

# z/OS 2.4 IBM Education Assistance

Element: z/OS Communications Server



# Agenda

- Trademarks
- Session Objectives
- For each epic
  - Overview
  - Usage & Invocation
  - Interactions & Dependencies (if any)
  - Migration & Coexistence considerations (if any)
  - Installation (if any)
- Session Summary
- Statement of directions
- Appendix
- Key Contacts

# Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- Additional Trademarks: None

# Session Objectives

Provide a high-level overview of the Communications Server functions in z/OS V2R4

- [Sysplex Notification of TCP/IP Stack Join or Leave](#)
- OSA-Express7S 25GbE Support
- Communications Server support for 25GbE RoCE Express2 features
- Code page enhancements for CSSMTP
- z/OS Encryption Readiness Technology (zERT) aggregation
- z/OS Encryption Readiness Technology (zERT) Network Analyzer
- TN3270E Telnet Server Express Logon Feature support for Multi-Factor Authentication
- Network Configuration Assistant support for multiple location TCP/IP configuration
- Multiple Installation support for Network Configuration Assistant
- IWQ Support for IPSec
- HiperSockets Converged Interface Support
- z/OS and Linux SMC Interoperability and Performance Testing
- [Communications Server Miscellaneous enhancements](#)

# Sysplex notification of TCP/IP stack join or leave

# Overview

## **Who (Audience)**

- Software developers that exploit dynamic VIPAs

## **What (Solution)**

- A new Event Notification Facility (ENF) signal will be raised as follows:
  - When the TCP/IP stack initially joins the TCP/IP Sysplex Group
  - When the TCP/IP stack leaves the TCP/IP Sysplex Group for any reason
  - When the TCP/IP stack rejoins the TCP/IP Sysplex Group

## **Wow (Benefit / Value, Need Addressed)**

- A Software developer can programmatically determine when TCP/IP Sysplex Autonomics has triggered an event to leave the sysplex and when it has successfully rejoined the sysplex by receiving an explicit notification in real time.

# Usage & Invocation

- Create an ENF 80 exit in order to listen for the new signal when a TCP/IP stack joins or leaves a Sysplex Group.
- To listen for ENF event code 80, specify the qualifying events (x'40000000') on the QUAL parameter  
Example: ENFREQ ACTION=LISTEN  
CODE(80)  
QUAL(X'40000000')
- The ENF signal contains
  - Flag bits representing a join or a leave
  - The job name of the TCPIP stack performing the leave or join

# OSA-Express7S 25GbE Support



# Overview

## **Who (Audience)**

- z/OS network administrators

## **What (Solution)**

- z/OS Communications Server support for the next generation OSA-Express7S 25 GbE feature
- Enhanced storage to accommodate the higher bandwidth

## **Wow (Benefit / Value, Need Addressed)**

- Support for OSA-Express7S with higher 25GbE bandwidth

# Usage & Invocation

- z/OS V2R2 and V2R3 with APARs PI95703 and OA55256 provide the new support but do not increase any storage defaults
- Available on z/OS V2R1 with APARs PH02249 and OA56093 - enables activation and display of 25 GbE support only

# Dependencies

- **Hardware Dependencies**

- z14 with OSA-Express7S
- 25GbE Ethernet Switch support

See the 3906DEVICE and 3907DEVICE Preventive Service Planning (PSP) bucket

# Migration considerations

- **Migration**

- If you are using QDIOSTG=126 and default READSTORAGE to GLOBAL
  - The increase in CSM fixed HVCOMMON work element storage takes effect for all 10GbE and 25GbE OSAs (as you are already using 8MB for read buffers)
  - This is also true on z/OS V2R2 and V2R3
- Default value for the fixed CSM buffers changed from 200 M to 512 M

- **Health check update**

- CSVTAM\_CSM\_STG\_LIMIT health check was updated to indicate the new default of 512M for FIXED CSM

# Communications Server support for 25 GbE RoCE Express2 features

# Overview

## **Who (Audience)**

- z/OS network administrators

## **What (Solution)**

- z/OS V2R4 Communications server extends the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function to support the IBM 25 GbE RoCE Express2 feature

## **Wow (Benefit / Value, Need Addressed)**

- Support for RoCE Express2 with higher 25 GbE bandwidth

# Dependencies

- **Hardware Dependencies**
  - IBM z14 with IBM 25 GbE RoCE Express2
  - 25 GbE Ethernet Switch support

# Code page enhancements for CSSMTP



# Overview – CSSMTP MBCS support

## **Who (Audience)**

- System administrators - SMTP users migrating to CSSMTP

## **What (Solution)**

- CSSMTP supports Multi-byte character sets (MBCS)

## **Wow (Benefit / Value, Need Addressed)**

- Enables z/OS mail client to use any language supported by Unicode Services
- Enables SMTPD-to-CSSMTP transition required for z/OS mail client users in V2R3 and beyond

# Usage & Invocation – CSSMTP MBCS support

- In the CSSMTP configuration file
- New statement: MBCS No | Yes  
Example: MBCS Yes  
Default value: No
- New parameter on the TargetServer statement: MBCharset *code page*  
Example:

```
TargetServer
{
    MBCharset IBM-5054
}
```
- Support also provided for z/OS V2R3, V2R2 and V2R1 (in 3Q 2018) with APAR PI93278

# Overview – Improved CSSMTP translation

## **Who (Audience)**

- System administrators

## **What (Solution)**

- CSSMTP supports non IBM-1047 characters in mail headers. Mail headers are translated from TRANSLATE code page to Charset/MBCharset code page (for Single-byte or Multi-byte) to send to the mail server

## **Wow (Benefit / Value, Need Addressed)**

- Non IBM-1047 characters such as euro symbol can be used in mail headers
- Improves CSSMTP code page compatibility with target servers

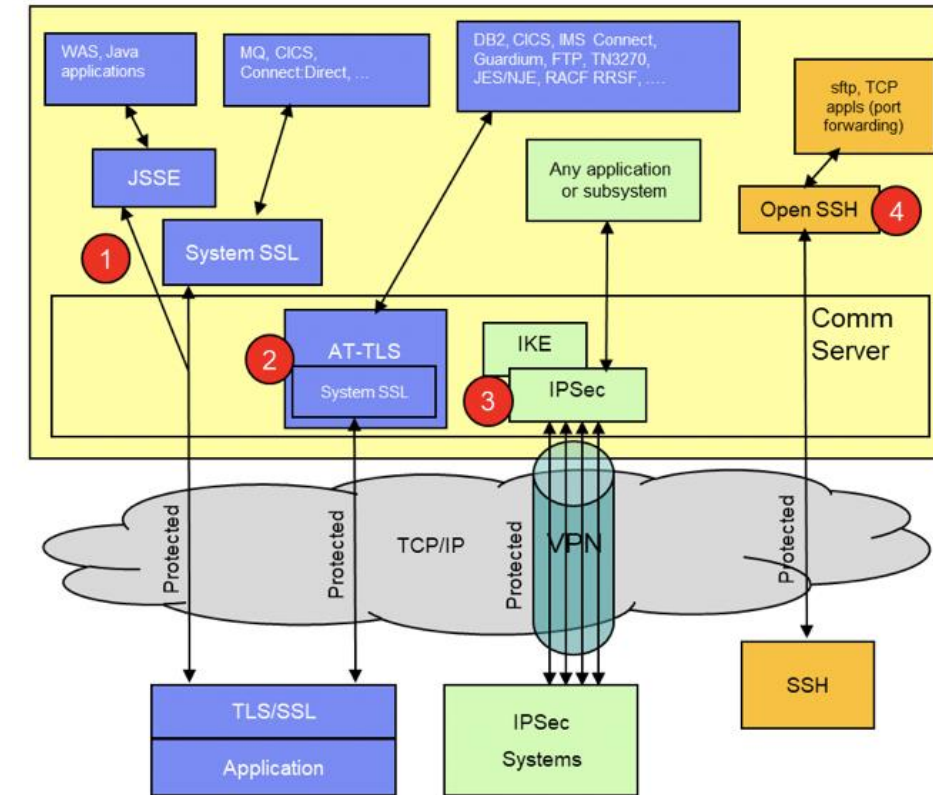
# Migration considerations

- **Migration**
  - To aid in migrating from SMTP to CSSMTP, a table with suggested TRANSLATE and MBCharset values for each SMTP DBCS statement value is in the [z/OS Communications Server: IP Configuration Reference](#) under the description of the CSSMTP MBCS statement.

# z/OS Encryption Readiness Technology (zERT) aggregation

# Background Information: Plethora of security options

- z/OS provides four security mechanisms to protect TCP and Enterprise Extender (EE) connection traffic:
  1. TLS/SSL direct usage (TCP only)
  2. Application Transparent TLS (AT-TLS) (TCP only)
  3. Virtual Private Networks using IPSec and IKED (IP traffic)
  4. Secure Shell using z/OS OpenSSH (TCP only)
- With this many options, how do you ..
  - tell which traffic is being protected, and which is not?
  - determine what is being used to protect the protected traffic?
  - determine who is generating the (un)protected traffic?
  - verify new security measures are being applied correctly?
  - provide the answers to auditors, if asked?



# Background Information: zERT Discovery

- z/OS Encryption Readiness Technology (zERT) discovery was introduced with z/OS V2R3 Communications Server
  - zERT discovery positioned the TCP/IP stack as the central collection point and repository for cryptographic security attributes for TCP and EE connections
  - Attributes are collected and reported on a per-connection basis
  - zERT connection detail information is reported as SMF Type 119 subtype 11 records to the z/OS SMF facility or across a real-time NMI (SYSTCPER) service

*A z/OS network security administrator can discover and audit the network encryption attributes associated with z/OS TCP and Enterprise Extender traffic by analyzing new SMF records generated by zERT.*

# Overview

## **Who (Audience)**

- z/OS Network Security administrators

## **What (Solution)**

- zERT aggregation provides comprehensive security information of network encryption across z/OS in a summarized view via new SMF interval records to the z/OS SMF facility or across a new real-time NMI (SYSTCPES) service

## **Wow (Benefit / Value, Need Addressed)**

- Summarize high volumes of granular zERT SMF data, ideally from multiple systems, into a condensed representation
- Saves SMF disk space and CPU



# Usage & Invocation – zERT Aggregation support

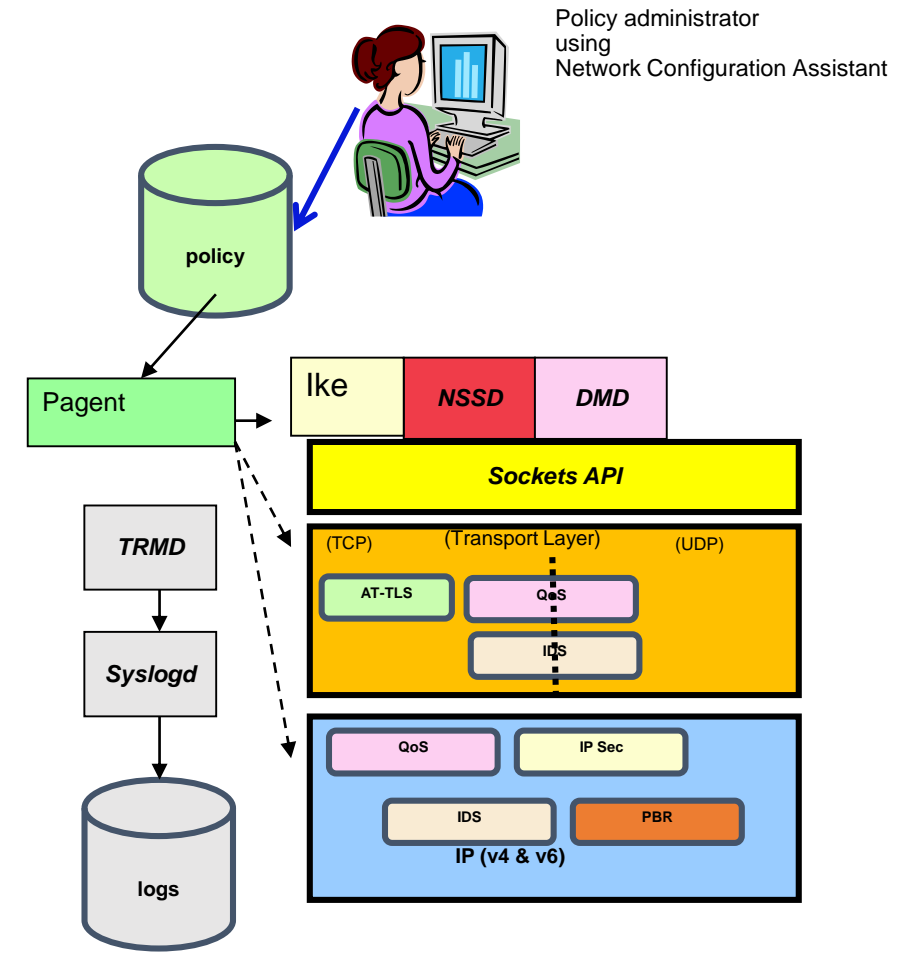
- In the TCP/IP configuration file
- New sub-parameters on the GLOBALCONFIG ZERT parameter to enable aggregation of zERT connection detail records: ZERT NOAGGregation | AGGregation  
Example: ZERT AGGregation  
Default value: NoAGGregation
- New sub-parameters on the SMFCONFIG TYPE119 parameter to enable generation of summary level SMF 119 subtype 12 records: SMFCONFIG TYPE119 NOZERTSUMmary | ZERTSUMmary  
Example: SMFCONFIG TYPE119 ZERTSUMmary  
Default value: NOZERTSUMmary

# Usage & Invocation – zERT Aggregation support (contd.)

- New sub-parameters on the NETMONitor parameter to enable the real time zERT summary NMI service (SYSTCPES): NETMONitor NOZERTSUMmary | ZERTSUMmary  
Example: NETMONitor ZERTSUMmary  
Default value: NOZERTSUMmary  
SAF-based access control available
  - EZB.NETMGMT.sysname.tcpname.SYSTCPES
- ZERT SMF records and the NMI SYSTCPES service are enabled/disabled independently – one, both, or neither can be enabled
- Support also provided for z/OS V2R3 (in 1Q 2018) with APAR PH00255

# Usage & Invocation – Network Configuration Assistant

- Network Configuration Assistant (NCA) is updated to support zERT TCP/IP profile parameters
- NCA is a GUI tool to simplify configuration of z/OS Communications Server
  - TCP/IP profile
  - Policy-based networking technologies:
    - IP Security – IP Filter rules and VPN tunnels
    - Application Transport TLS (AT-TLS)
    - Intrusion Detection Services (IDS)
    - Policy-based Routing (PBR)
    - Quality of Service (QoS)



# Usage & Invocation – NCA (contd.)

Click checkbox to enable zERT

Click checkbox to enable zERT

Click dropdown

Select Enable to turn on zERT Aggregation

Network Configuration Assistant (Home) > TCP/IP Profile > TCP/IP Profile : PLEX1.LPAR1.STACK1 > Security

### Configure Network Security

#### z/OS Encryption Readiness Technology

Global Property Setting:  
Customize the following property. Configuration will be generated to enable or disable this property.

☒ z/OS Encryption Readiness Technology (zERT) (Available beginning with V2R3)

Default value: Aggregation of z/OS Encryption Readiness Technology data

Disable: work management data, management output

**Enable**

Global Property Setting:  
Default taken for the following property. Configuration for this property will not be generated.

☐ For IPv6, enable IP filters, IPSec tunnels, or defensive filters

Additional IP Security global properties...

Select the requirement for Profile filters for TCP/IP traffic:

OK Cancel Reset

Network Configuration Assistant (Home) > TCP/IP Profile > TCP/IP Profile : PLEX1.LPAR1.STACK1

### TCP/IP Profile for Group PLEX1, System Image LPAR1, Stack STACK1

Configure

Use the following links to create and modify TCP/IP resources to define this stack's profile configuration.

TCP/IP Stack Resources	Status
Interfaces: Attach to networks	Configured
Routes: Connect to other systems	Configured
Ports: Reserve ports for TCP/IP applications	Configured
<b>Security: Control network access to and from the System</b>	Configured
Source IP Addressing: Control outbound connection source IP addressing	Not configured
Performance and Protocol: Tune your TCP/IP stack	Configured
Management and Traces: Enable TCP/IP stack systems management and diagnosis	Not configured

# Coexistence considerations

- **Coexistence considerations**
  - In a sysplex with TCP/IP stacks at different release levels
    - Distributing stack and target stack must be at release V2R3 with zERT aggregation enabled to be able to collect any IPSec protection details
  - When the Network Security Server (NSSD) provides certificate services for IPSec protection, NSSD must be at release V2R3 for certificate details to be available

# Installation

- **Planning considerations**

- If you operate multiple FTP servers at the same server IP address, and you use PASSIVEDATAPORTS, consider assigning different port ranges to the different FTP servers in order to aggregate the data connections into separate SMF records for the FTP servers
- SMF interval processing must be enabled in SMFPRMxx member even if SMF records are only be reported to the real-time NMI
- Partial wildcard *jobname* value on PORT or PORTANGE definitions might result in multiple servers being aggregated into one record

# z/OS Encryption Readiness Technology (zERT) Network Analyzer

# Overview

## **Who (Audience)**

- z/OS Network security administrators

## **What (Solution)**

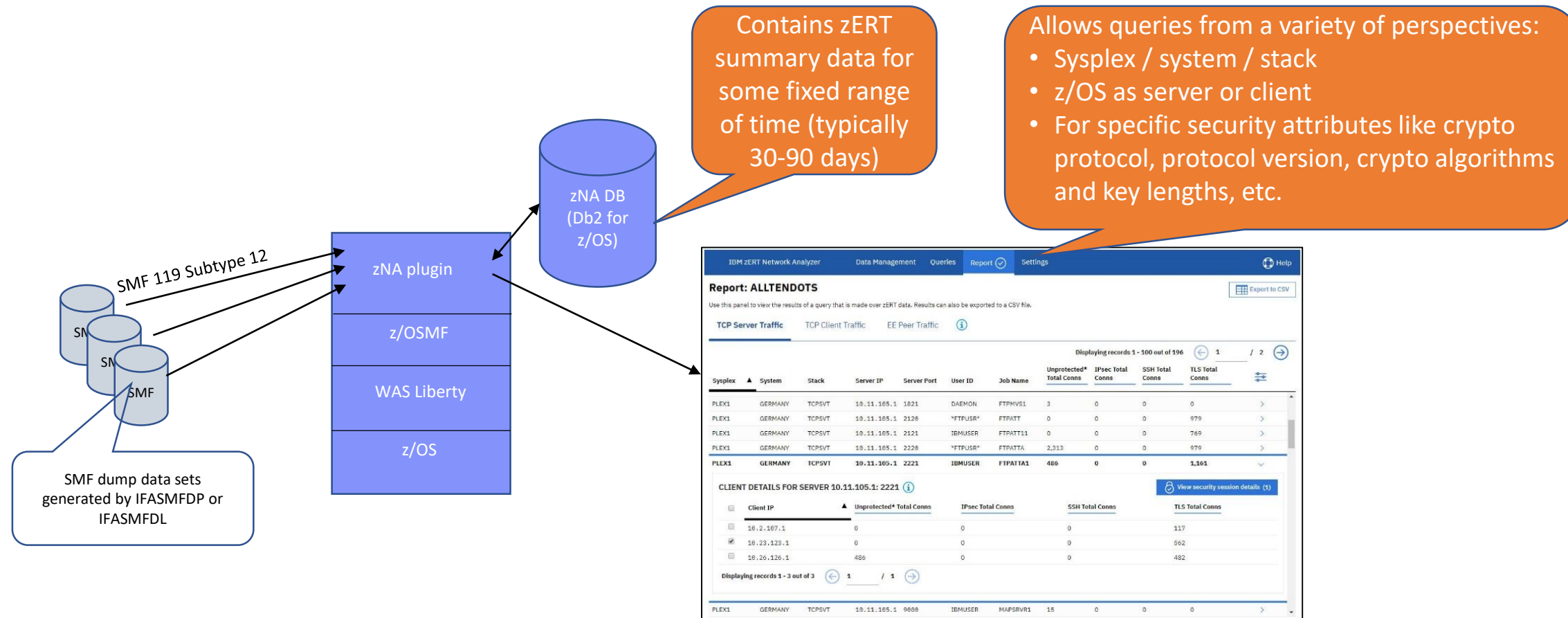
- GUI for zERT data analysis and reporting

## **Wow (Benefit / Value, Need Addressed)**

- Significantly improves Time-To-Value of gaining insights into zERT data and driving a Pervasive Encryption strategy for all z/OS network communications



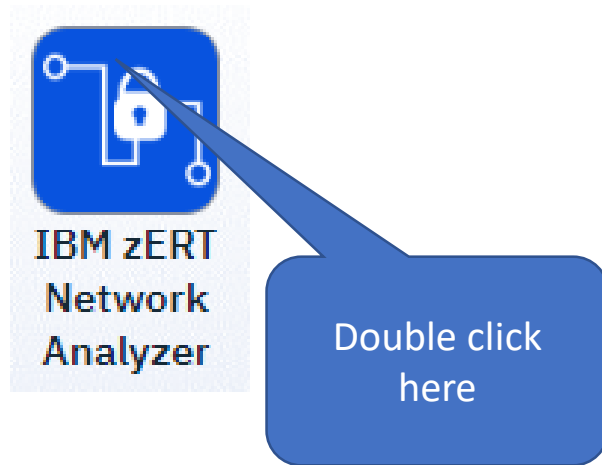
# Usage & Invocation



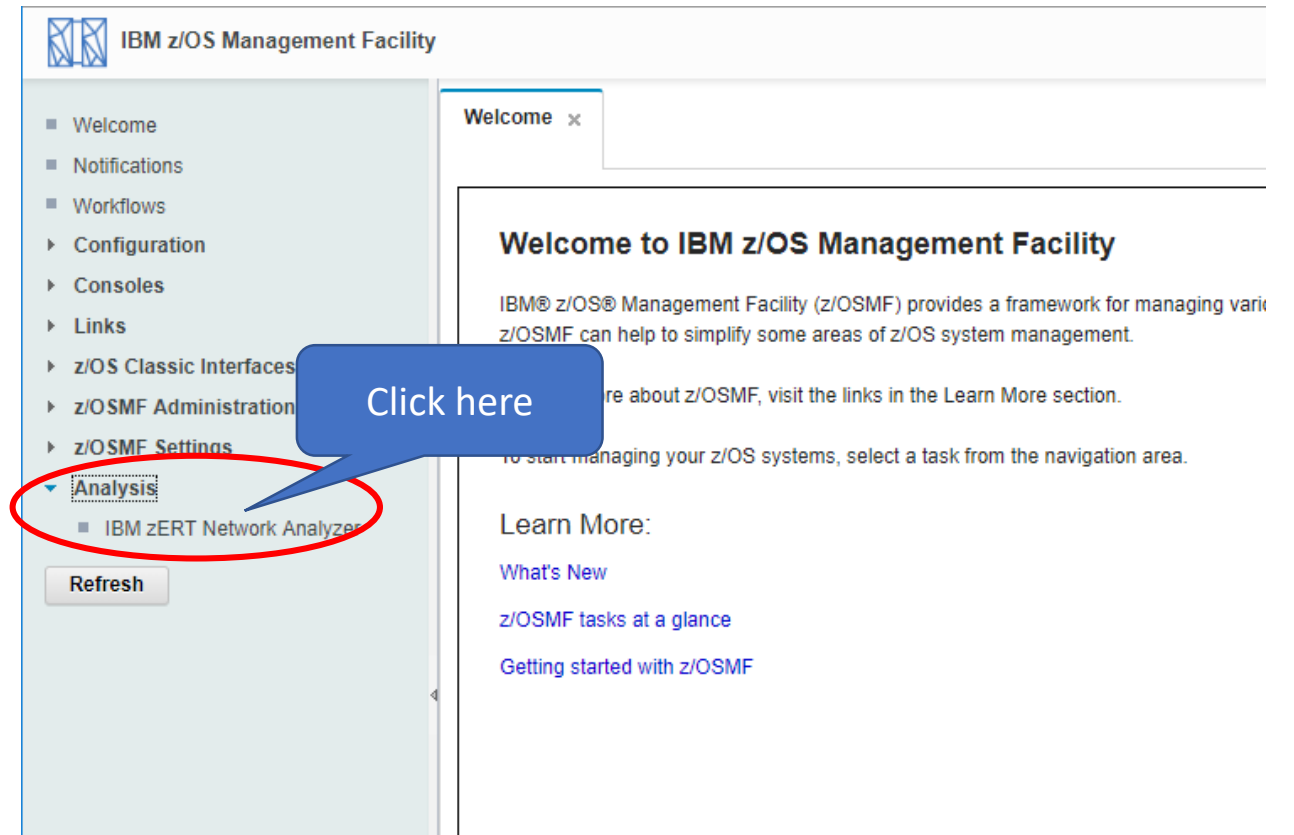
Support also provided for z/OS V2R3 (in 4Q 2018) with APAR PH03137

# Usage & Invocation (contd.)

➤ z/OSMF Desktop mode:



➤ z/OSMF Classic mode:



# Usage & Invocation (contd.)

The screenshot displays the IBM zERT Network Analyzer web interface. At the top is a dark blue navigation bar with the title 'IBM zERT Network Analyzer' and five tabs: 'Data Management', 'Queries', 'Report', 'Settings', and 'Help'. Below the navigation bar, the main content area is titled 'Welcome to IBM zERT Network Analyzer' and includes a subtitle 'Analyze the cryptographic network protection of your z/OS TCP/IP and Enterprise Extender traffic.' The interface is divided into two main sections: 'Getting started with IBM zERT Network Analyzer' and 'Common tasks with IBM zERT Network Analyzer'. The 'Getting started' section contains a link to the 'Tutorial of IBM zERT Network Analyzer' with a checkmark icon. The 'Common tasks' section lists five tasks, each with an icon and a link: 'Configure IBM zERT Network Analyzer' (wrench icon), 'Import SMF dump data sets' (floppy disk icon), 'Manage operation history' (clock icon), and 'Create, manage, and run queries' (gear icon). The fifth task, 'Manage queries', is partially obscured by a callout. Six callouts provide additional information: three blue callouts point to the 'Data Management', 'Queries', and 'Settings' tabs, explaining their functions; two orange callouts point to the 'Help' tab and the top navigation bar, explaining their roles; and one blue callout points to the 'Tutorial of IBM zERT Network Analyzer' link, explaining its purpose.

Click here to import SMF dump data sets and to prune old data out of the database

Click here to create, modify, and run queries over the imported data

Click here to view the query results

UI Feature – topical help: Click here for topical help in the IBM Knowledge Center

UI Feature – Navigation: Main functions are accessed through top-level tabs

Click here to modify application and database settings

The tutorial is a great way to become familiar with each of the zERT Network Analyzer

# Usage & Invocation – Settings (1 of 2)

The first time a user logs into the zERT Network Analyzer after it is installed, they will be forced to this dialog to fill in the database configuration information. Until the correct information is saved, no other panels are accessible (other than Help and the Tutorial).

Note that any time this information is saved, it will cause the zERT Network Analyzer plugin to recycle since the save causes z/OSMF XML configuration files to be updated.

IBM zERT Network Analyzer | Data Management | Queries | Report | **Settings** | Help

Application Settings | **Database Settings**

## Database Settings

Use this panel to configure database connection settings

Refresh database settings | Save settings

**Warning:** Changing database settings causes the IBM zERT Network Analyzer to restart and all current user sessions, data management operations, and unsaved data to be lost.

**DATABASE SETTINGS** ⓘ

Required fields are denoted with an asterisk (\*).

Host name *	<input type="text" value="127.0.0.1"/>	User ID *	<input type="text" value="sysadm"/>
Port number *	<input type="text" value="446"/>	Password *	<input type="password" value="....."/>
Location name *	<input type="text" value="NETA"/>		
JDBC classpath *	<input type="text" value="/usr/lpp/db2c10/jdbc/classes/"/>		

# Usage & Invocation – Settings (2 of 2)

IBM zERT Network Analyzer   Data Management   Queries   Report   **Settings**   Help

Application Settings   **Database Settings**

## Application Settings

Use this panel to configure application logging and export settings

**LOG SETTINGS** ⓘ

Log level: INFO   Number of debug log files: 10

Debug log level: FINEST   Maximum debug log file size (bytes): 1048576

**EXPORT SETTINGS** ⓘ

Default delimiter for exported CSV files

☒ Comma ,   ☐ Pipe |   ☐ Semicolon ;   ☐ Tab ↵   ☐ Custom \_\_\_\_

The network analyzer plugin supports two different logs. The “Log level” controls zNA messages that go into the z/OSMF log. This log only contains INFO, WARNING and SEVERE messages. The “Debug log level” controls messages that go into zNA’s own private log. This log can be configured to contain much finer-grained log information.

Export settings here to set the default CSV file delimiter.

Refresh application settings   Save settings

# Usage & Invocation – Data management (1 of 3)

The screenshot shows the 'Data Management' section of the IBM zERT Network Analyzer. The 'Import SMF Data' tab is selected. The main heading is 'Import SMF Data', with a subtext: 'Use this panel to define a set of SMF dump data sets that can then be scheduled for import into IBM zERT Network Analyzer.' A blue button 'Import selected' is in the top right. Below this is a section 'Refreshed data set list' with an information icon and a close icon. The main area is titled 'SMF DUMP DATA SETS' with an information icon. Above the table are buttons: 'Refresh import list', 'Save import list', 'Remove selected', and 'Add data set'. A note states: 'Required fields are denoted with an asterisk (\*)'. The table has columns 'Name \*' and 'Comments'. It lists five data sets: 'IPCS.TUTORIAL.SMF0AT02' (GERMANY system - various traffic 1), 'IPCS.TUTORIAL.SMF0AT01' (MVS034 EE), 'IPCS.TUTORIAL.SMF0AT03' (MVS202 small sample), 'IPCS.TUTORIAL.SMF0AT04' (all sample), and 'IPCS.TUTORIAL.SMF0AT05' (system - various traffic 2). Each row has a checkbox and a blue icon with a minus sign.

IBM zERT Network Analyzer | **Data Management** | Queries | Report | Settings | Help

**Import SMF Data** | Data Management History | Manage Database

**Import SMF Data**

Use this panel to define a set of SMF dump data sets that can then be scheduled for import into IBM zERT Network Analyzer.

Import selected

Refreshed data set list

SMF DUMP DATA SETS

Refresh import list | Save import list | Remove selected | Add data set

Required fields are denoted with an asterisk (\*).

<input type="checkbox"/> Name *	Comments
<input type="checkbox"/> IPCS.TUTORIAL.SMF0AT02	GERMANY system - various traffic 1
<input type="checkbox"/> IPCS.TUTORIAL.SMF0AT01	MVS034 EE
<input type="checkbox"/> IPCS.TUTORIAL.SMF0AT03	MVS202 small sample
<input type="checkbox"/> IPCS.TUTORIAL.SMF0AT04	all sample
<input type="checkbox"/> IPCS.TUTORIAL.SMF0AT05	system - various traffic 2

UI Feature – Temporary Status Messages: When data has been retrieved or updated, a temporary status message like this appears for 10 seconds.

Click here to create a new row in the SMF dump data set list.

Click one or more check boxes to select the data sets you want to work with. Then click the "Import selected" or "Remove selected" buttons above.

You can also save or delete a data set name individually.

# Usage & Invocation – Data management (2 of 3)

IBM zERT Network Analyzer

Data Management Queries Report Settings

Help

Import SMF Data Data Management History **Manage Database**

## Manage Database

Use this panel to manage the IBM zERT Network Analyzer database:

- To view latest summary of the database
- To prune imported data from the database

### DATABASE SUMMARY ⓘ

Refresh database statistics

Total number of SMF 119 subtype 12 records	5,232
Total security sessions	5,232
Earliest record date	2018-01-18T11:11:10.940Z
Latest record date	2018-01-18T11:11:11.030Z

### PRUNE DATABASE ⓘ

☒ Remove all data

☐ Older than  days

☐ Custom range

to

**Prune imported data**

# Usage & Invocation – Data management (3 of 3)

IBM zERT Network Analyzer | **Data Management** | Queries | Report | Settings | Help

Import SMF Data | **Data Management History** | Manage Database

## Data Management History

Use this panel to view previous IBM zERT Network Analyzer import and prune operations.

**DATA MANAGEMENT OPERATIONS** ⓘ

Each row displays either an Import or Prune data management operation. Click on a row to view more details about the operation.

Refresh history

Submitted	Operation	Status	Start time
2019-02-26T09:48:50.867Z	Import - IPCS.TUTORIAL.SMFDAT02	Complete	2019-02-26T09:48:50.877Z
2019-02-26T09:46:08.823Z	Prune - All data	Complete	2019-02-26T09:46:08.836Z
2019-02-26T09:43:52.355Z	Import - IPCS.TUTORIAL.SMFDAT01	Complete	2019-02-26T09:43:52.367Z
2019-02-26T09:36:58.698Z	Import - IPCS.TUTORIAL.SMFDATA1	Failed	2019-02-26T09:36:58.709Z
2019-02-26T08:14:14.222Z	Prune - Custom date range	Complete	2019-02-26T08:14:14.345Z
2019-02-21T16:40:28.827Z	Import - IPCS.ZERTFVT.EE.IPSEC.SYS1.SMFDAT02	Complete	2019-02-21T16:40:28.880Z
2019-02-21T16:35:13.928Z	Import - IPCS.ZERTFVT.EE.IPSEC.SYS1.SMFDAT02	Complete	2019-02-21T16:35:14.077Z
2019-02-21T15:50:01.939Z	Import - IPCS.ZERTFVT.EE.IPSEC.SYS1.SMFDAT02	Complete	2019-02-21T15:50:01.981Z
2019-02-21T15:49:45.453Z	Import - IPCS.ZERTFVT.EE.IPSEC.SYS1.SMFDAT02	Complete	2019-02-21T15:49:45.464Z
2019-02-21T15:46:02.826Z	Import - IPCS.ZERTFVT.EE.IPSEC.SYS1.SMFDAT02	Complete	2019-02-21T15:46:02.838Z
2019-02-21T15:40:16.422Z	Import - IPCS.ZERTFVT.EE.SYS1.SMFDAT50	Failed	2019-02-21T15:40:16.438Z
2019-02-21T15:11:13.565Z	Import - IPCS.ZERTFVT.EE.IPSEC.SYS1.SMFDAT02	Failed	2019-02-21T15:11:13.763Z

**IMPORT DETAILS**

IPCS.TUTORIAL.SMFDAT02 - GERMANY various traffic 1

USER3

**IMPORT STATISTICS**

Number of records added	Number of duplicate records	Number of records ignored	Earliest record imported	Latest record imported
5,232	0	1	2018-01-18T11:11:10.940Z	2018-01-18T11:11:11.030Z

**IMPORT DETAILS**

IZUET0023I Cannot import a migrated data set

IPCS.ZERTFVT.EE.SYS1.SMFDAT50

USER1



# Usage & Invocation – Queries (1 of 4)

The screenshot shows the 'Manage Queries' page in the IBM zERT Network Analyzer. The top navigation bar includes 'Data Management', 'Queries' (highlighted with a red box), 'Report', 'Settings', and 'Help'. Below the navigation bar, a 'Manage Queries' section contains a 'Manage Queries' button (also highlighted with a red box) and a 'New query' button. A 'Refresh queries list' button is located on the right. The main content area displays a table of 'SAVED QUERIES' with columns for 'Name' and 'Description'. The first query is 'ALL TENDOT SERVERS' with the description 'Traffic to all 10.0.0.0/8 servers'. The second query, 'BATCH 7 WORKLOAD', is highlighted in blue and has a callout pointing to its description: 'Check workload for weak IPsec encryption'. Below this query, there are two sections: 'SCOPE FILTERS' and 'SECURITY FILTERS'. The 'SCOPE FILTERS' section includes 'Systems' (PLEX1/GERMANY/\*) and 'TCP Endpoints' ((Server) Server: \*, Client: 10.11.123.2, (Client) Server: \*:8080,25, Client: \*). The 'SECURITY FILTERS' section includes 'IPSec symmetric encryption algorithm' (DES, 3DES). Callouts explain that 'Scope filters define the range of systems, endpoints and time over which the query applies' and 'Security filters define the specific security attributes of interest'. Each query row has action buttons: 'Run query', 'Edit query', 'Export query', and 'Delete query'.

IBM zERT Network Analyzer Data Management **Queries** Report Settings Help

**Manage Queries**

Use this panel to manage existing queries saved to IBM zERT Network Analyzer.

**SAVED QUERIES**

Refresh queries list

Name	Description	Run query	Edit query	Export query	Delete query
ALL TENDOT SERVERS	Traffic to all 10.0.0.0/8 servers	Run query	Edit query	Export query	Delete query
<b>BATCH 7 WORKLOAD</b>	<b>Check workload for weak IPsec encryption</b>	Run query	Edit query	Export query	Delete query

**SCOPE FILTERS**

Systems  
PLEX1/GERMANY/\*

TCP Endpoints  
(Server) Server: \*, Client: 10.11.123.2  
(Client) Server: \*:8080,25, Client: \*

**SECURITY FILTERS**

IPSec symmetric encryption algorithm  
DES, 3DES

Scope filters define the range of systems, endpoints and time over which the query applies.

Security filters define the specific security attributes of interest.

# Usage & Invocation – Queries (2 of 4)

IBM zERT Network Analyzer   Data Management   **Queries**   Report   Settings   Help

Manage Queries   **New Query** (X)

## New Query

Use this panel to create a new query.

No scope or security filters added, running query as-is will return all imported data

**Query Details**   Scope Filters (0)   Security Filters (0)

**QUERY DETAILS** ⓘ

Required fields are denoted with an asterisk (\*).

**Name \***

EXAMPLE QUERY

**Description**

Example for Beta presentation

29/50

Every query must have a unique name...

...and may also have a short description.

Save query   Close query   Save and run query

# Usage & Invocation – Queries (3 of 4)

The screenshot shows the 'New Query' interface of the IBM zERT Network Analyzer. The top navigation bar includes 'IBM zERT Network Analyzer', 'Data Management', 'Queries' (active), 'Report', and 'Settings'. Below this, there are tabs for 'Manage Queries' and 'New Query' (selected). The main title is 'New Query' with a subtitle 'Use this panel to create a new query.'.

On the left, there are three categories of filters: 'Time and Date', 'Systems', and 'Network'. The 'Systems' category is highlighted with a red box and labeled 'Scope Filters (2)'. An orange callout bubble points to this box, stating: 'Query Builder Feature: Each category selected on the left pane causes the related builder dialog to appear in the right pane where the specific details are specified.'

The right pane shows the 'DATE RANGE' and 'SYSTEMS' filter builders. The 'DATE RANGE' section has a 'Within the last 30 days' option selected, with a date range of '1/22/2019 to 1/22/2019'. The 'SYSTEMS' section has a 'Sysplex' dropdown set to 'PLEX1' and a 'System' dropdown with a list of options: 'Any system', 'System', 'GERMANY', and 'Custom system'. A blue callout bubble points to the 'System' dropdown, stating: 'Topology-related values are populated based on current data in database.'

At the top right of the right pane, there are three buttons: 'Save query', 'Close query', and 'Save and run query'. Each filter section has a 'Remove filter' button and an 'Add system' button.

# Usage & Invocation – Queries (4 of 4)

IBM zERT Network Analyzer    Data Management    **Queries**    Report    Settings    Help

Manage Queries    **New Query** (X)

## New Query

Use this panel to create a new query.

Save query    Close query    Save and run query

Query Details    Scope Filters (2)    **Security Filters (2)**

**Unprotected\* Traffic**

- ☒ All traffic with no recognized cryptographic protection

**IPSec**

- ☐ All IPSec protected traffic
- ☐ IPSec symmetric encryption algorithm
- ☐ IPSec message authentication algorithm
- ☐ IPSec certificate digital signature algorithm
- ☐ IPSec certificate asymmetric key length
- ☐ IPSec key exchange algorithm

**TLS**

- ☐ All TLS protected traffic
- ☒ TLS protocol version
- ☐ TLS symmetric encryption algorithm
- ☐ TLS message authentication algorithm
- ☐ TLS certificate digital signature algorithm
- ☐ TLS certificate asymmetric key length

**ALL TRAFFIC WITH NO RECOGNIZED CRYPTOGRAPHIC PROTECTION** ⓘ Remove filter

ⓘ The query report shows all sessions with no recognized cryptographic protection.

**TLS PROTOCOL VERSION** ⓘ Remove filter

<input type="checkbox"/> Unknown version	<input checked="" type="checkbox"/> SSL 3.0	<input type="checkbox"/> TLS 1.1
<input checked="" type="checkbox"/> SSL 2.0	<input checked="" type="checkbox"/> TLS 1.0	<input type="checkbox"/> TLS 1.2

# Usage & Invocation – Report (1 of 3)

IBM zERT Network Analyzer

Data Management

Queries

Report ✓

Settings

Help

## Report: EXAMPLE QUERY

Export to CSV

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file.

TCP Server TrafficTCP Client TrafficEE Peer Traffic

Displaying records 1 - 100 out of 109

						Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns	
						12	0	0	0	>
					*FTPUSR*	26	0	0	0	>
					DAEMON	2	0	0	0	>
PLEX1	GERMANY	TCPSVT	10.11.105.1	23	OMVSKERN	1	0	0	0	>
PLEX1	GERMANY	TCPSVT	10.11.105.1	80	SVTWSRV	3,009	0	0	0	>
PLEX1	GERMANY	TCPSVT	10.11.105.1	175	IBMUSER	1	0	0	0	>
PLEX1	GERMANY	TCPSVT	10.11.105.1	512	IBMUSER	0	0	0	5	>
PLEX1	GERMANY	TCPSVT	10.11.105.1	620	*FTPUSR*	230	0	0	0	>

Displays summary information about a server running on a local stack (that is, the z/OS stack that is identified by the Sysplex, System, and Stack attributes).

Displays summary information about a foreign server (that is, a server that is connected to by a client running on the local stack). The foreign server might or might not be running on the local stack.

Displays summary information about a single local EE peer.

# Usage & Invocation – Report (2 of 3)

IBM zERT Network Analyzer Data Management Queries **Report** Settings Help

## Report: EXAMPLE QUERY

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file. [Export to CSV](#)

**TCP Server Traffic** TCP Client Traffic EE Peer Traffic ⓘ

Displaying records 1 - 100 out of 109 1 / 2

Sysplex	System	Stack	Server IP	Server Port	User ID	Job Name	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.201.4	80	SVTWSRV	WEBSERV1	70	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.211.3	923	IBMUSER	TNPRC923	375	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.211.3	925	IBMUSER	TNPRC925	1	0	0	375

**CLIENT DETAILS FOR SERVER 10.11.211.3:925** ⓘ [View security session details \(1\)](#)

<input type="checkbox"/> Client IP	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
<input type="checkbox"/> 10.2.15.9	0	0	0	130
<input type="checkbox"/> 10.2.16.103	0	0	0	126
<input checked="" type="checkbox"/> 10.2.107.1	1	0	0	119

Displaying records 1 - 3 out of 3 1 / 1

PLEX1	GERMANY	TCPSVT	10.11.250.105	50000	IBMUSER	DMP50000	3	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.250.105	50030	IBMUSER	DMP50030	7	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.250.105	50050	IBMUSER	DMP50050	0	0	0	0

# Usage & Invocation – Report (3 of 3)

PLEX1	GERMANY	TCPSVT	10.11.211.3	923	IBMUSER	TNPRC923	375	0	0	0	>
PLEX1	GERMANY	TCPSVT	10.11.211.3	925	IBMUSER	TNPRC925	1	0	0	375	▼
<b>SECURITY SESSION DETAILS FOR SERVER 10.11.211.3:925</b> ⓘ <a href="#">View client details</a>											
Unprotected* Session Details ▼ Traffic Details ▼											
Unprotected* Session Details											
TLS Session Details											
Client IP Total Conns Partial Conns Bytes In Bytes Out Segs In Segs Out											
10.2.107.1 1 1 549.0 B 2.4 KB 19 16											
Displaying records 1 - 1 out of 1 ◀ 1 / 1 ▶											
PLEX1	GERMANY	TCPSVT	10.11.250.105	50000	IBMUSER	DMP50000	3	0	0	0	>

PLEX1	GERMANY	TCPSVT	10.11.211.3	923	IBMUSER	TNPRC923	375	0	0	0	>
PLEX1	GERMANY	TCPSVT	10.11.211.3	925	IBMUSER	TNPRC925	1	0	0	375	▼
<b>SECURITY SESSION DETAILS FOR SERVER 10.11.211.3:925</b> ⓘ <a href="#">View client details</a>											
TLS Session Details ▼ Cryptographic Details ▼											
Certificate Details											
Distinguished Name Details											
Traffic Details											
Client IP Negotiated Cipher Key Exchange Alg Symm Encryption Alg Message Auth Alg											
10.2.107.1 0035 RSA AES CBC 256 HMAC-SHA1											
Displaying records 1 - 1 out of 1 ◀ 1 / 1 ▶											
PLEX1	GERMANY	TCPSVT	10.11.250.105	50000	IBMUSER	DMP50000	3	0	0	0	>

# Dependencies & Installation

- **Software Dependencies**
  - z/OS Db2 11 or above on the same or different LPAR
- **Installation**
  - Access to UI controlled through SAF resource  
IZUDFLT.ZOSMF.ZERT\_NETWORK\_ANALYZER in the ZMFAPLA class



# TN3270E Telnet Server Express Logon Feature support for Multi- Factor Authentication

# Overview

## **Who (Audience)**

- Security administrator

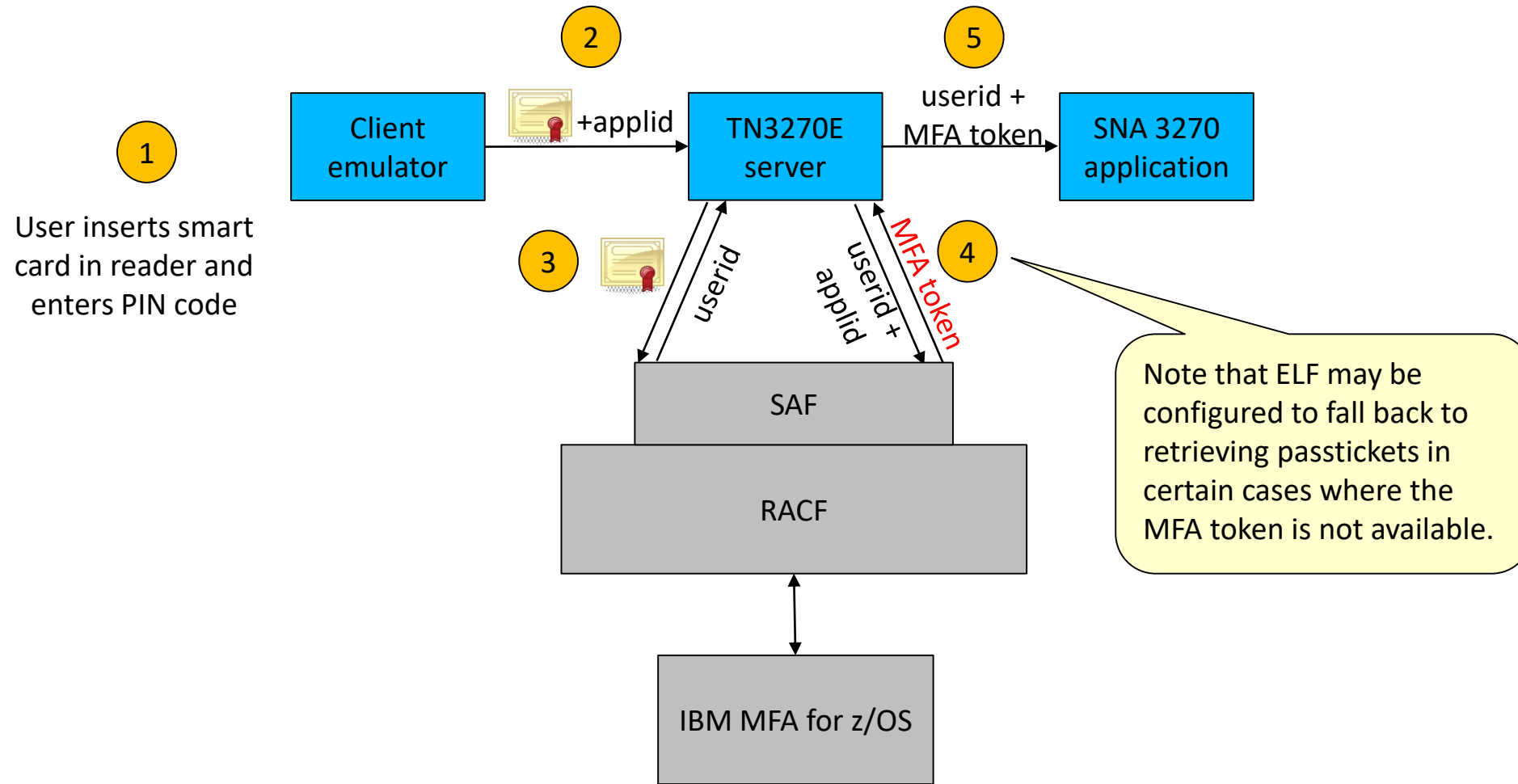
## **What (Solution)**

- TN3270E Express Logon Feature accepts either passticket or a multi-factor authentication token from SAF

## **Wow (Benefit / Value, Need Addressed)**

- Multi-factor Authentication (MFA) for z/OS provides a way to raise the assurance level of OS and applications / hosting environments by extending SAF-enabled security managers to authenticate users with multiple authentication factors

# Usage & Invocation



# Usage & Invocation (contd.)

- In the Telnet profile
- New statement: EXPRESSLOGONMFA | NOEXPRESSLOGONMFA
  - EXPRESSLOGONMFA sub-parameters: FALLBACK | NOFALLBACK

Example: EXPRESSLOGONMFA FALLBACK

Default value: NOEXPRESSLOGONMFA

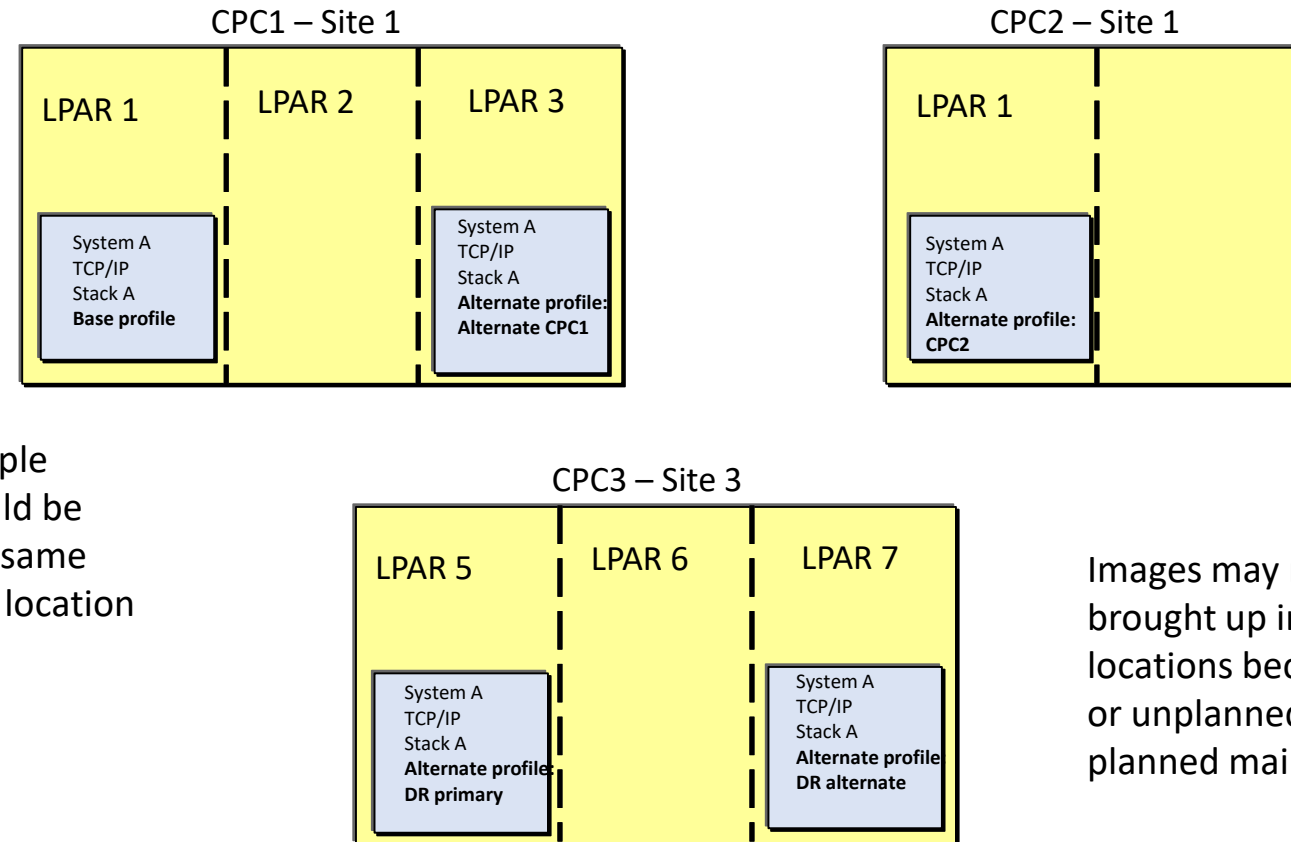
Sub-parameter default value: NOFALLBACK
- Support also provided for z/OS V2R3 Communications Server (in 1Q 2018) with APAR PI85185, RACF APAR OA53002, and IBM MFA for z/OS APARs PI86470 and PI93341

# Dependencies

- **Software Dependencies**
  - RACF
  - IBM MFA

Network Configuration Assistant  
support for multiple location  
TCP/IP configuration

# Background Information: Alternate configurations



A system image may have multiple alternate locations where it could be running. These could be on the same CEC, same site, or at a different location altogether.

Images may need to be brought up in alternate locations because of planned or unplanned outages or planned maintenance

# Background Information: Alternate configuration (contd.)

Common configuration file for all three systems

```
INTERFACE OSA&CHIPID.  
DEFINE IPAQENET CHPIDTYPE OSD  
PORTNAME PORT&CHIPID.  
IPADDR 2.2.2.&HOST.
```



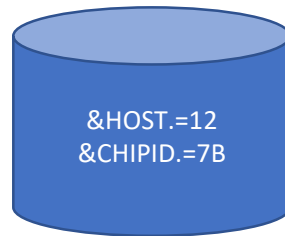
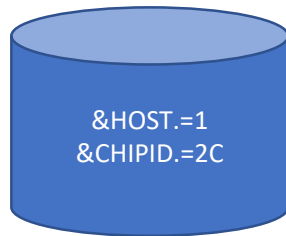
IEASYM MAIN



IEASYM BACKUP



IEASYM DEV



- Today customers use system symbol tables to manage variation in configuration across alternate locations.
  - These are manually edited MVS system configuration datasets
- Keeping those values straight across systems usually requires significant out of band, manual work using spreadsheets, etc.
  - This is tedious and error-prone



Sym	Main	Backup	Dev
&HOST.	1	2	22
&CHIPID.	2C	3A	7B



# Overview

## **Who (Audience)**

- z/OS network administrators

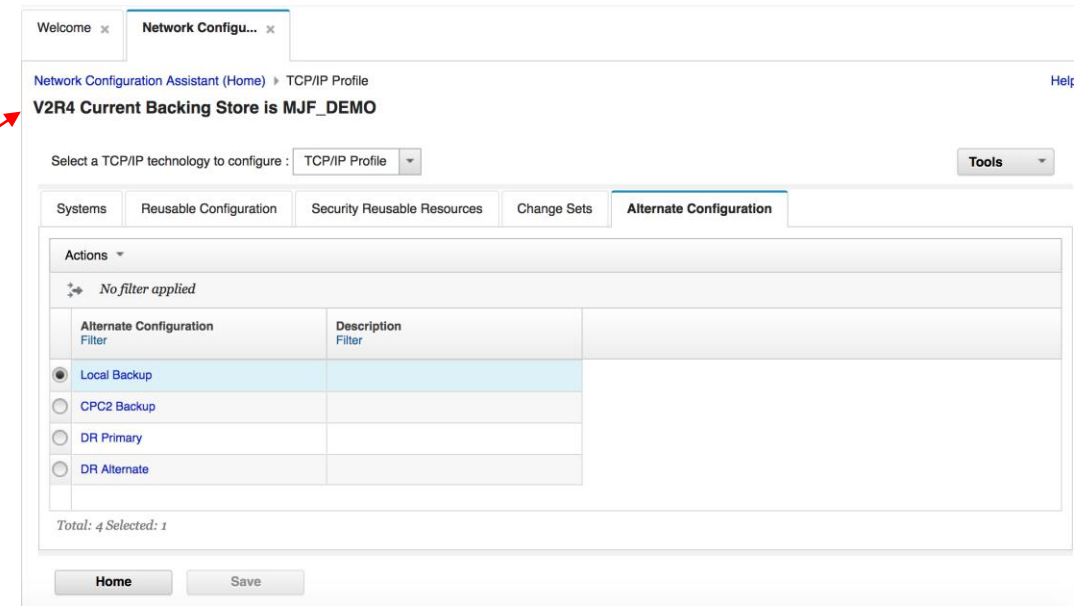
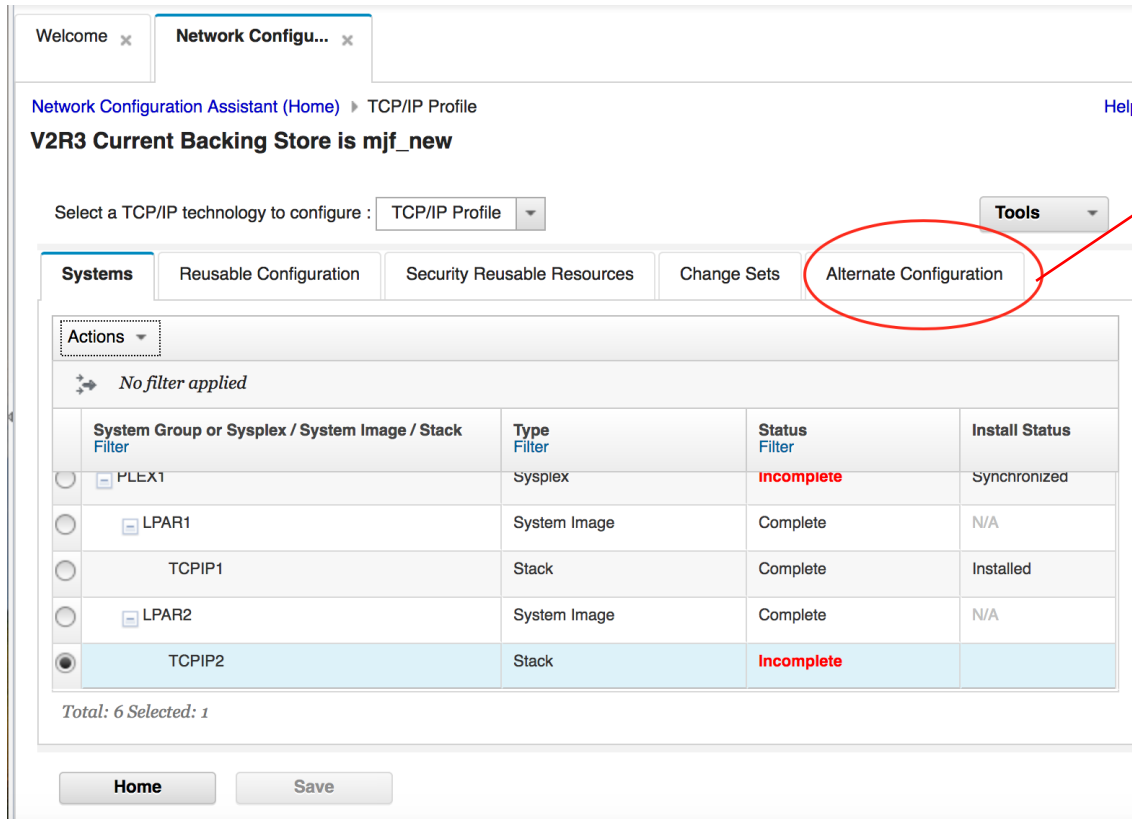
## **What (Solution)**

- Enables creation of TCP/IP configuration for an image that can be used in multiple locations with a minimum of changes required between alternates
- Provides capability to install TCP/IP configuration files to Alternate Configuration locations with the correct symbol values for each location

## **Wow (Benefit / Value, Need Addressed)**

- z/OS network administrators can define high availability and disaster recovery configurations for multiple systems using Network Configuration Assistant without repeating redundant information per alternative configuration

# Usage and Invocation: Alternate configuration

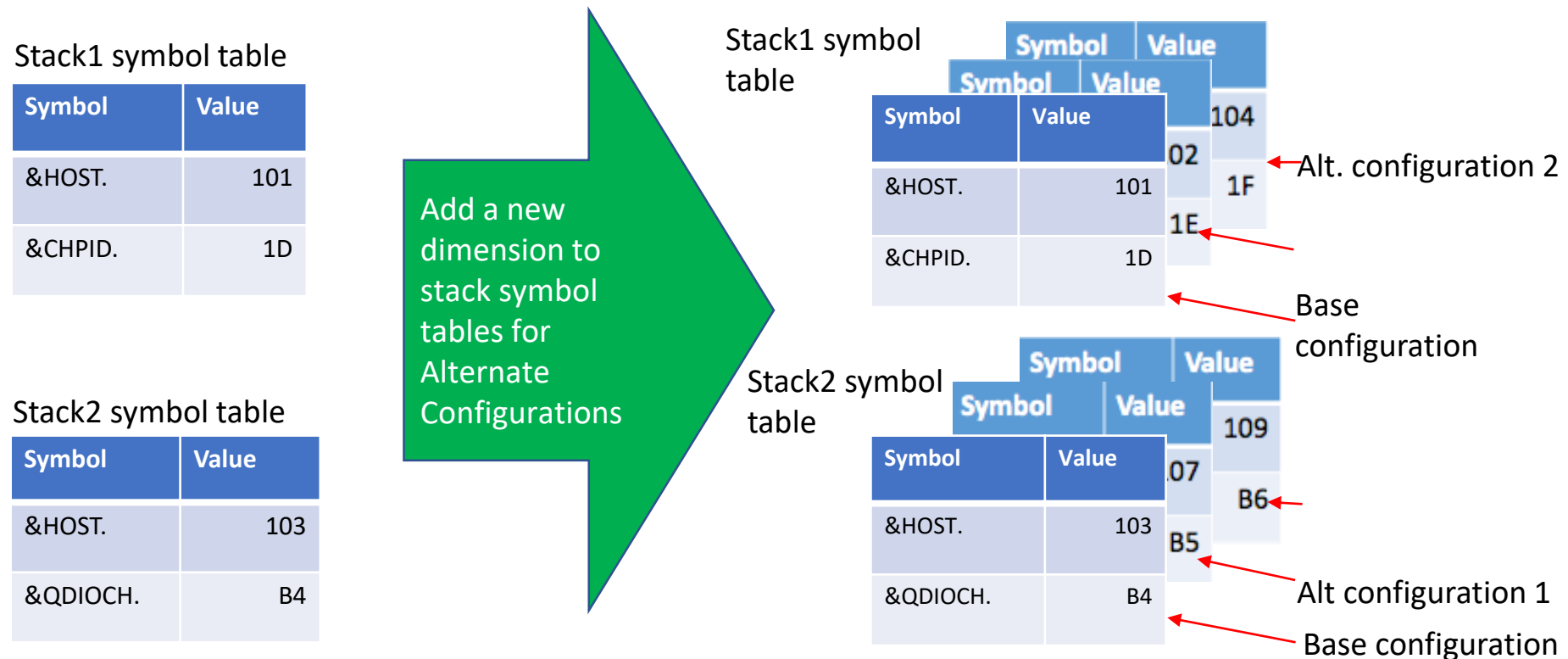


- New tab on the TCP/IP systems tree for Alternate configuration

- Each Alternate Configuration object represents a different way an image can be installed - different location, different LPAR, etc.

# Usage & Invocation (contd.)

- Only the symbol values vary by alternate configuration ... the configuration does not!



- NCA Alternate Configuration support was delivered on V2R3 in APAR PI97737 (in 3Q 2018)

# Usage & Invocation (contd.)

- View all Symbol Details panel consolidates all symbols for all alternate locations, for a stack

Network Configuration Assistant (Home) > TCP/IP Profile > TCP/IP Stack

Stack Symbols for System Group PLEX1, Image LPAR1, Stack STACK1

Symbols | Symbol Migration Report

Actions

- View Details
- Modify...
- Show Where Used
- View All Symbol Details**
- Hide Filter Row
- Clear Sorts

Base Configuration Value	Required	Reusable Configuration	Description
2001:DB8:1:1::1	Yes		
5	Yes	osas	
1	Yes	osas	
&internalSysplexv4.	Yes		

Total: 4 Selected: 0

Close Save

Network Configuration Assistant (Home) > TCP/IP Profile > TCP/IP Stack > View All Symbol Details

View All Symbol Details

Close Printable page

Symbols Associated with Stack: PLEX1.LPAR1.STACK1

Symbol/Alternate Configuration	Value	Status	Reusable Configuration	Description
<b>&amp;internalSysplexv6.</b>	<b>2001:DB8:1:1::1</b>	<b>Base Value</b>		
Local Backup	2001:DB8:1:1::1	LINKED	---	---
CPC2 Backup	2001:DB8:1:1::1	LINKED	---	---
DR Primary	2001:DB8:1:1::1	LINKED	---	---
DR Alternate	2001:DB8:1:1::1	LINKED	---	---
<b>&amp;SYM1.</b>	<b>5</b>	<b>Base Value</b>	<b>osas</b>	
Local Backup	5	LINKED	---	---
CPC2 Backup	55	CONFIGURED	---	---
DR Primary	5	LINKED	---	---
DR Alternate	55	CONFIGURED	---	---
<b>&amp;HOST.</b>	<b>1</b>	<b>Base Value</b>	<b>osas</b>	
Local Backup	1	LINKED	---	---

Close Back to Top

- Now you no longer have to use manual spreadsheets and other out of band practices to keep track of your symbol values across stacks and locations!

# Installation

- **Planning considerations:** Alternate Configuration interaction with Change Set and Reusable Configuration
  - For a TCP/IP stack to be considered fully installed by NCA, it must be installed in all Alternate Configurations
    - This is prerequisite for basing a change set on a stack, or a sysplex or reusable configuration that includes that stack
  - Similar to stacks, Change Sets are installed on an Alternate Configuration basis, if a stack in an Alternate Configuration is affected by a Change Set.
  - Recall that symbols are defined in Reusable Configuration
    - Symbol values can be changed in Reusable Configuration change sets
    - In Reusable Configuration Change Sets, you can change symbols for a stack on an Alternate Configuration basis

# Multiple Installation support for Network Configuration Assistant

# Overview

## **Who (Audience)**

- z/OS network administrators

## **What (Solution)**

- The new “install multiple” allows you to check multiple files to be installed, then install them all in one action

## **Wow (Benefit / Value, Need Addressed)**

- This function becomes even more valuable when paired with the new Alternate Configuration support... you can install multiple configurations in one action.

# Usage and Invocation

Network Configuration Assistant (Home) > TCP/IP Profile > Configuration Files > Choose Configuration > Multiple Install

### Install Multiple Stacks

Install Multiple Stacks

Actions	Configuration Type	Configuration	Status	Last Install	Configured File Name
<input type="checkbox"/> System Image					
<input type="checkbox"/> PLEX1.LPAR2.STACK2	TCP/IP Profile	Base Configuration	Installed	2019-01-18 12:20:36	'USER1.TCPPARMS(STACK2)'
<input type="checkbox"/> PLEX1.LPAR2.STACK2	TCP/IP Profile	Local Backup	Never installed	Never	'user1.tcpparms(stack22)'
<input type="checkbox"/> PLEX1.LPAR2.STACK2	TCP/IP Profile	CPC2 Backup	Never installed	Never	
<input type="checkbox"/> PLEX1.LPAR2.STACK2	TCP/IP Profile	DR Primary	Installed	2019-01-21 15:28:35	'USER1.TCPPARMS(stack21)'
<input type="checkbox"/> PLEX1.LPAR2.STACK2	TCP/IP Profile	DR Alternate	Never installed	Never	'user1.tcpparms(stack2a)'

1

Network Configuration Assistant (Home) > TCP/IP Profile > Configuration Files > Choose Configuration > Multiple Install

### Install Multiple Stacks

Install Multiple Stacks

Configuration Type	Configuration	Status	Last Install	Configured File Name
TCP/IP Profile	Base Configuration	Installed	2019-01-18 12:20:36	'USER1.TCPPARMS(STACK2)'
TCP/IP Profile	Local Backup	Never installed	Never	'user1.tcpparms(stack22)'
TCP/IP Profile	CPC2 Backup	Never installed	Never	
TCP/IP Profile	DR Primary	Installed	2019-01-21 15:28:35	'USER1.TCPPARMS(stack21)'
TCP/IP Profile	DR Alternate	Never installed	Never	'user1.tcpparms(stack2a)'

2

3

4

Info

All selected configurations were successfully installed with no messages or warnings. For details on each install, view the history log.

OK Show History

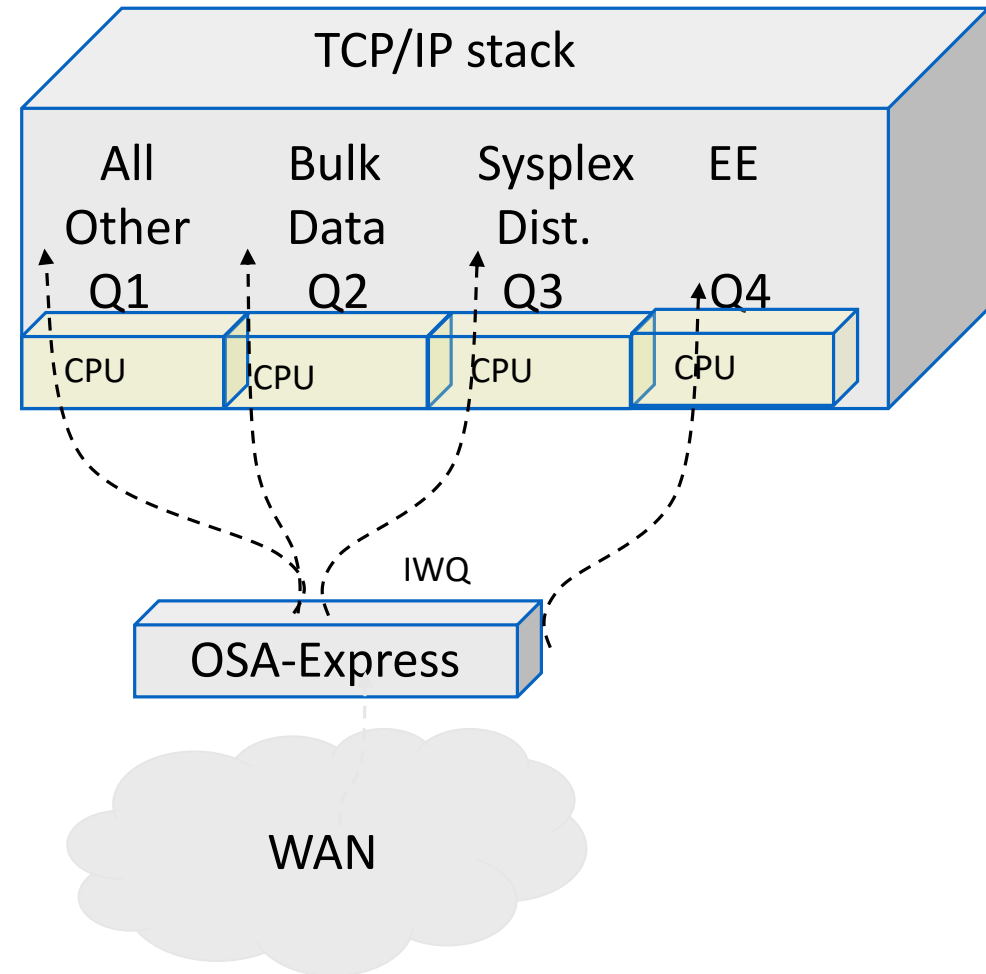
NCA Multiple Install support was delivered on V2R3 with APAR PH04130 (in 4Q 2018).



# IWQ support for IPSec

# Background Information: OSA-Express Inbound Workload Queueing (IWQ)

- OSA-Express separates inbound packets and routes them over four different ancillary input queues (AIQ) on the same interface
- z/OS can service each queue concurrently using separate processors
- Stack receives pre-sorted packets



# Overview

## Who (Audience)

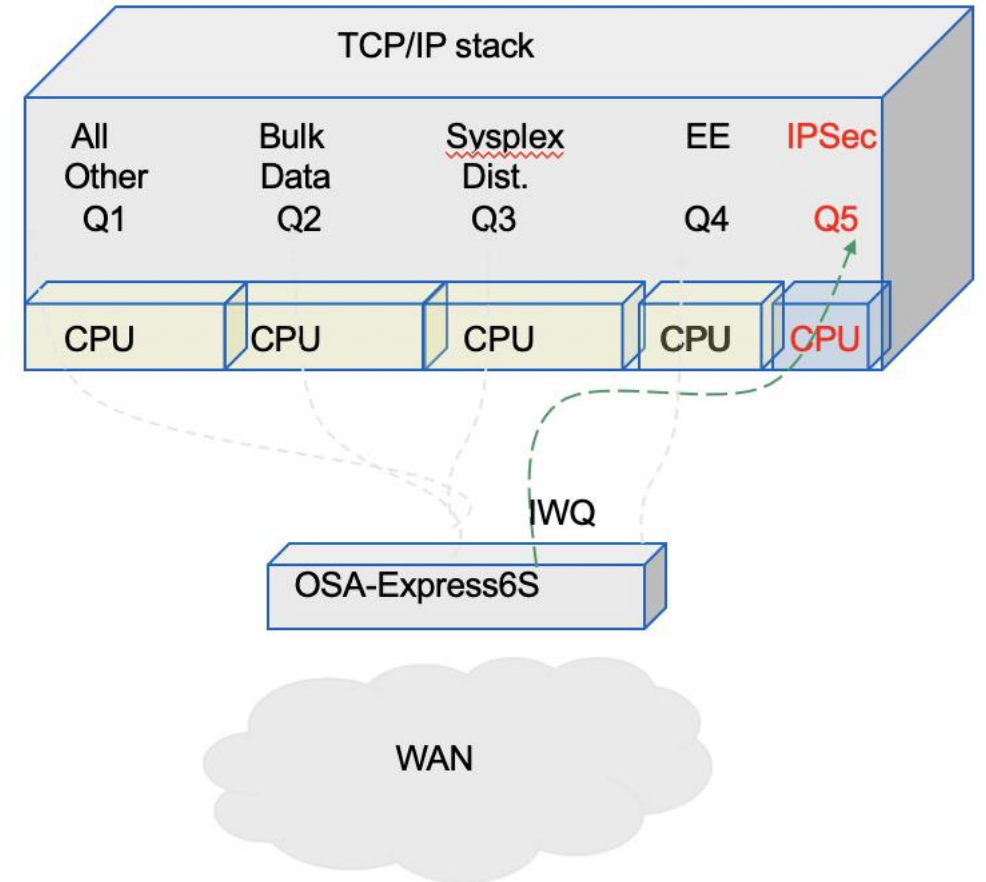
- z/OS network administrators

## What (Solution)

- With OSA-Express6S, inbound traffic separation for IPSec traffic is supported using a new ancillary input queue.

## Wow (Benefit / Value, Need Addressed)

- Significantly improves performance of inbound network traffic when IPSec is used for network encryption - up to 25% (IPSec) and 52% (non-IPSec) improvement measured in benchmarks



# Usage & Invocation

- No action required to enable IWQ for IPSec
  - Existing WORKLOADQ parameter on the INTERFACE statements enables IWQ for all supported traffic types
- Support also provided for z/OS V2R3 (in 2Q 2018) with APAR PI77649 and for z/OS V2R2 with APARs PI77649 and OA52275

# Dependencies

- **Hardware Dependencies**

- OSA-Express6S or above
- z14 server or later

See the 3906DEVICE or 3907DEVICE Preventive Service Planning (PSP) bucket

# Migration considerations

- **Migration**

- If you have enabled QDIO inbound workload queuing (WORKLOADQ) and you have IPSec traffic, the IWQ IPSec function (input queue) will automatically be enabled
- Each Ancillary Input Queue increases storage utilization in the following two areas:  
Approximately 36 KB of fixed ECSA and 4MB of fixed CSM HVCOMMON for READSTORAGE
- The new input queue will not be used (and will not be backed by 4MB of storage) until the first IPSec tunnel is activated
- There are no configuration options for controlling each input queue type

- **2 new Health checks**

- **ZOSMIGV2R4PREV\_CS\_IWQSC***\_tcpipstackname*

**If IWQ and IPSec are enabled on the stack, but OSA is down-level** - warns about checking storage for new ancillary queue before migrating to a new OSA-E6 or later card.

- **CSTCP\_IWQ\_IPSEC***\_tcpipstackname*

**If IWQ and IPSec are enabled on the stack, and OSA supports IWQ for IPSec** – warns about ensuring sufficient storage for new ancillary queue that was added

# Installation

- **Planning considerations**

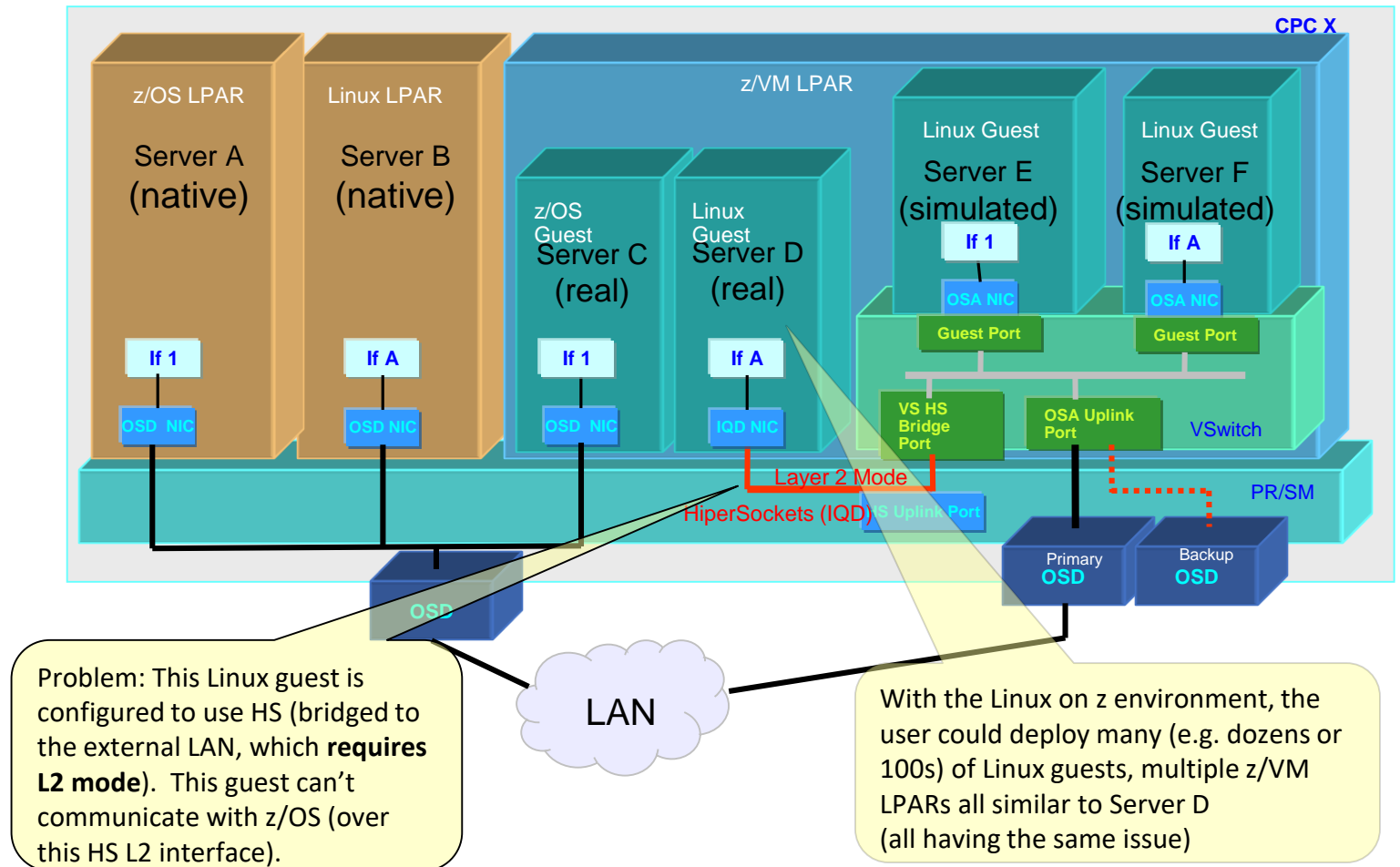
- Verify that sufficient ECSA is available
- Verify that sufficient real (fixed) storage is available  
See z/OS Migration book for details
- IWQ is not supported:
  - for DEVICE/LINK definitions
  - when z/OS is running as a z/VM guest with simulated devices (VSWITCH or guest LAN)

# HiperSockets Converged Interface Support

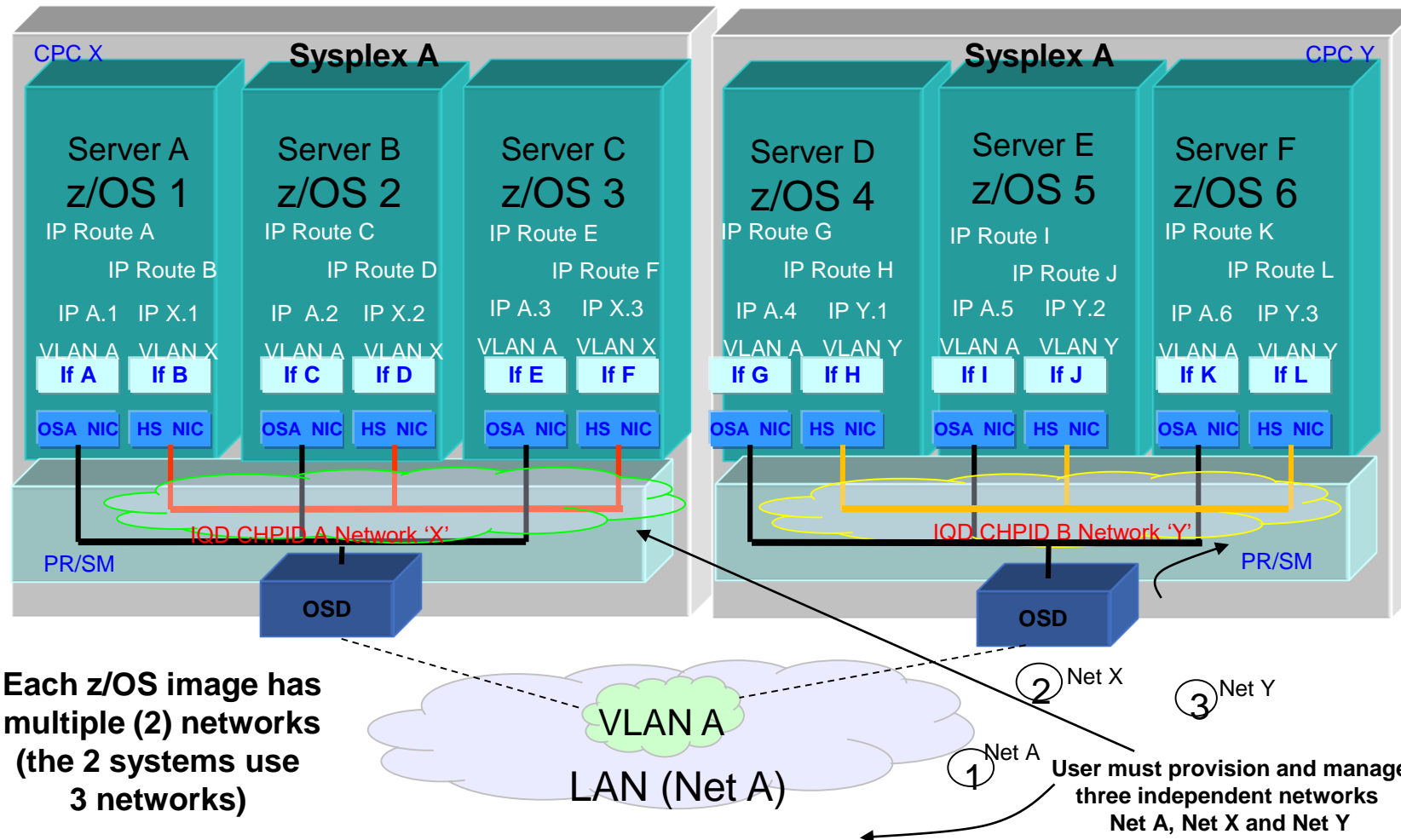


# Background Information: Incompatibility issue

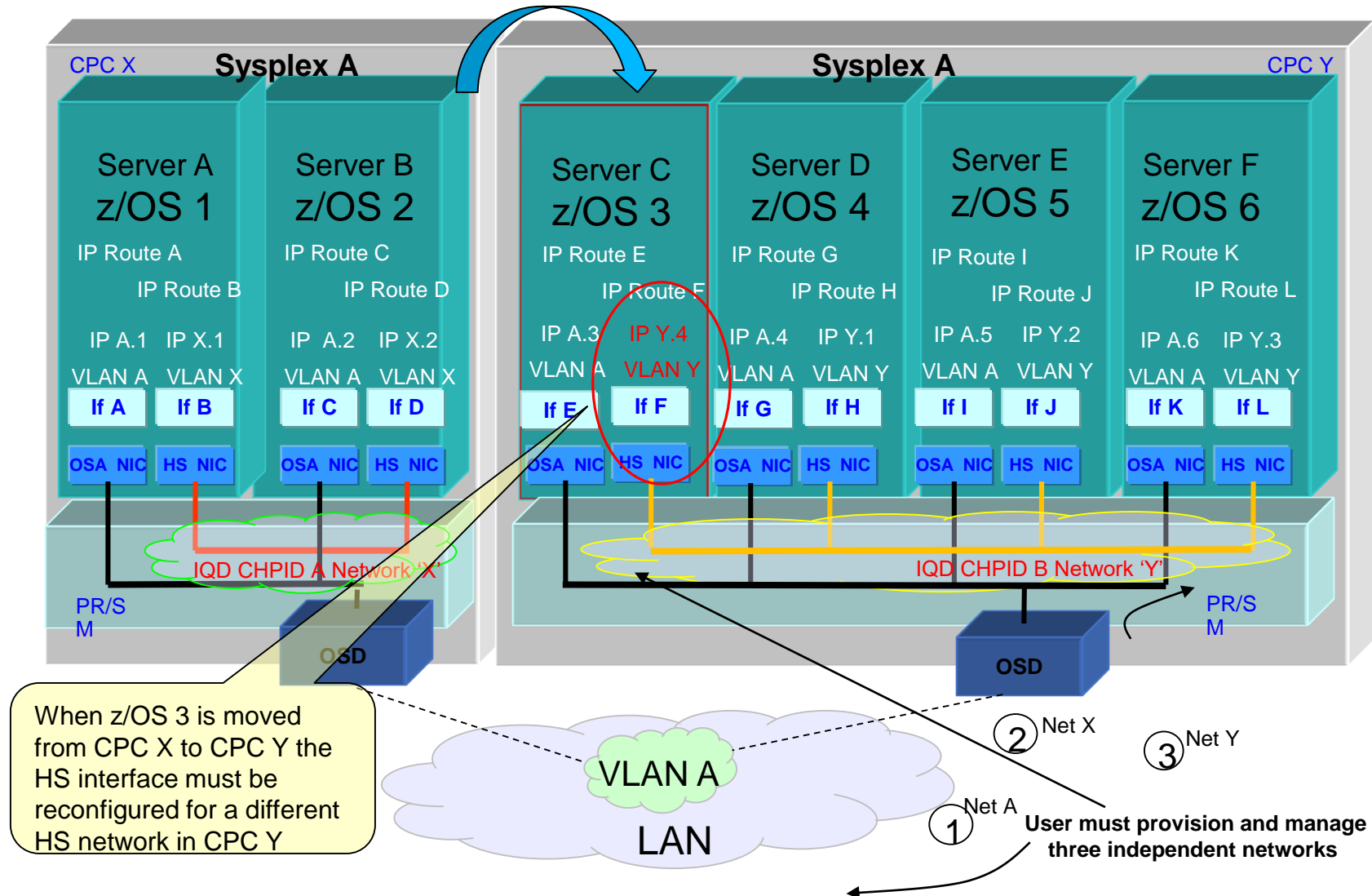
- OSA/HiperSockets (QDIO) architecture defines two “transport” modes of adapter connectivity:
  - Layer 3 mode (IP address routing) or
  - Layer 2 mode (MAC routing)
- LPARs using HiperSockets in Layer 2 mode **can not** communicate with LPARs in Layer 3 mode (note. OSA can bridge L2 to L3 hosts sharing the same OSA)
- z/OS only supports L3 mode, Linux supports both modes.



# Background Information: Usability issue



# Background Information: Usability issue (contd.)



# Overview

## **Who (Audience)**

- z/OS network administrators

## **What (Solution)**

- HiperSockets converged interface support for z/VM bridge Layer 2 environment
- Allows configuration of HiperSockets on z/OS without defining additional network interfaces/networks

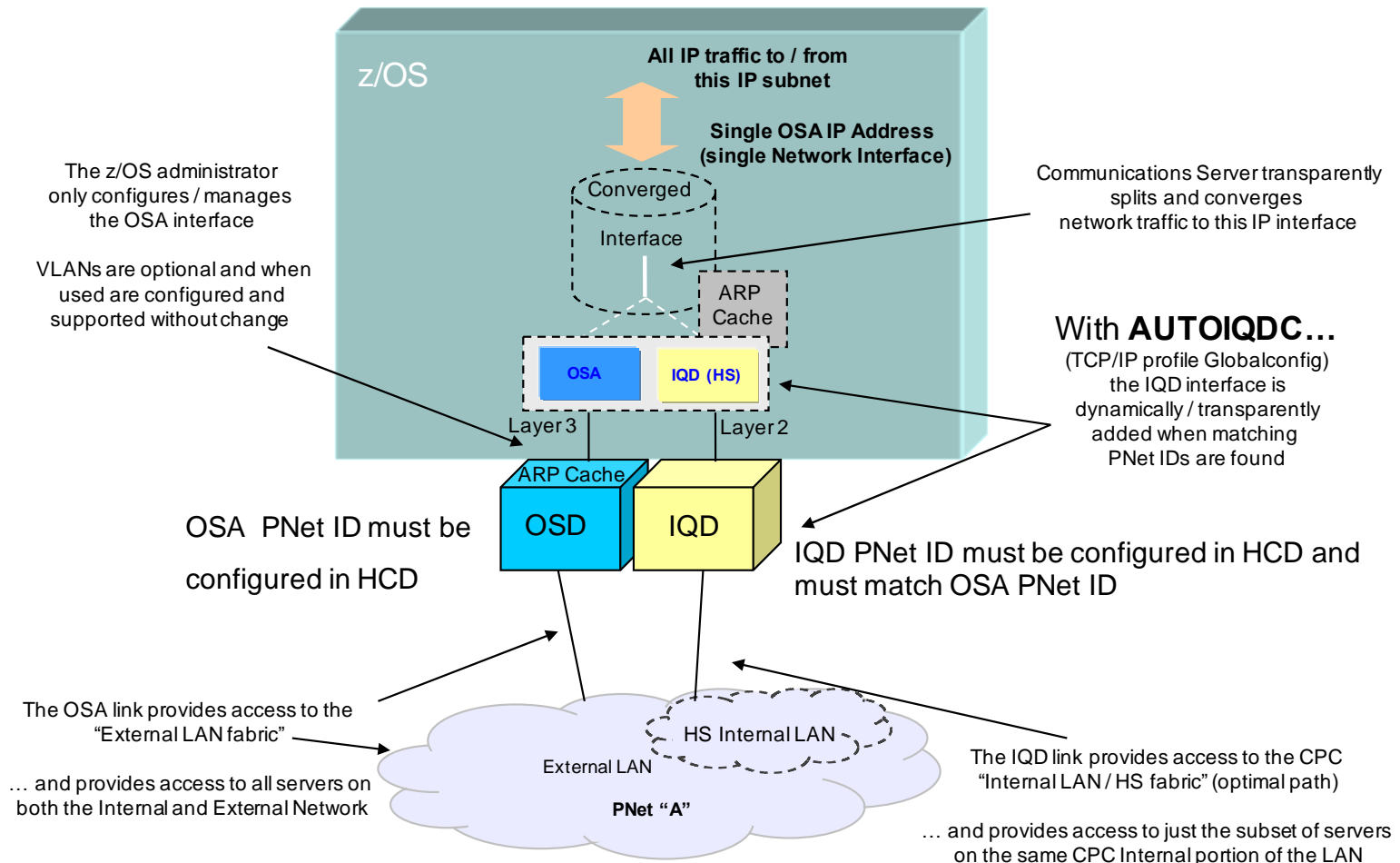
## **Wow (Benefit / Value, Need Addressed)**

- z/OS network administrators can now exploit HiperSockets for connectivity to Linux on z and z/OS systems with minimal effort

# Usage & Invocation

## z/OS HiperSockets Converged Interface (HSCI)

No matter how many OSA interfaces or variations are used, a single IQD device is used (per stack per IP version per PNetID). The first associated OSA activates the IQD device and the last OSA interface that terminates will also terminate the IQD device.



# Usage & Invocation (contd.)

- In the TCP/IP Profile
- New parameters on the GLOBALCONFIG statement: AUTOIQDC | NOAUTOIQDC
  - Sub-parameter on AUTOIQDC ALLTRAFFIC | NOLARGEDATA

Example: AUTOIQDC ALLTRAFFIC  
Default value: NOAUTOIQDC  
Sub-parameter default value: ALLTRAFFIC
- Support also provided for z/OS V2R3 Communications Server (in 1Q 2018) with APARs PI83372 and OA53198

# Usage & Invocation (contd.)

## z/OS Configuration Assistant for Communications Server updated to support Hipersockets Converged Interface

Welcome x Network Configu... x

Network Configuration Assistant (Home) > TCP/IP Profile > TCP/IP Profile : PLEX1.LPAR1.STACK1 > Network Interfaces > Global Interface Properties [Help](#)

### Global Interface Properties

Specify how long an ARP table entry remains valid:  
 (minutes) Range is 1 - 1440 Default is 20

Global Property Setting:  
Default taken for the following property. Configuration for this property will not be generated.

☐ Dynamically create Hipersockets Interfaces that are logically converged with OSA interfaces with matching PNetIDs for OSD CHIPIDs (IQDC interfaces) (Available beginning with V2R3.)

☒ **Customize the following property. Configuration will be generated to enable or disable this property.**

☐ Do not use IQDC interfaces for outbound TCP socket data transmissions of length 32KB or larger. Use IQDC interfaces for all other eligible outbound traffic.

[Configure settings if this TCP/IP is in an ensemble...](#)

[Other advanced settings...](#)

OK Cancel Reset

Welcome x Network Configu... x

Network Configuration Assistant (Home) > TCP/IP Profile > TCP/IP Profile : PLEX1.LPAR1.STACK1 > Network Interfaces > Global Interface Properties [Help](#)

### Global Interface Properties

Specify how long an ARP table entry remains valid:  
 (minutes) Range is 1 - 1440 Default is 20

Global Property Setting:  
Customize the following property. Configuration will be generated to enable or disable this property.

☒ Dynamically create Hipersockets Interfaces that are logically converged with OSA interfaces with matching PNetIDs for OSD CHIPIDs (IQDC interfaces) (Available beginning with V2R3.)

☐ Use IQDC interfaces for all eligible traffic between LPARs in this CEC.

☐ Do not use IQDC interfaces for outbound TCP socket data transmissions of length 32KB or larger. Use IQDC interfaces for all other eligible outbound traffic.

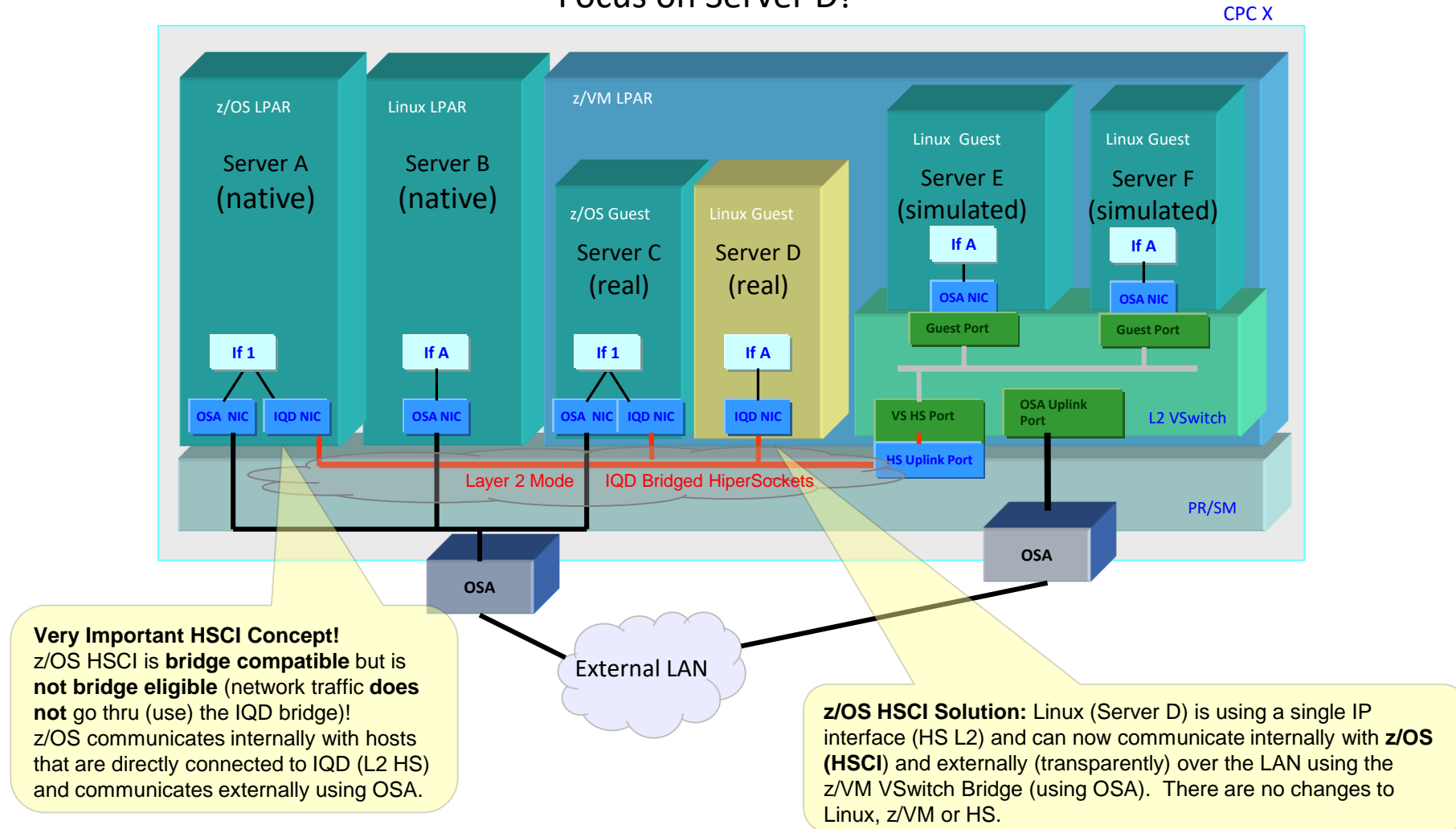
[Configure settings if this TCP/IP is in an ensemble...](#)

[Other advanced settings...](#)

OK Cancel Reset

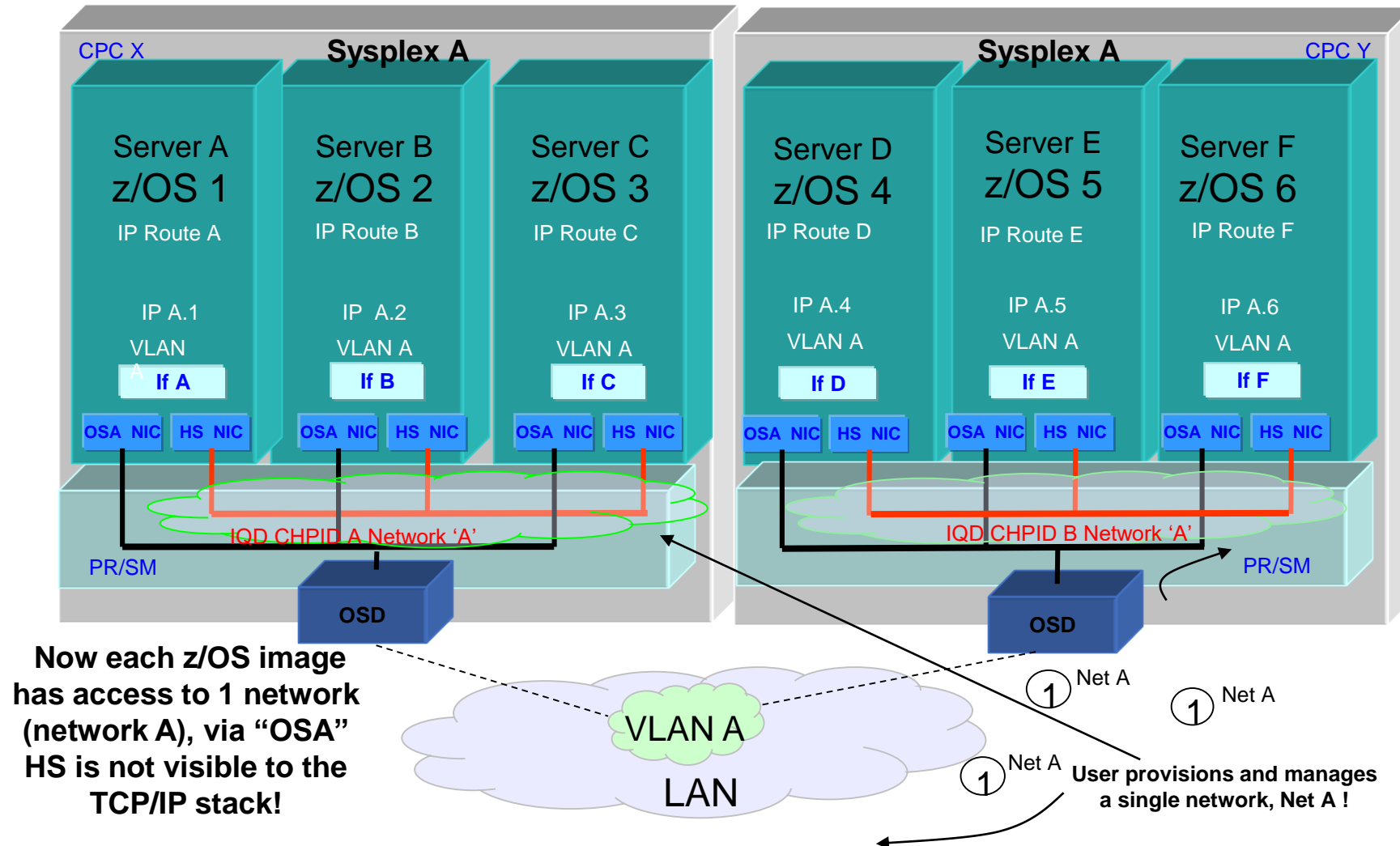
# Usage & Invocation (contd.)

Focus on Server D!

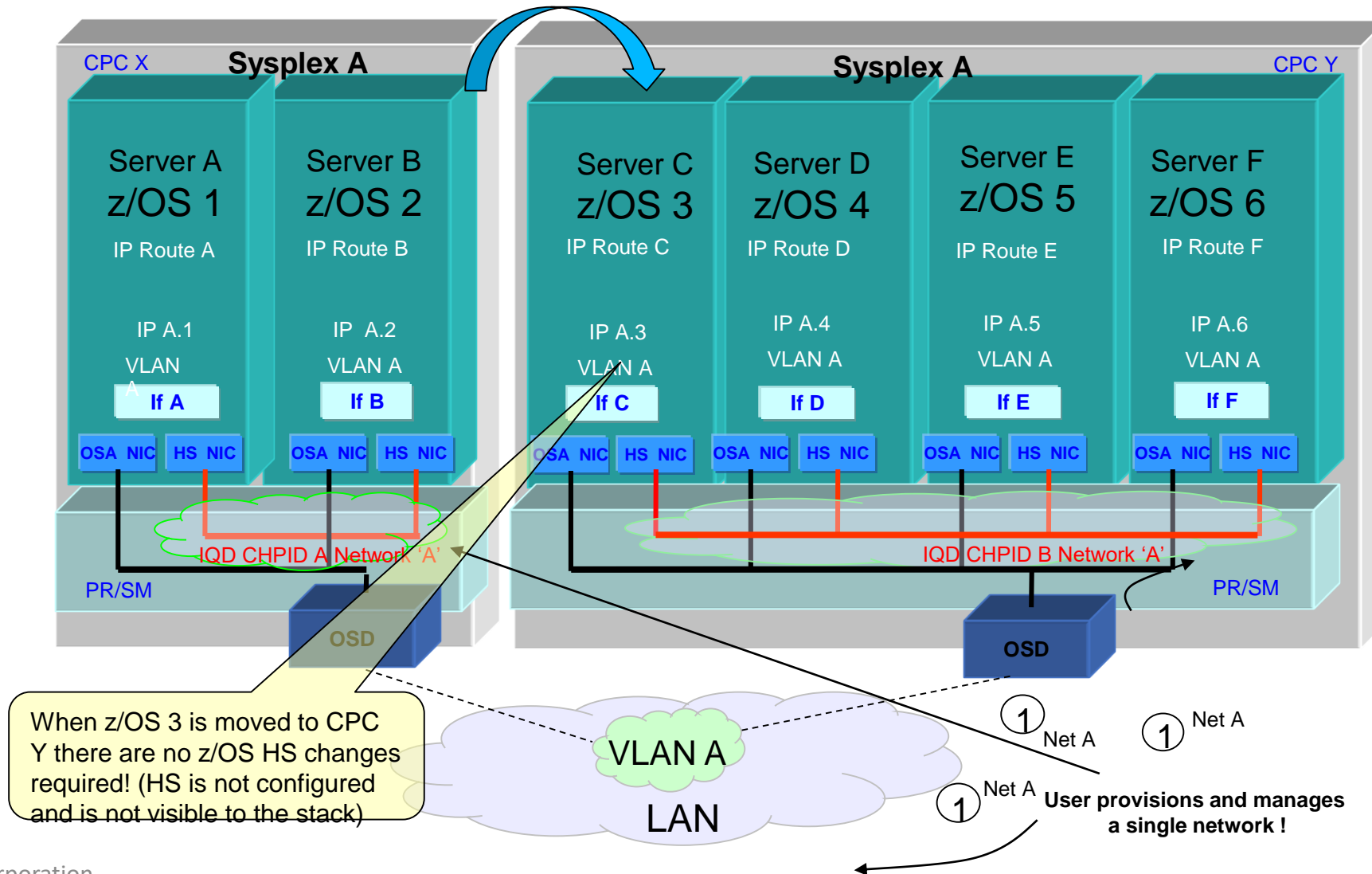




# Usage & Invocation (contd.)



# Usage & Invocation (contd.)



# Coexistence considerations

- **Coexistence considerations**
  - When using HSCI for z/OS to z/OS, both z/OS instances must be at V2R4 (or V2R3 with APARs).

# Installation

- **Planning considerations**

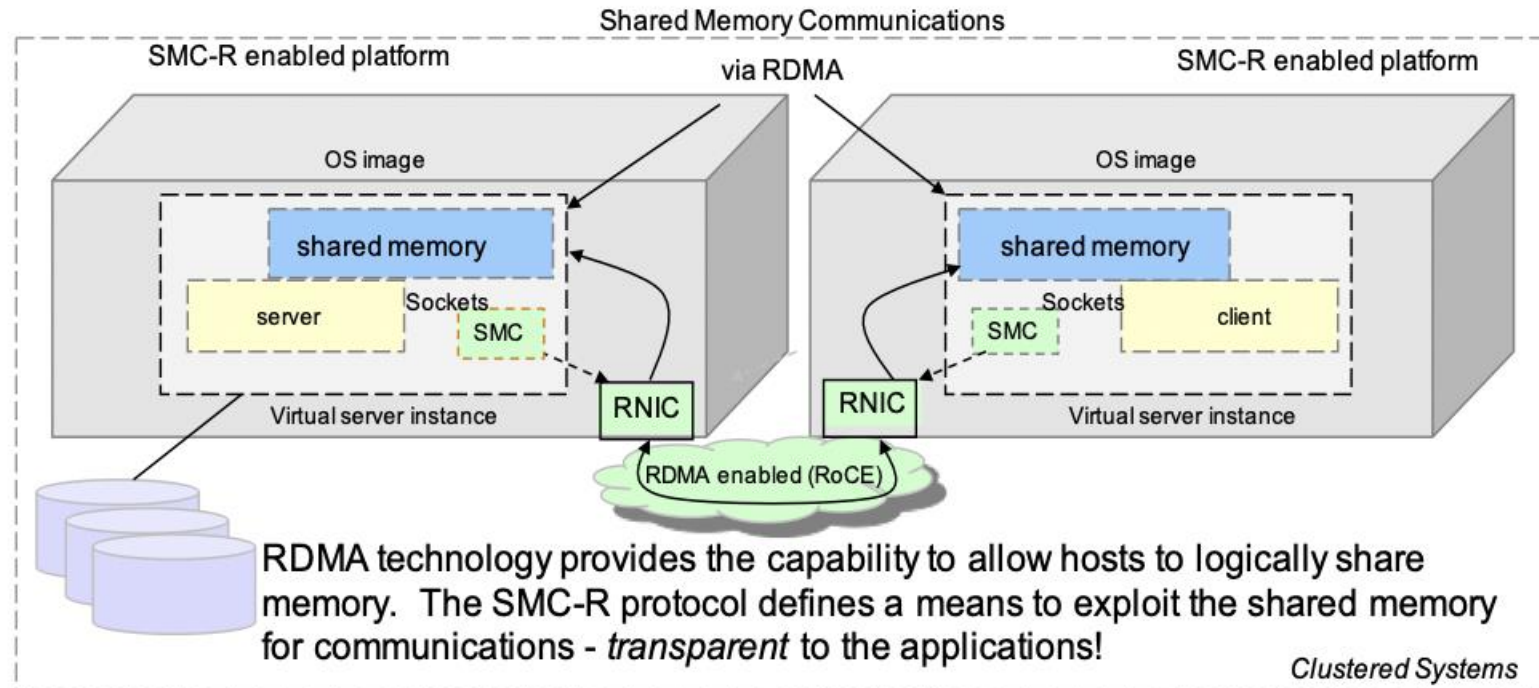
- Software configuration: In addition to enabling AUTOIQDC, the configuration for OSA (OSD) requires:
  - INTERFACE statement (dev/link is not supported for HSCI)
  - VMAC (OSA generated, a user defined VMAC is not supported)  
Note. VLAN ID is optional. If configured it will be duplicated on the HSCI.
- Hardware configuration
  - IQD CHPID:
    - Must have a PNetID<sup>1</sup> and External Bridge configured
    - The number of required IQD channel devices per TRLE: Two devices (read/write) are required for control + one additional device per TCP/IP stack, up to 8 stacks for a total of 10 devices per TRLE. A TRLE is created for each IP version (up to 2 TRLEs). TRLEs are created for each unique IQD CHPID (PNetID)<sup>1</sup>.
    - IQD Max Frame Size **Recommendation**: Use (at least) 24k (16k MTU)
  - OSD CHPID(s) must have a PNetID<sup>1</sup> configured that matches your IQD (External Bridge) CHPID PNetID

## Notes

1. When using SMC-R or SMC-D, both OSA and IQD might already have PNetID configured. PNetIDs are configured on a port basis in HCD and represent a user defined “Physical Network ID” for the physical network that this port will be connected.

# z/OS and Linux SMC Interoperability and Performance Testing

# Background information – Shared Memory Communications over Remote Direct Memory Access (SMC-R)

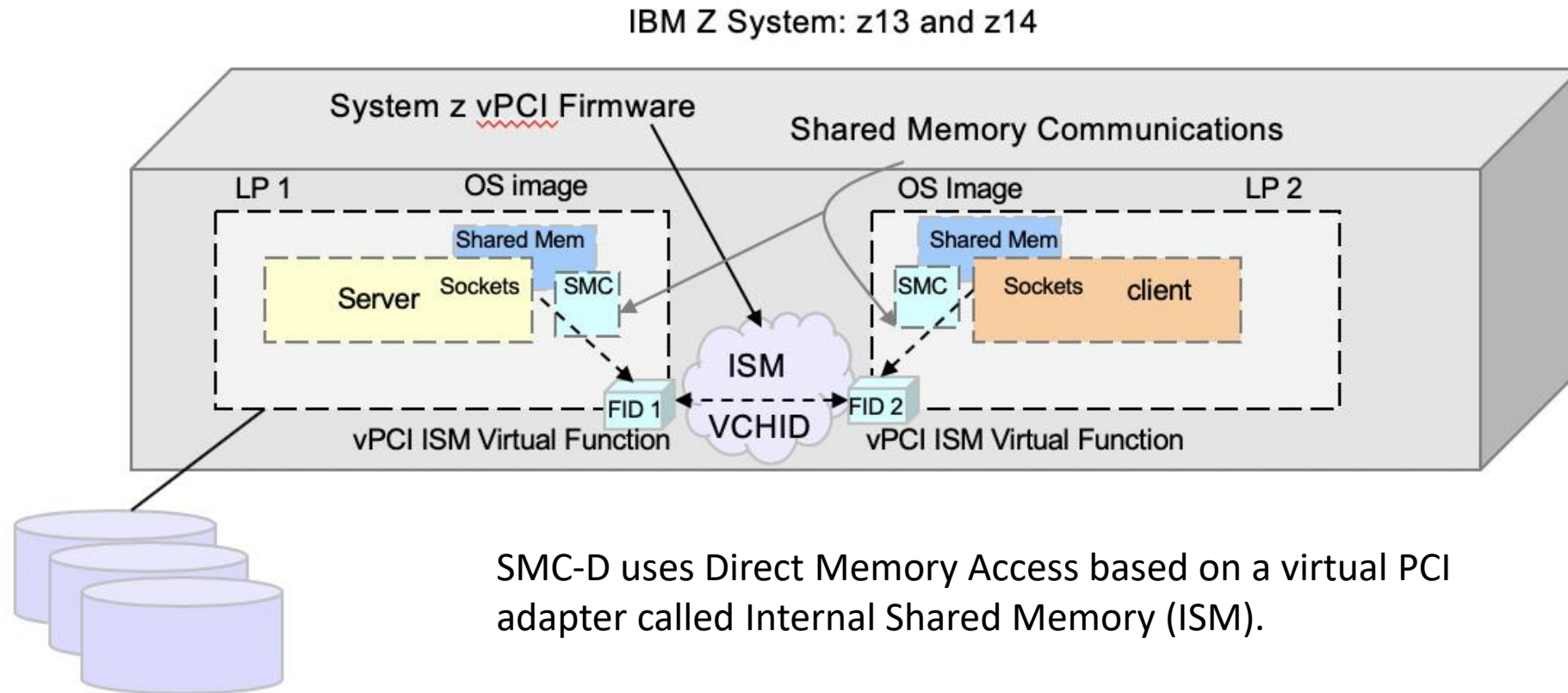


SMC-R is an *open* sockets over RDMA protocol that provides transparent exploitation of RDMA (for TCP based applications) while preserving key functions and qualities of service from the TCP/IP ecosystem that enterprise level servers/network depend on!

IETF RFC for SMC-R:

<http://www.rfc-editor.org/rfc/rfc7609.txt>

# Background Information – Shared Memory Access – Direct memory Access (SMC-D)



# Overview

## **Who (Audience)**

- z/OS and Linux system administrators

## **What (Solution)**

- Linux on Z Systems Shared Memory Communications support – drove test requirements for z/OS and Linux interoperability and performance testing for SMC-R and SMC-D

## **Wow (Benefit / Value, Need Addressed)**

- Benefits from the savings offered by SMC for z/OS to Linux co-located workloads as well as Linux to Linux workloads



# Dependencies

- **Software Dependencies**
  - Linux distributions with SMC support
    - Ubuntu: 18.10
    - SuSE: SLES 12 SP4

# Communications Server Miscellaneous enhancements

# Overview - Resolver

- Resolver communicates with DNS to find hostname or IP information as requested by the applications
- Resolver can cache these results to use for future requests
- When DNS can't find a hostname it returns an NX record (non-existent)
- DNS returns a time-to-live (TTL) with each record that tells resolver how long to keep the entry in a cache
- Resolver's MAXTTL parameter allows you to further limit cache entry TTL

# Overview

## **Who (Audience)**

- System administrators

## **What (Solution)**

- Resolver is enhanced to allow specifying time-to-live for negative cache entries and display the name of the most recently used resolver setup file

## **Wow (Benefit / Value, Need Addressed)**

- More control on how long negative cache entries are kept in the cache

# Usage & Invocation

- In the Resolver setup file
- New statement: MAXNEGTTT *time-to-live*  
Example: MAXNEGTTT 200  
Default value: Same as MAXTTT (configured or defaulted)
- MAXNEGTTT is ignored if caching is not enabled

# Overview – QDIO Read errors

## **Who (Audience)**

- System administrators

## **What (Solution)**

- VTAM TRLE display enhanced to display QDIO Read errors

## **Wow (Benefit / Value, Need Addressed)**

- Better diagnostics for when there is a read error in OSA

# Usage & Invocation

- TRLE display example:

```
IST924I -----  
IST2457I OSA DETECTED INBOUND ERRORS ON PRIMARY QUEUE:  
IST2458I  TOTAL INVALID INBOUND PACKETS = 23  
IST2459I  LAST INVALID INBOUND PACKET AT 03:39:00 ON 02/06/19  
IST2460I  TOTAL INBOUND SBAL ERRORS    = 15  
IST2461I  LAST INBOUND SBAL ERROR AT 01:21:23 ON 02/05/19  
IST2462I  CONSECUTIVE SBAL ERRORS: LAST = 1 MAX = 5  
IST2463I  MAX CONSECUTIVE SBAL ERRORS AT 11:23:45 ON 08/24/18  
IST924I -----
```

# Session Summary

- Sysplex Notification of TCP/IP Stack Join or Leave
- OSA-Express7S 25GbE Support
- Communications Server support for 25GbE RoCE Express2 features
- Code page enhancements for CSSMTP
- z/OS Encryption Readiness Technology (zERT) aggregation
- z/OS Encryption Readiness Technology (zERT) Network Analyzer
- TN3270E Telnet Server Express Logon Feature support for Multi-Factor Authentication
- Network Configuration Assistant support for multiple location TCP/IP configuration
- Multiple Installation support for Network Configuration Assistant
- IWQ Support for IPSec
- HiperSockets Converged Interface Support
- z/OS and Linux SMC Interoperability and Performance Testing
- Communications Server Miscellaneous enhancements



# Statement of Directions for V2R4

## 1. Withdrawal of ISPF Workstation Agent (WSA)

z/OS V2.4 is planned to be the last release to support the ISPF Workstation Agent (WSA), also known as the ISPF Client/Server Component. WSA is an application that runs on your local workstation and maintains a connection between the workstation and the ISPF host. It is primarily used to transfer files between the workstation and the host. IBM recommends using more current file transfer solutions such as those provided by the Zowe Dataset Explorer, z/OS FTP, and similar file transfer mechanisms. These solutions have more capabilities, including the ability to provide secure communications.

## 2. Withdrawal of CMIP

z/OS V2.4 is planned to be the last release to support the VTAM Common Management Information Protocol (CMIP). CMIP services is an API that enables a management application program to gather various types of SNA topology data from a CMIP application called the topology agent that runs within VTAM. IBM recommends using the SNA network monitoring network management interface (NMI) to monitor SNA Enterprise Extender and High Performance Routing data.

# Statement of Directions for V2R4 (contd.)

## **3. Removal of native TLS/SSL support from TN3270E Telnet server, FTP server, and DCAS**

z/OS V2.4 is planned to be the last release in which the z/OS TN3270E Telnet server, FTP server, and Digital Certificate Access Server (DCAS) will support direct invocation of System SSL APIs for TLS/SSL protection. In the future, the only TLS/SSL protection option for these servers will be Application Transparent Transport Layer Security (AT-TLS). The direct System SSL support in each of these components is functionally outdated and only supports TLS protocols up through TLSv1.1. IBM recommends converting your TN3270E Telnet, FTP server, and DCAS configurations to use AT-TLS, which supports the latest System SSL features, including the TLSv1.2 and TLSv1.3 protocols and related cipher suites. Note that while native TLS/SSL support for z/OS FTP client is not being withdrawn at this time, no future enhancements are planned for that support. IBM recommends using AT-TLS to secure FTP client traffic.

# Statement of Directions for V2R4 (contd.)

## **4. Removal of policy data import function from the Network Configuration Assistant (NCA)**

z/OS V2.4 will be the last release that the Network Configuration Assistant z/OSMF plugin supports the policy data import function, which allows you to import existing Policy Agent configuration files into the Network Configuration Assistant. After z/OS V2.4, import of policy configuration files will no longer be supported for AT-TLS, IPSec, PBR, and IDS technologies.

## **5. Removal of Sysplex Distributor support for workload balancing to IBM DataPower Gateway products**

z/OS V2.4 is the last release to support Sysplex Distributor target controlled distribution to DataPower Gateway products. This feature is deprecated in the DataPower Gateway. IBM recommends that you implement another solution for workload balancing that might be through an external load balancer. This removal does not impact any other Sysplex Distributor functions, only configurations that have TARGCONTROLLED specified on the VIPADISTRIBUTE statement.

# Appendix

## z/OS Communications Server Publications

- z/OS Communications Server: IP and SNA Codes SC27-3648
- z/OS Communications Server: IP CICS Sockets Guide SC27-3649
- z/OS Communications Server: IP Configuration Guide SC27-3650
- z/OS Communications Server: IP Configuration Reference SC27-3651
- z/OS Communications Server: IP Diagnosis Guide GC27-3652
- z/OS Communications Server: IP IMS Sockets Guide SC27-3653
- z/OS Communications Server: IP Programmer's Guide and Reference SC31-8787
- z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference SC27-3660
- z/OS Communications Server: IP System Administrator's Commands SC31-8781
- z/OS Communications Server: IP User's Guide and Commands SC27-3662
- z/OS Communications Server: IPv6 Network and Application Design Guide SC27-3663
- z/OS Communications Server: New Function Summary GC31-8771
- z/OS Communications Server: SNA Network Implementation Guide SC27-3672
- z/OS Communications Server: SNA Operation SC31-8779
- z/OS Communications Server: SNA Resource Definition Reference SC27-3675

# Appendix

## Other Publications

- z/OS UNIX System Services Programming: Assembler Callable Services Reference SA23-2281
- z/OS XL C/C++ Runtime Library Reference SC14-7314
- z/OS Unicode Services User's Guide and Reference SA38-0680

# Key Contacts

- Chief Product Owner
  - Gus Kassimis ([kassimis@us.ibm.com](mailto:kassimis@us.ibm.com))
- Release Manager
  - Doris Bunn ([dbunn@us.ibm.com](mailto:dbunn@us.ibm.com))
- Chief Iteration Manager
  - Navya Ramanjulu ([navyaram@us.ibm.com](mailto:navyaram@us.ibm.com))
- Product Owners
  - Sam Reynolds ([samr@us.ibm.com](mailto:samr@us.ibm.com))
  - Christopher Meyer ([meyerchr@us.ibm.com](mailto:meyerchr@us.ibm.com))
  - Mike Fox ([mjfox@us.ibm.com](mailto:mjfox@us.ibm.com))
- IDD Coordinator
  - Yi Chen Zhang ([zhangyic@cn.ibm.com](mailto:zhangyic@cn.ibm.com))