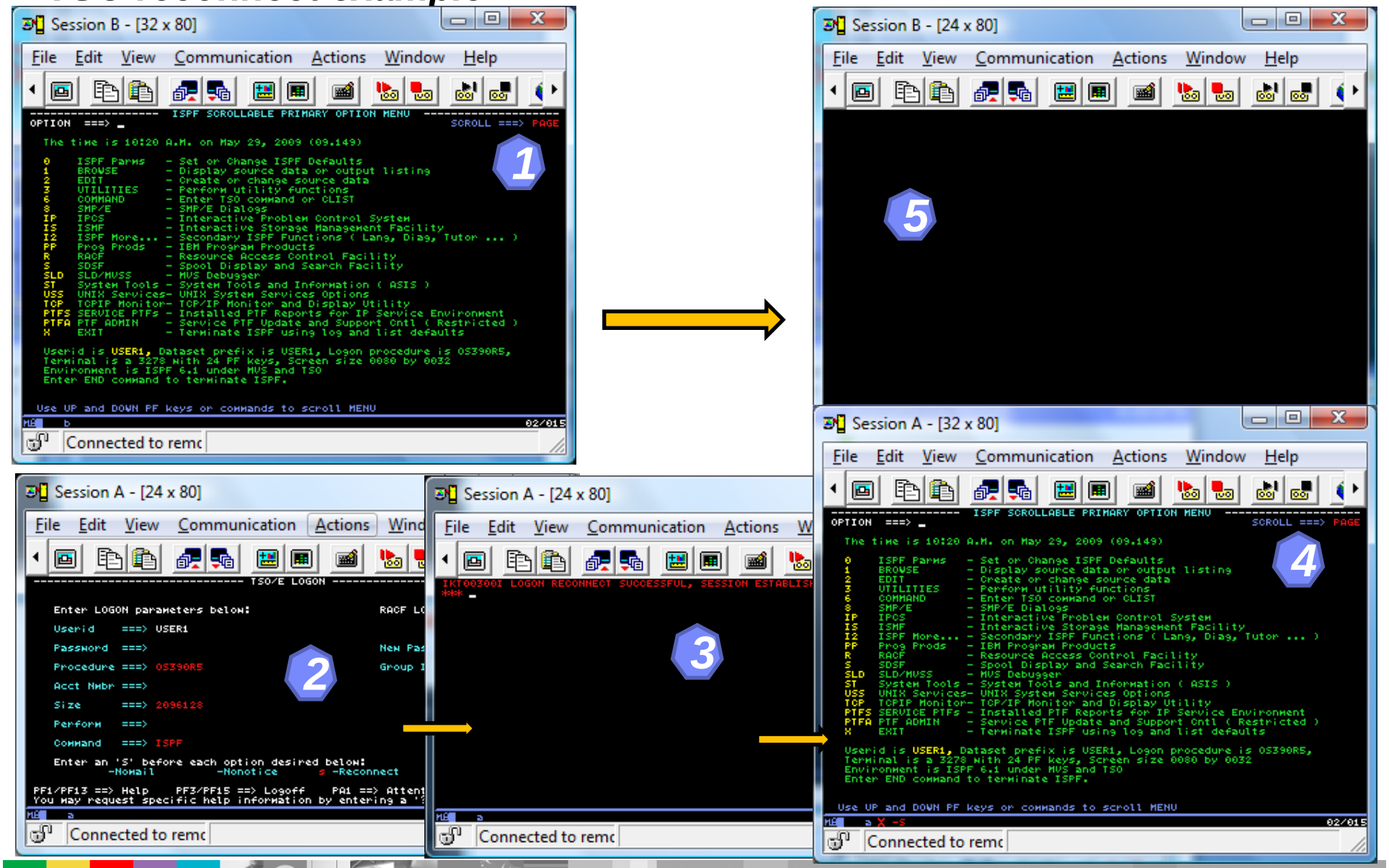
If old SNA session exists, when user attempts reconnect, disconnect old SNA session and proceed with TSO logon reconnect.

TSO Reconnect Possible	Single session	Multiple sessions	NATed connecti-vity
TKOGENLU[RECON]	✓		
CheckClientConn	✓	✓	
TKOSPECLU[RECON]	✓	✓	✓
TSO LOGONHERE	✓	✓	✓
TIMEMARK/SCANINTERVAL	✓	✓	✓

TSO LOGON reconnect – hints and tips

- CA TPX Session Manager
  - If virtual LUs are defined as ‘SHR’, TPX does not allow TSO reconnect
    - You need to define virtual LUs with GRP or UNQ to allow TSO reconnect through TPX
- IBM CL/Supersession
  - Similar problem as observed with TPX
  - CL/Supersession has addressed this via APAR OA30103
- z/OS Communications Server APAR OA30405
  - Fixes a blank screen problem with intra-Sysplex cross-LPAR reconnect processing
- z/OS TSO/E APAR OA30078
  - Improved error messages (IKJ56468I) if reconnect fails – more specifics about the reason, such as RECONLIM=0 specified, or USERMAX exceeded, etc.

TSO reconnect example

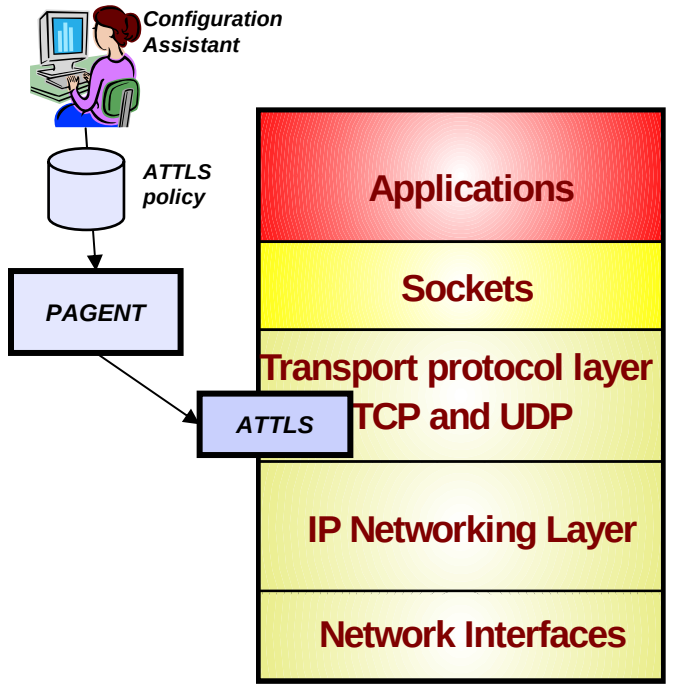


AT-TLS enhancements

- AT-TLS enhancements are immediately available to secure TN3270 connections, if they are secured with AT-TLS

- AT-TLS to support new System SSL functions that have been added to System SSL since z/OS V1R7:
  - TLS V1.1
  - Using RFC3280 to validate a certificate
  - Negotiation and use of a truncated HMAC
  - Negotiation and use of a maximum SSL fragment size
  - Negotiation and use of handshake server name indication
  - Setting the CRL LDAP server access security level

- AT-TLS is also updated to address FIPS 140-2 requirements for applications that use AT-TLS to provide secure connections.

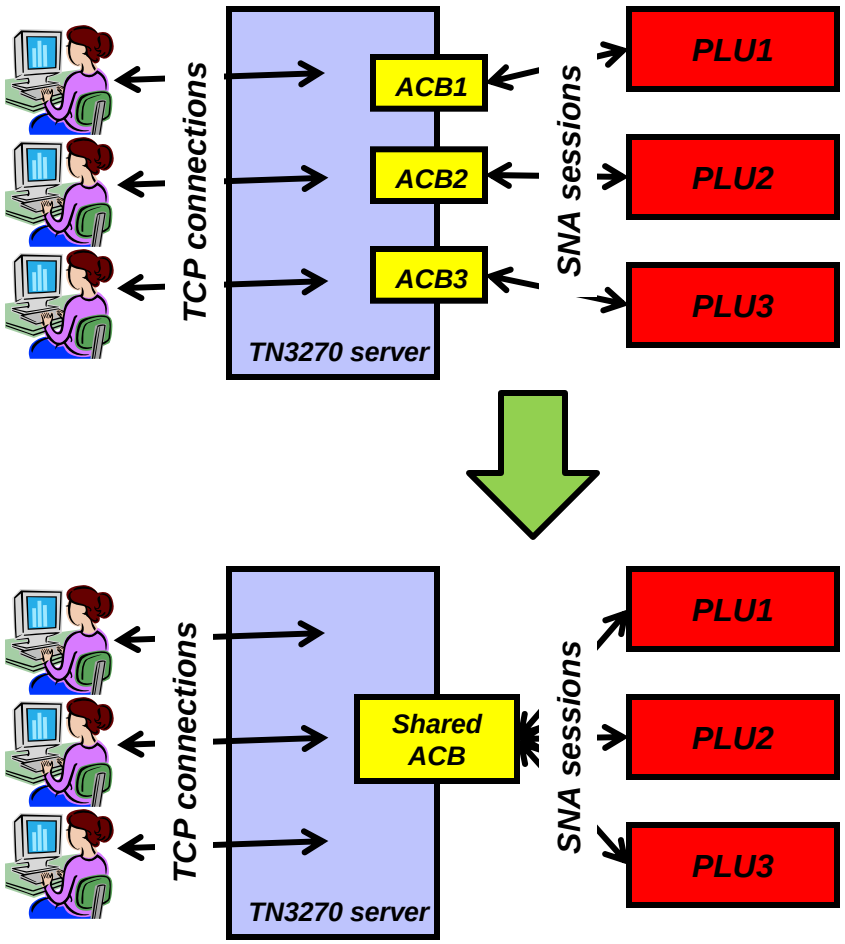


What's New with z/OS Communications Server TN3270?

z/OS V1R12 CS

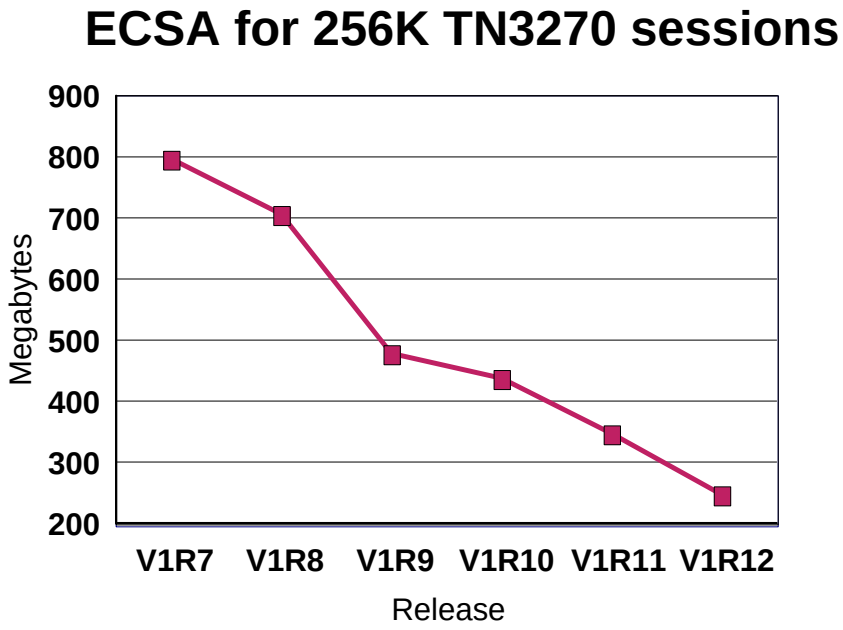
TN3270 server improvements – shared ACB support for improved performance and reduced ECSA storage use

- Telnet shared ACB support can be turned on or off with a simple statement in TELNETGLOBALS section
- VTAM model statements must be used to define the Telnet LUs
- Shared ACBs remain open until the Telnet server is ended.
  - Improve path length for client logon by using an ACB which is already open
  - Improve path length for client logoff by avoiding CLOSE ACB
  - Improve path length for Telnet termination by having fewer ACBs to close
  - Reduce the likelihood of Telnet hangs due to CLOSE ACB
  - Reduce TN3270 server ECSA usage



TN3270 server ECSA usage improvement up to and including z/OS V1R12 Communications Server

Release	ECSA for 256K TN3270 sessions
V1R7	798M
V1R8	708M
V1R9	480M
V1R10	440M
V1R11	347M
V1R12 (1)	249M

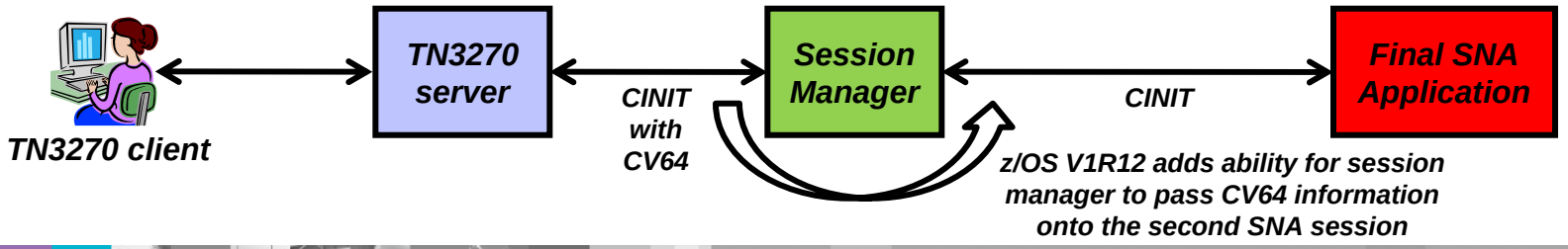


The numbers are configuration dependent, but they should give you an idea of the magnitude of the savings achieved in the recent releases.

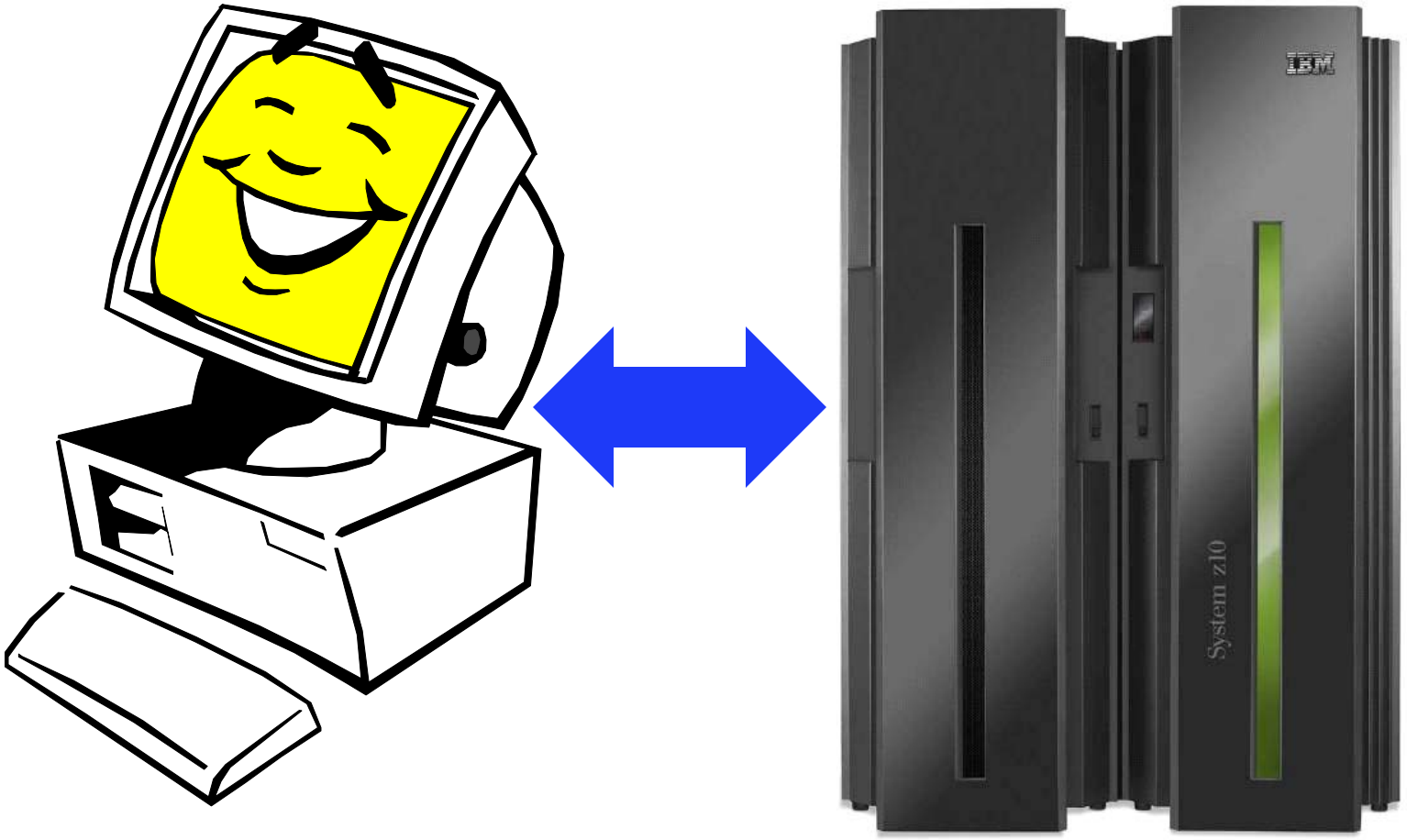
Note (1): The V1R12 number is a preliminary number based on use of shared ACBs - it may change before general availability of z/OS V1R12 Communications Server

TN3270 server improvements – IP management information through a relay-mode session manager

- TN3270 server passes selected IP management information to the SNA side via a control vector known as a "CV64"
  - CV64 includes client IP address, port, and optionally host name
    - A VTAM display of the Telnet LU includes this information
  - The CV64 is also passed to the SNA PLU via its logon exit
- When the SNA PLU is a session manager that relays the SNA session over another LU to the final SNA application PLU, the CV64 information is lost on that second session
  - The session manager has no SNA APIs available to propagate the CV64 information
- z/OS V1R12 adds such an API, allowing an enabled session manager to pass the CV64 information to the final SNA application
- IBM Session Manager (ISM) plans to support this API



Happy telnetting …..



For more information

URL	Content
http://www.twitter.com/IBM_Commserver	IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver	IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/	IBM Communications Server library
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server

For pleasant reading ….