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-bye 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

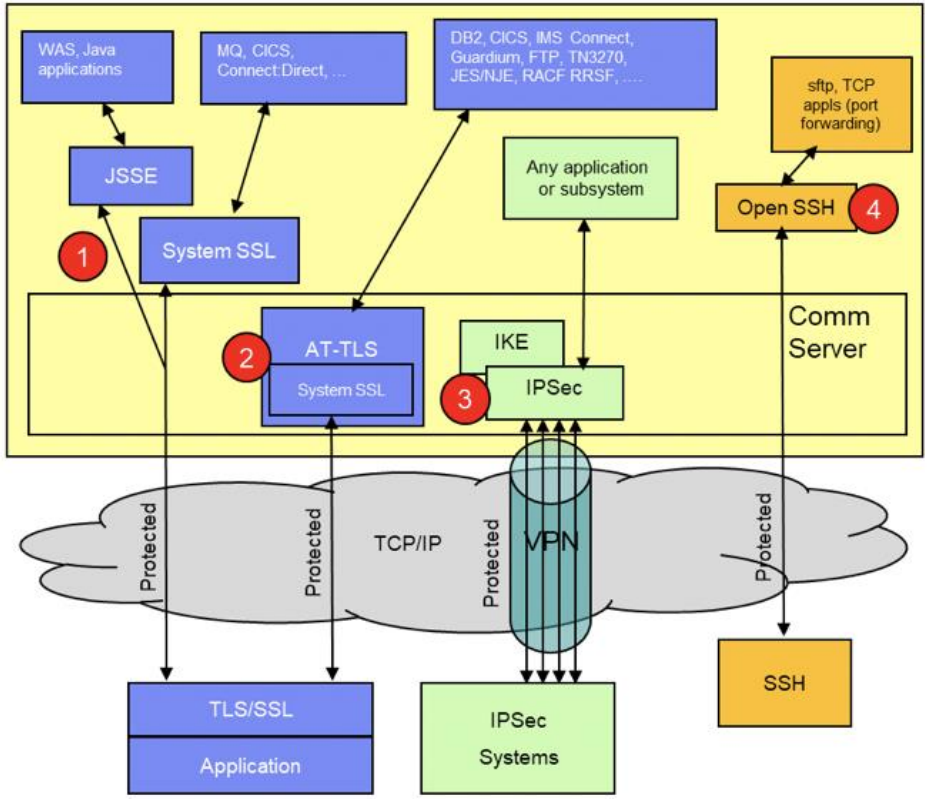
Migration considerations

- **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

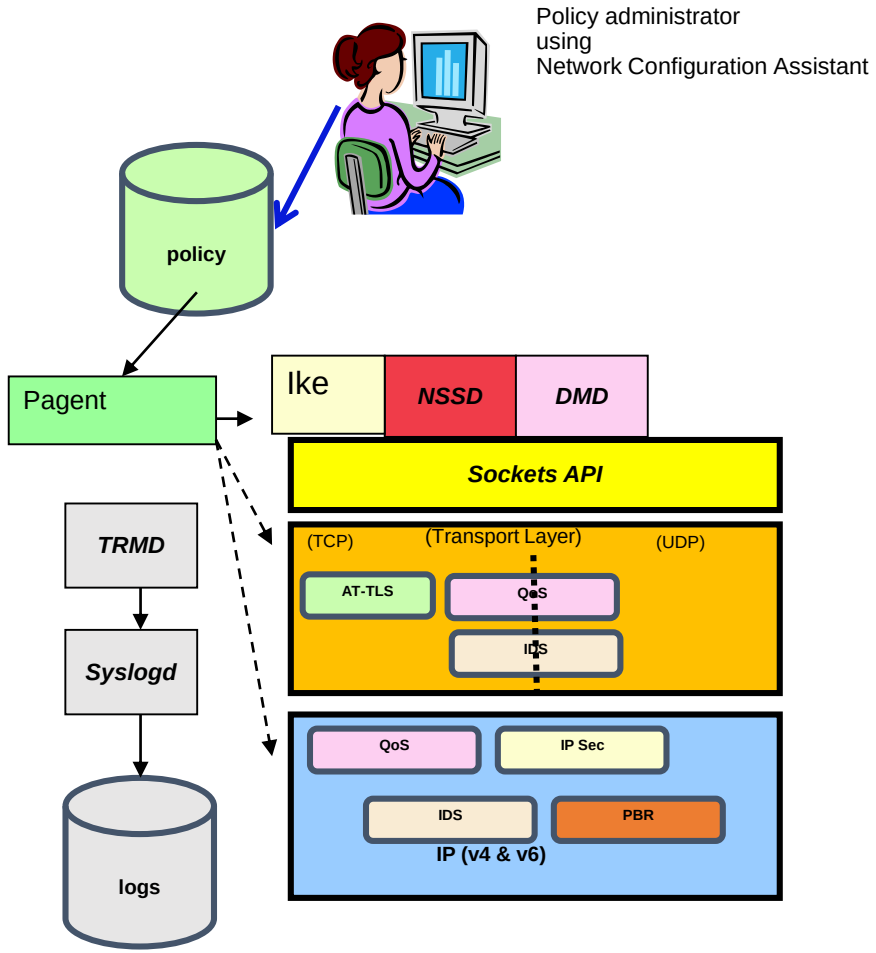
- ZERT SMF records and the NMI SYSTCPES service are enabled/disabled independently – one, both, or neither can be enabled

- 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)



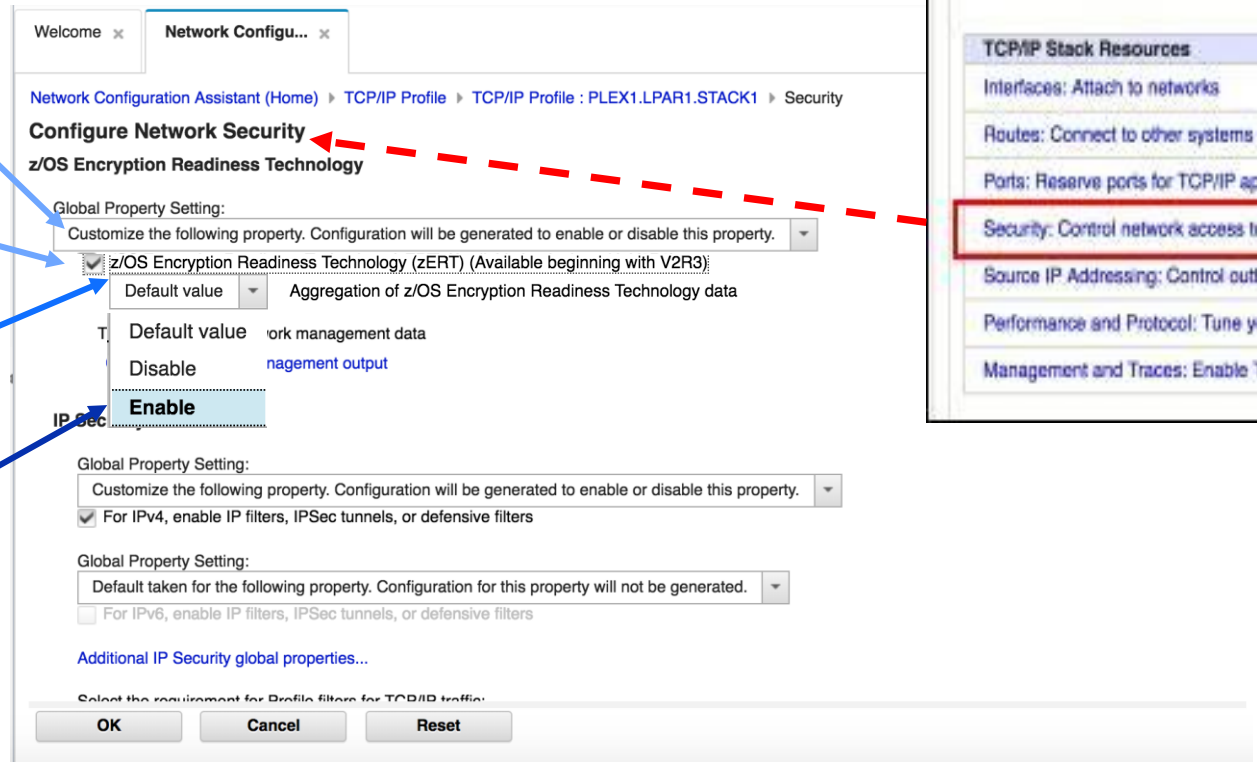
Usage & Invocation – NCA (contd.)

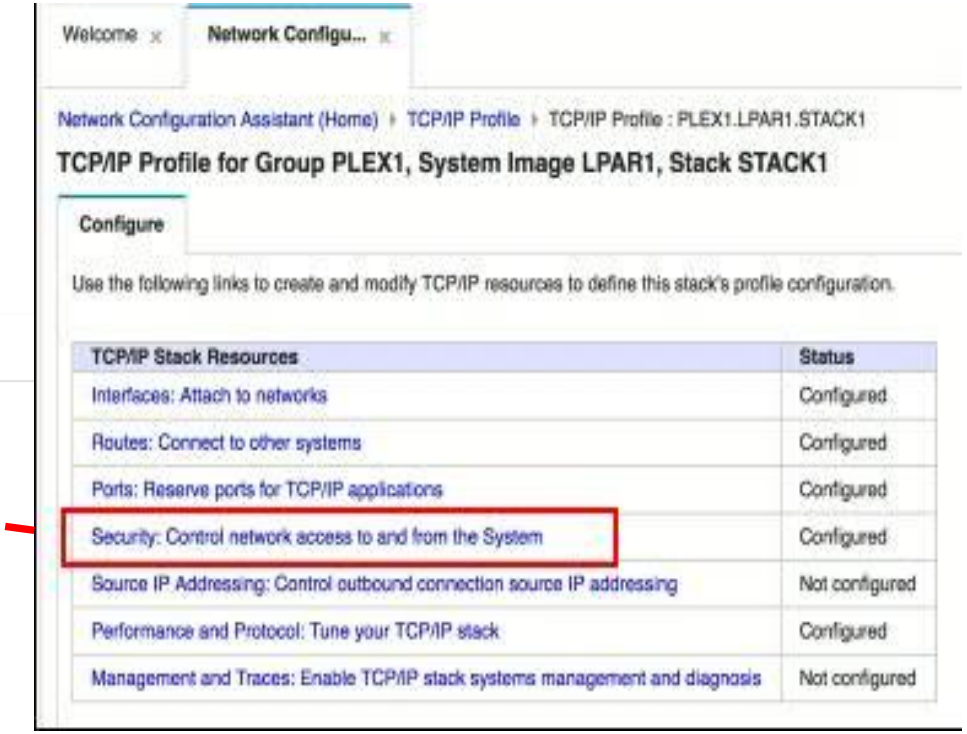
Click checkbox to enable zERT

Click checkbox to enable zERT

Click dropdown

Select Enable to turn on zERT Aggregation





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

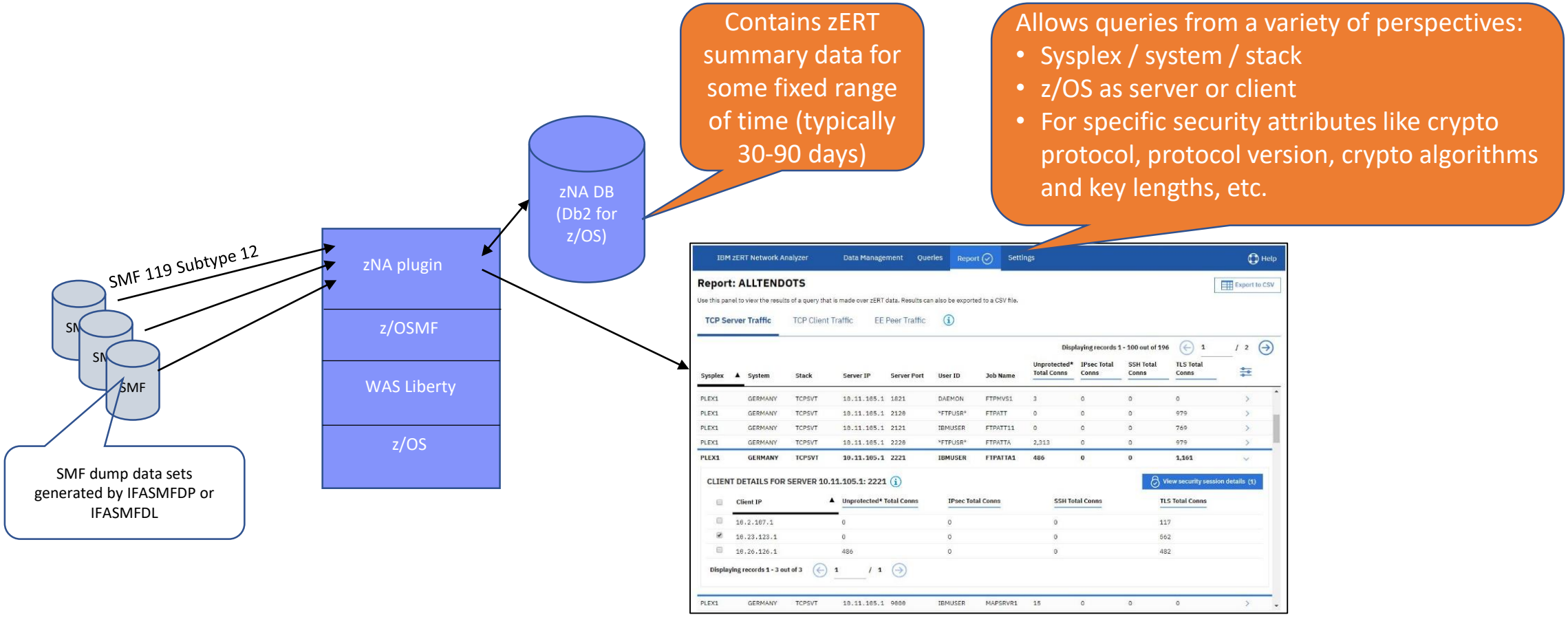
What (Solution)

- 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

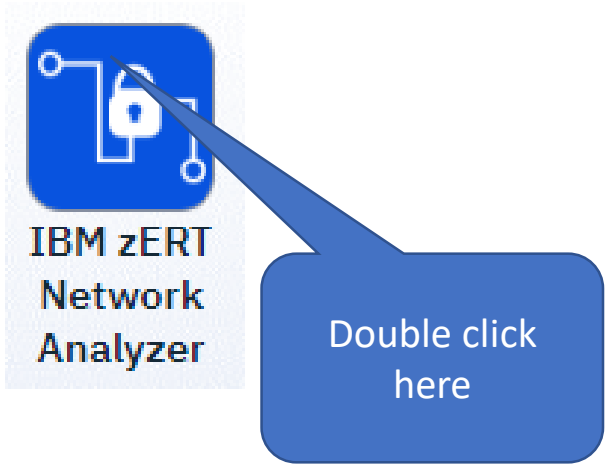
Usage & Invocation



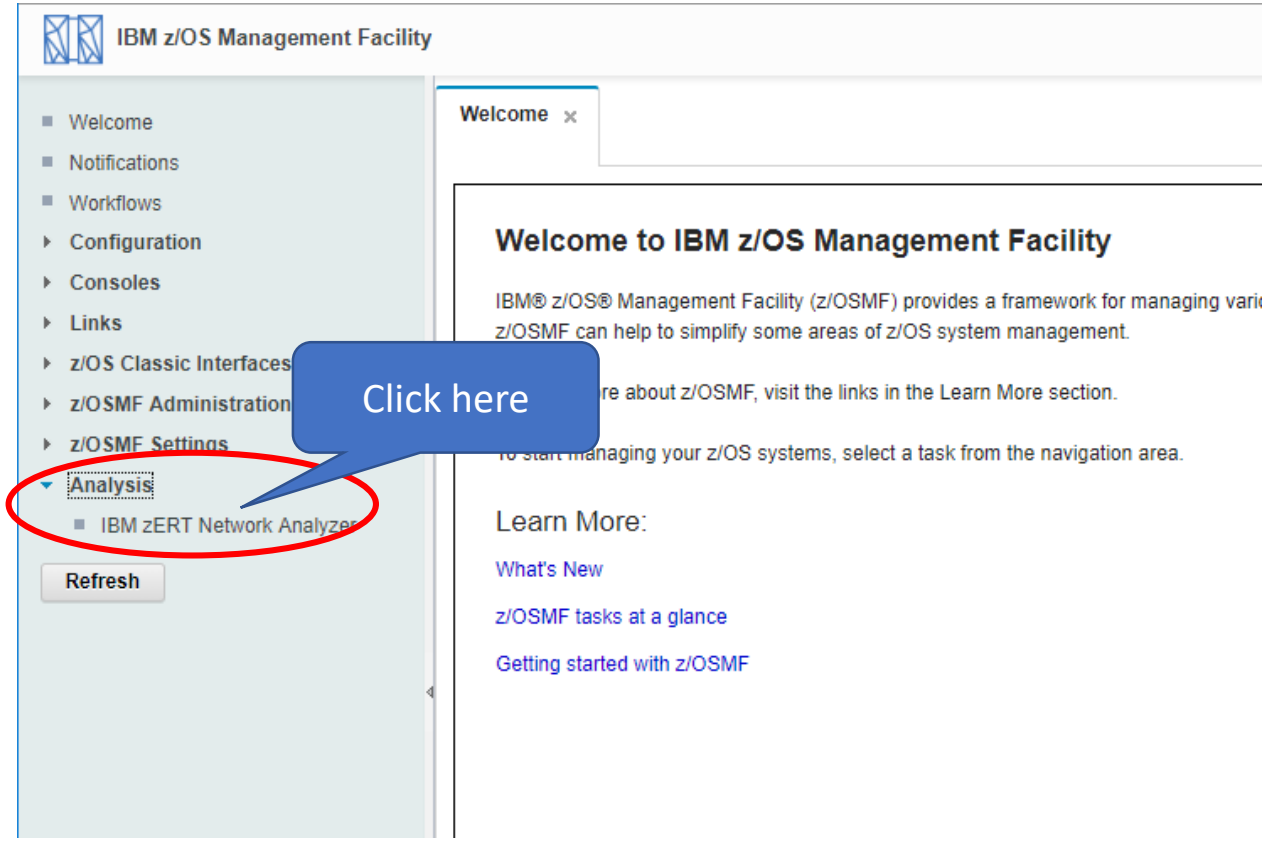
Support also provided for z/OS V2R3 (in 4Q 2018) with APAR PH03137

Usage & Invocation (contd.)

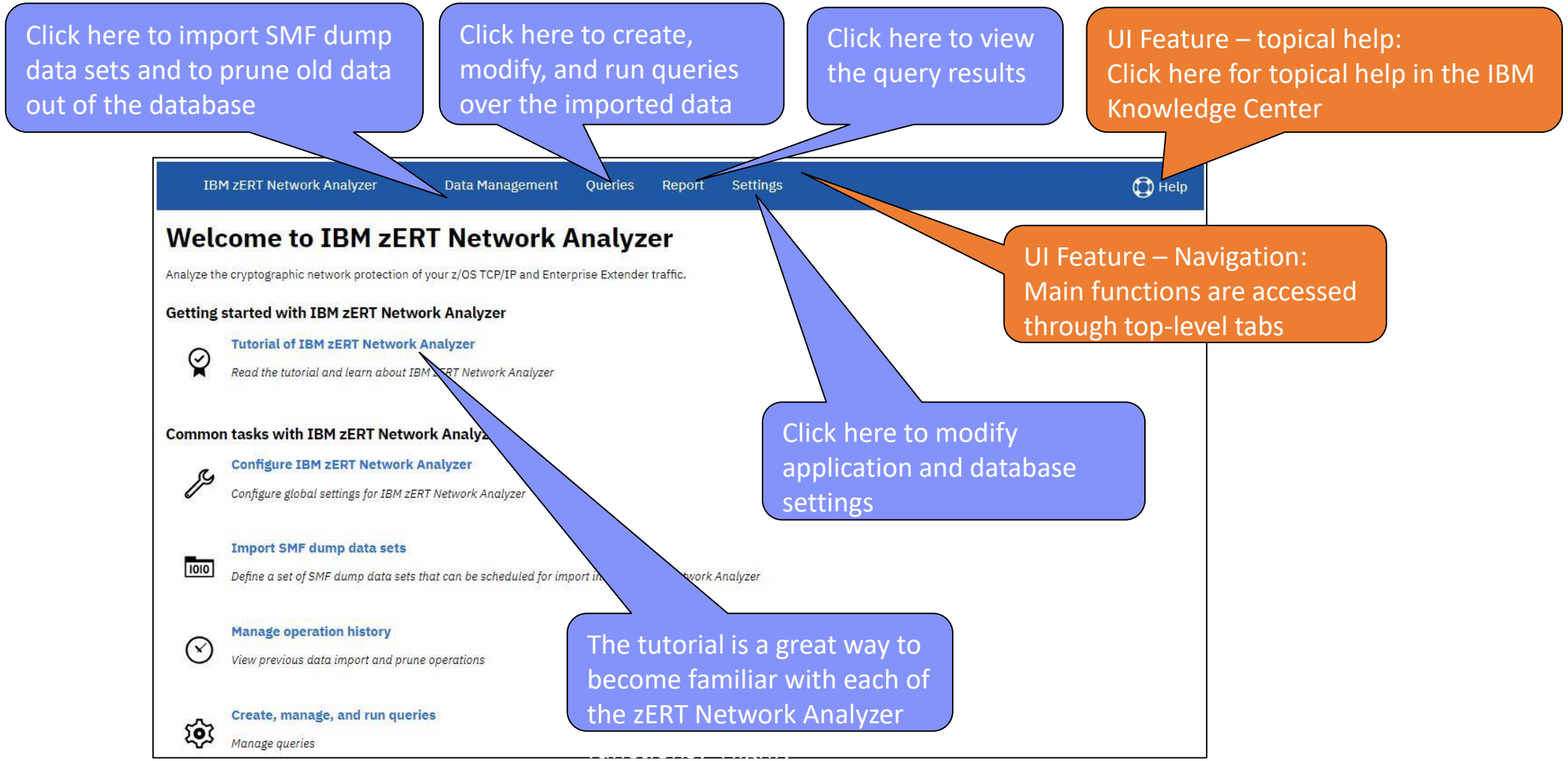
- z/OSMF Desktop mode:



- z/OSMF Classic mode:



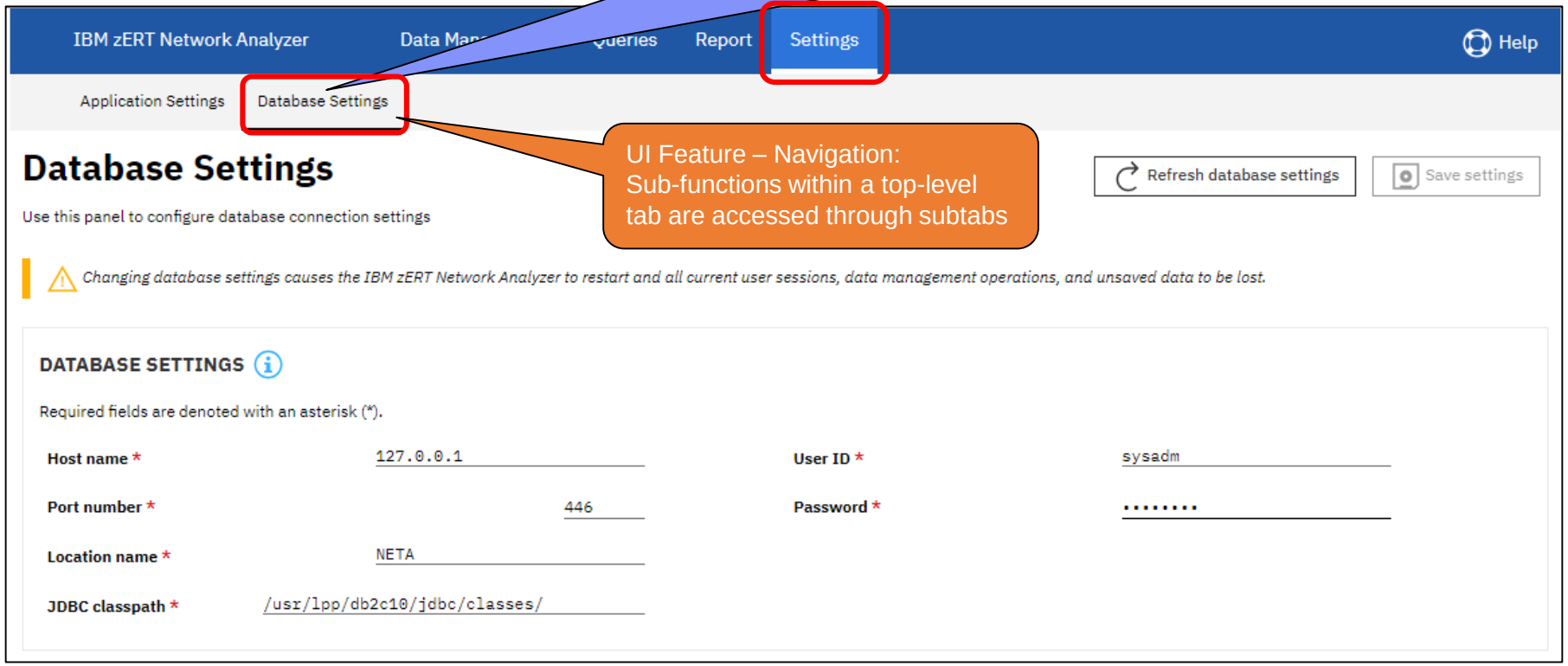
Usage & Invocation (contd.)



Usage & Invocation – Settings (1 of 2)

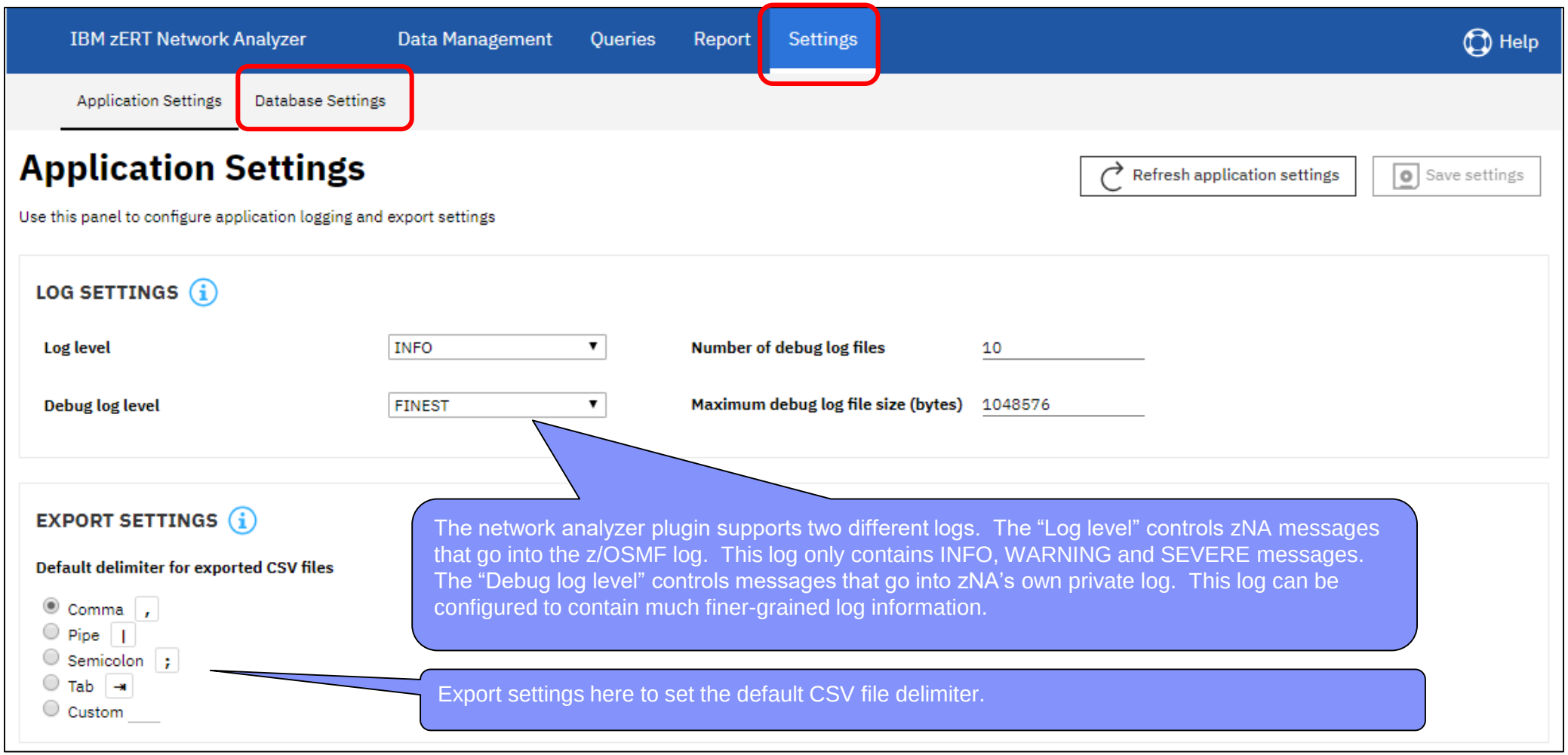
The first time a user logs into the zERT Network Analyzer after it is installed, they will be forced to this dialog to fill in the database configuration information. Until the correct information is saved, no other panels are accessible (other than Help and the Tutorial).

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.

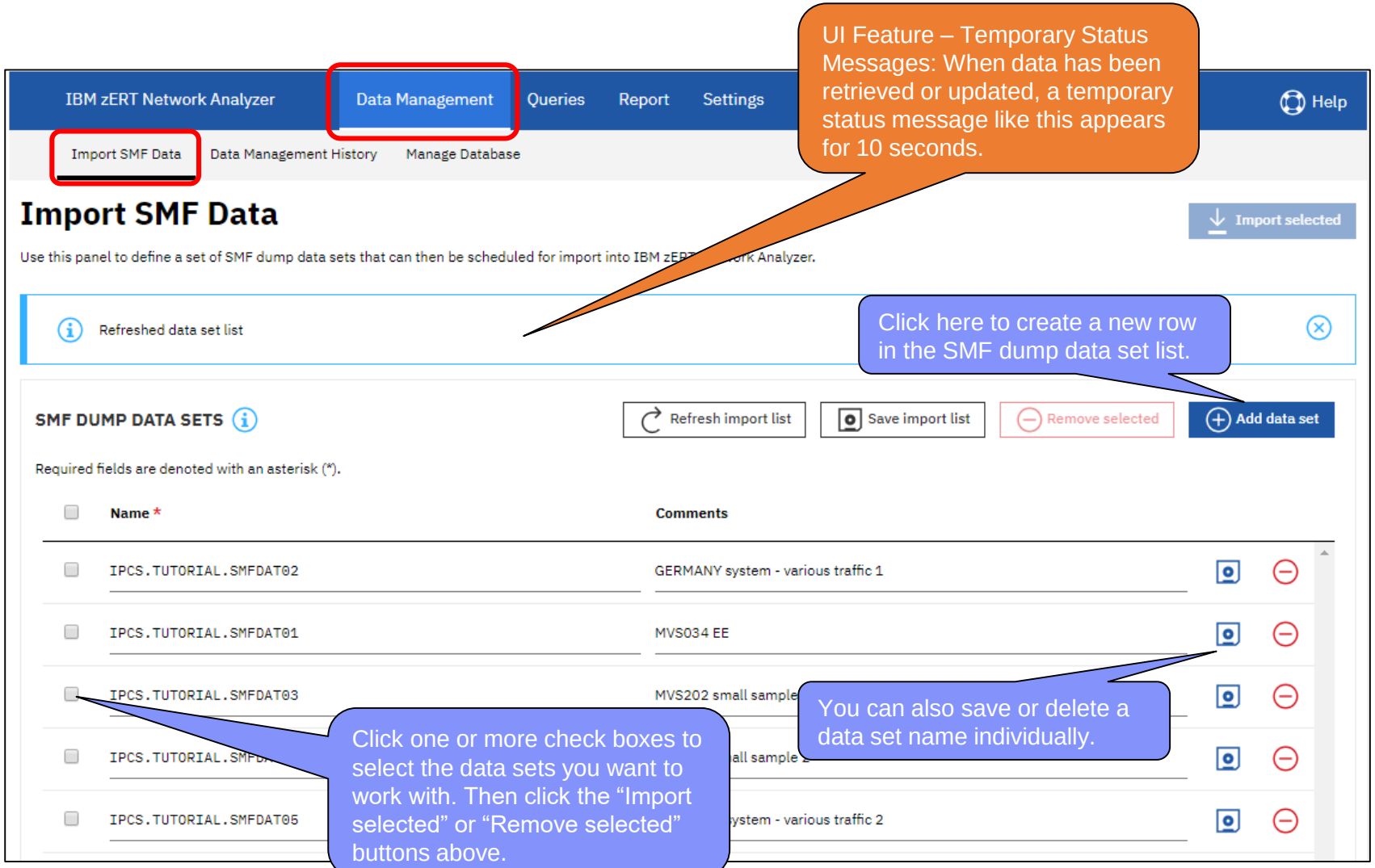


UI Feature – Navigation:
Sub-functions within a top-level tab are accessed through subtabs

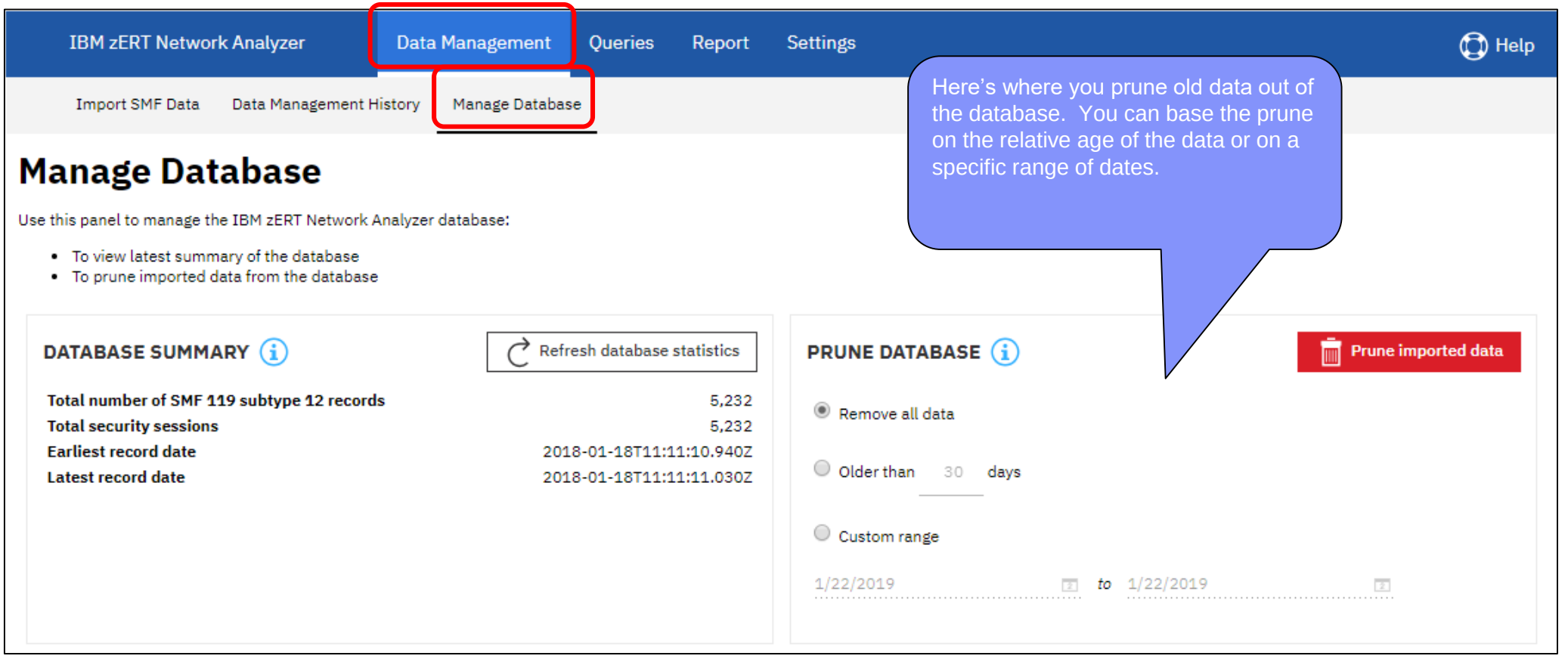
Usage & Invocation – Settings (2 of 2)



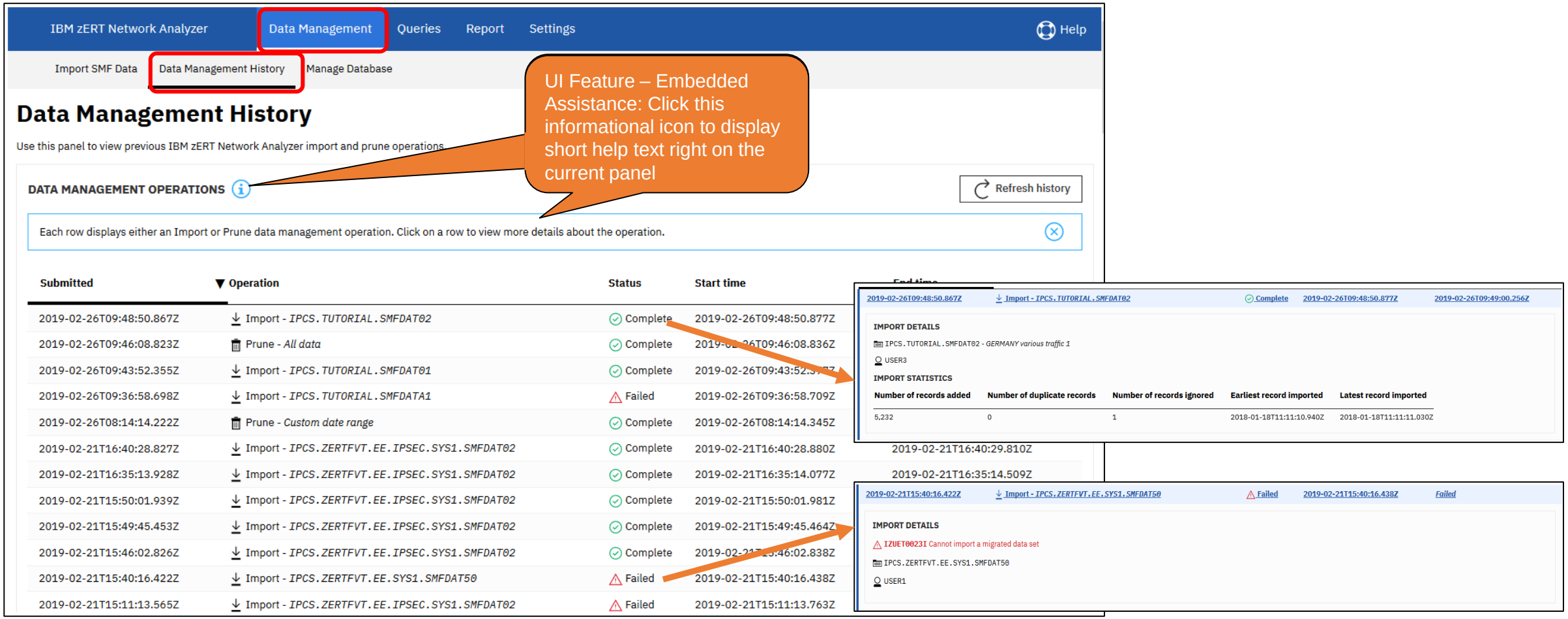
Usage & Invocation – Data management (1 of 3)



Usage & Invocation – Data management (2 of 3)

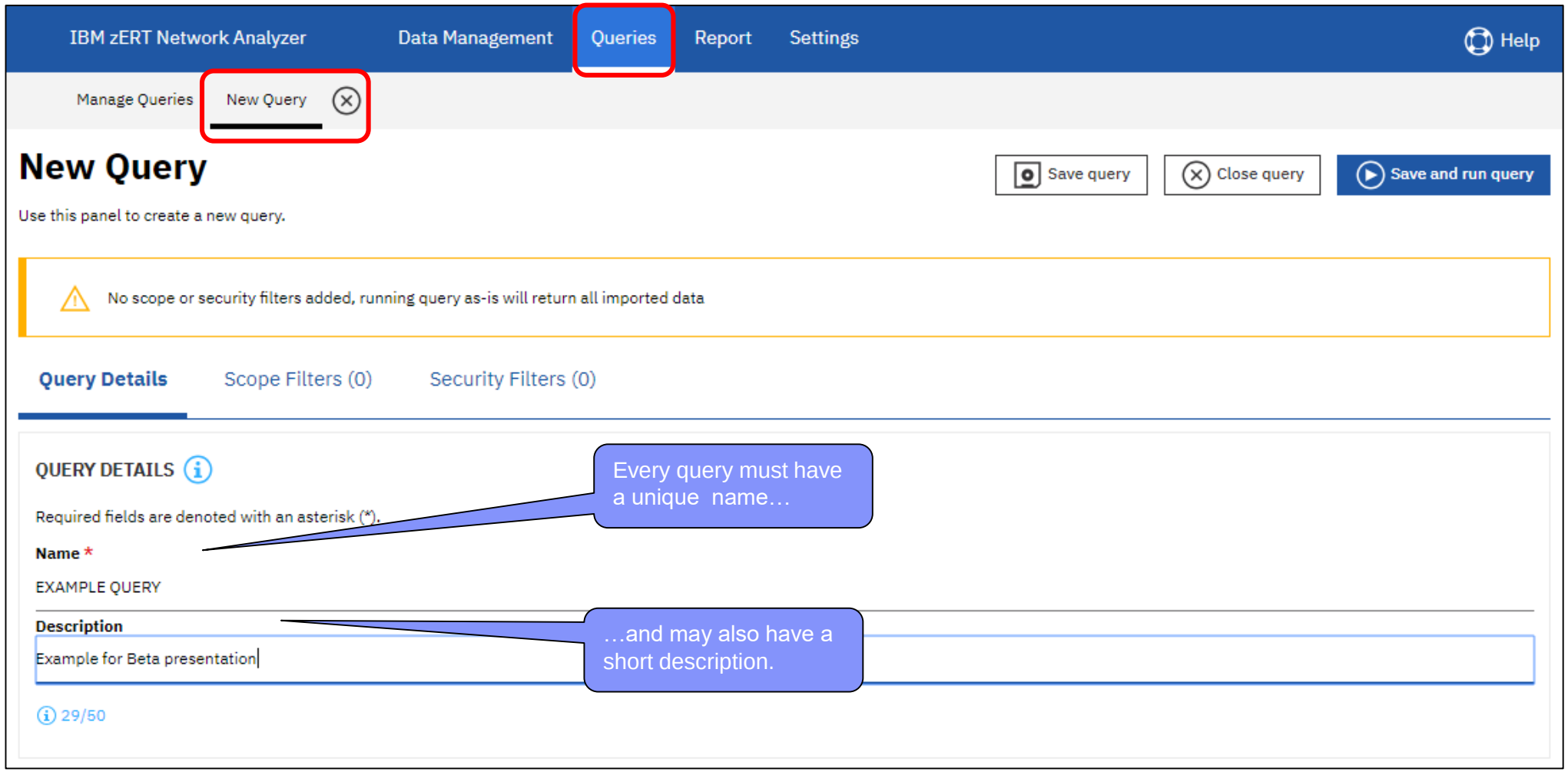


Usage & Invocation – Data management (3 of 3)

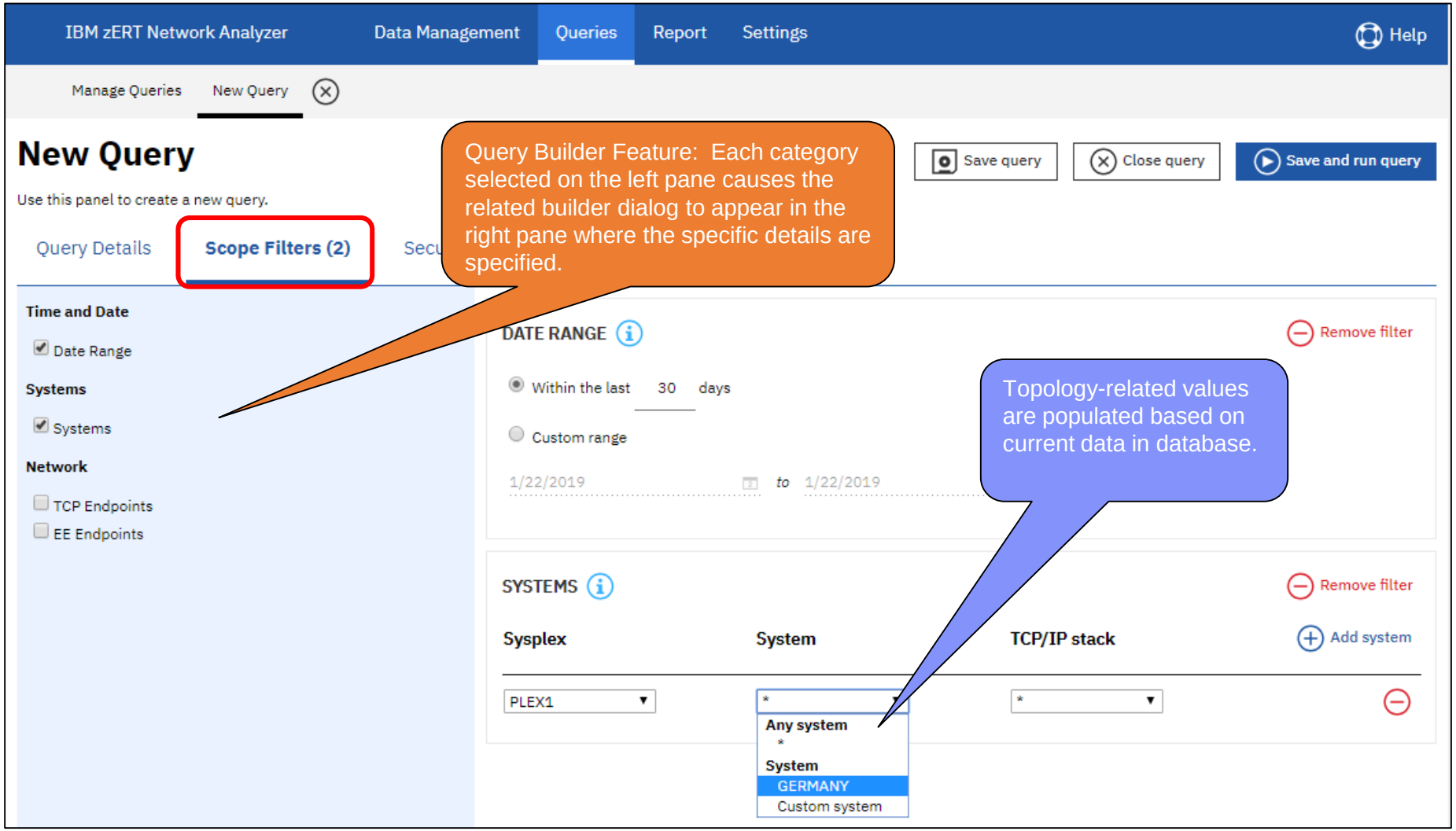


Usage & Invocation – Queries (1 of 4)

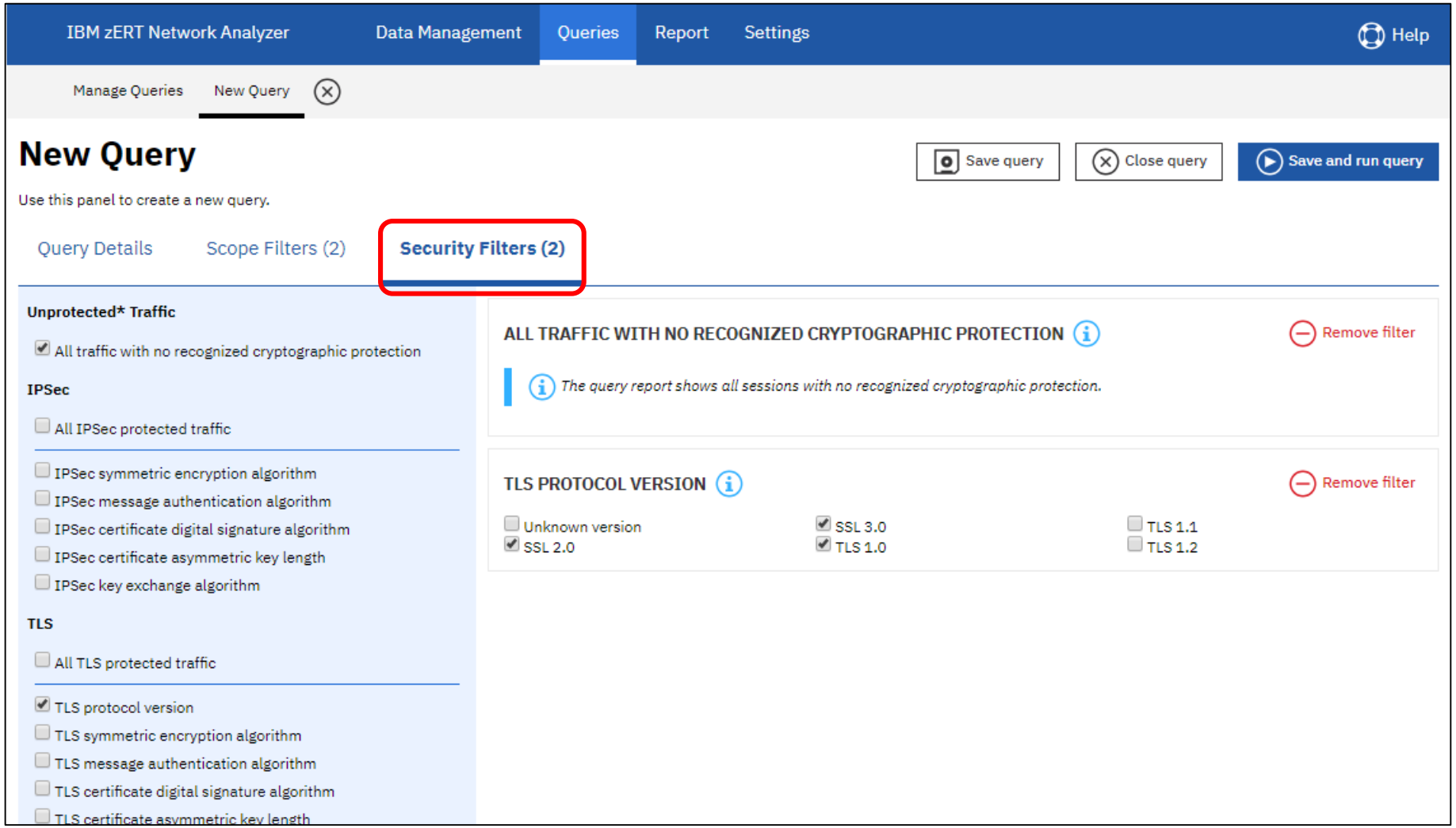
Usage & Invocation – Queries (2 of 4)



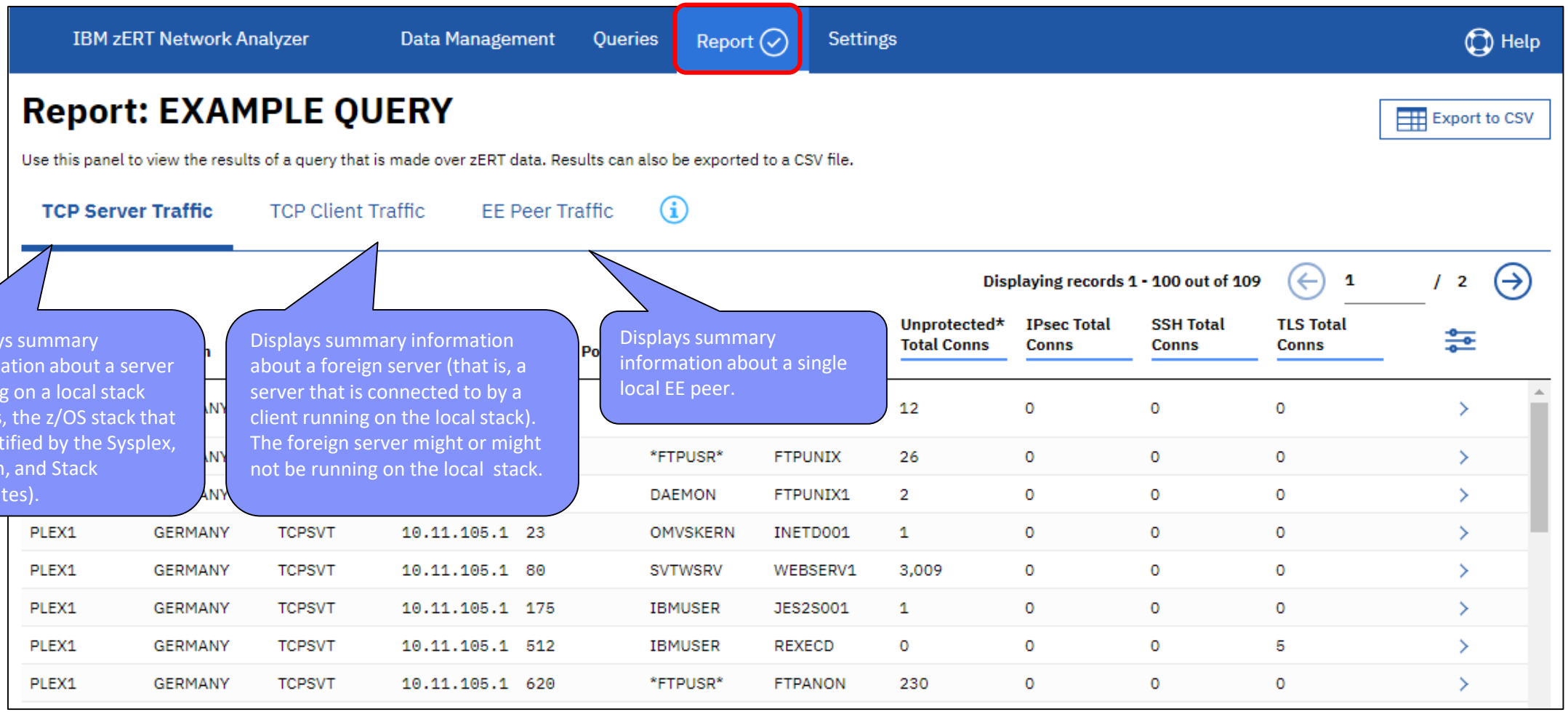
Usage & Invocation – Queries (3 of 4)



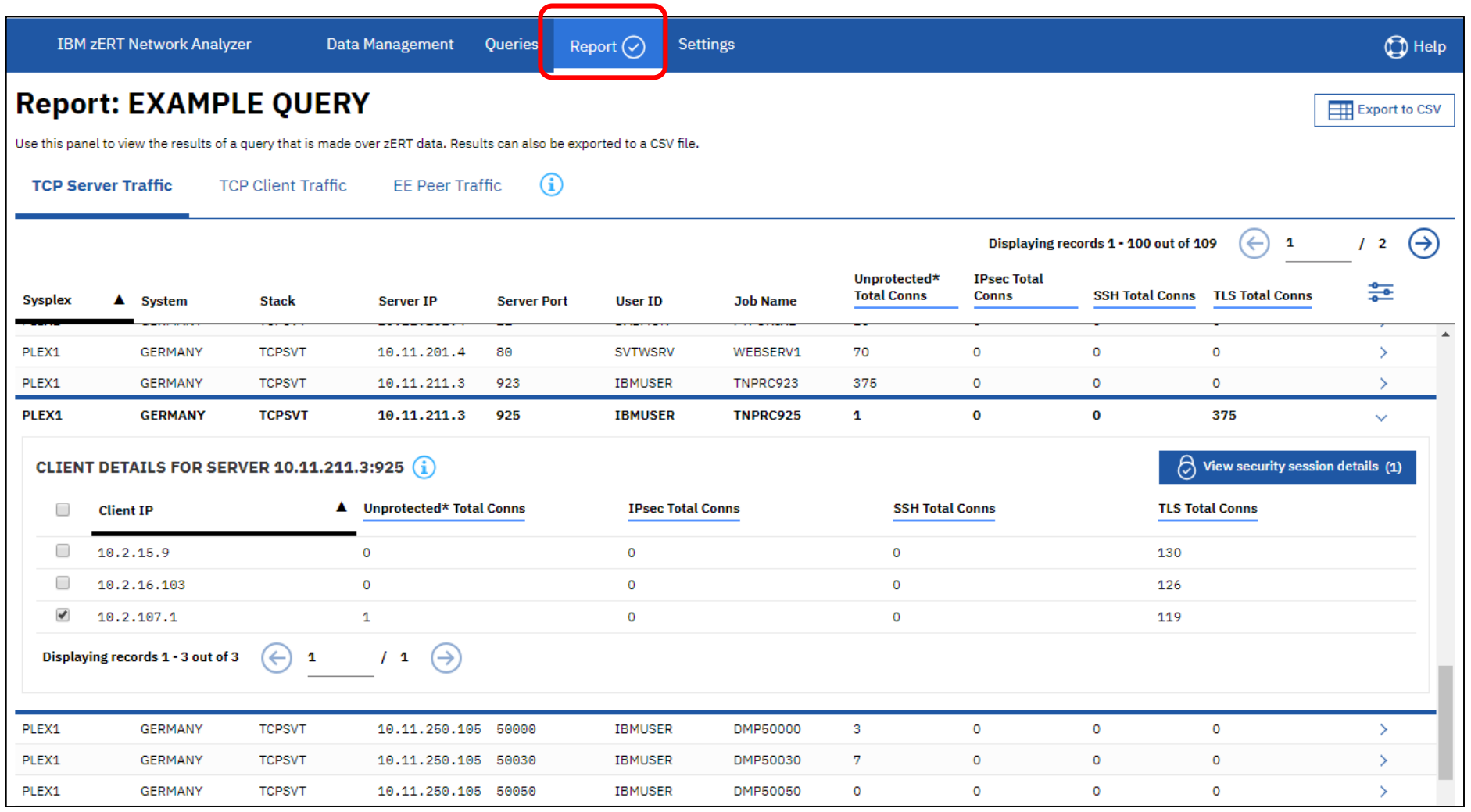
Usage & Invocation – Queries (4 of 4)



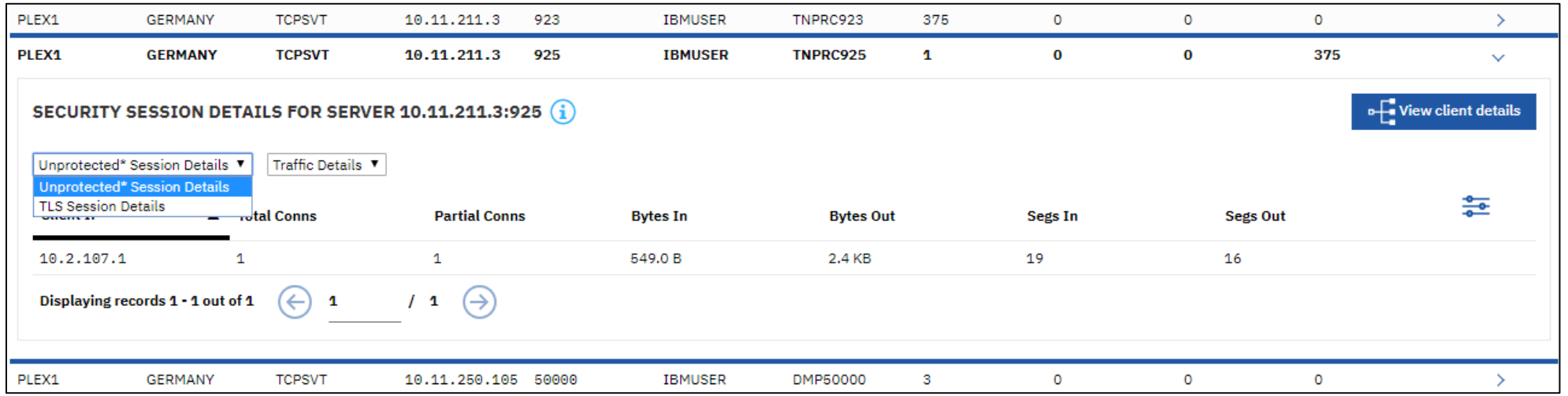
Usage & Invocation – Report (1 of 3)

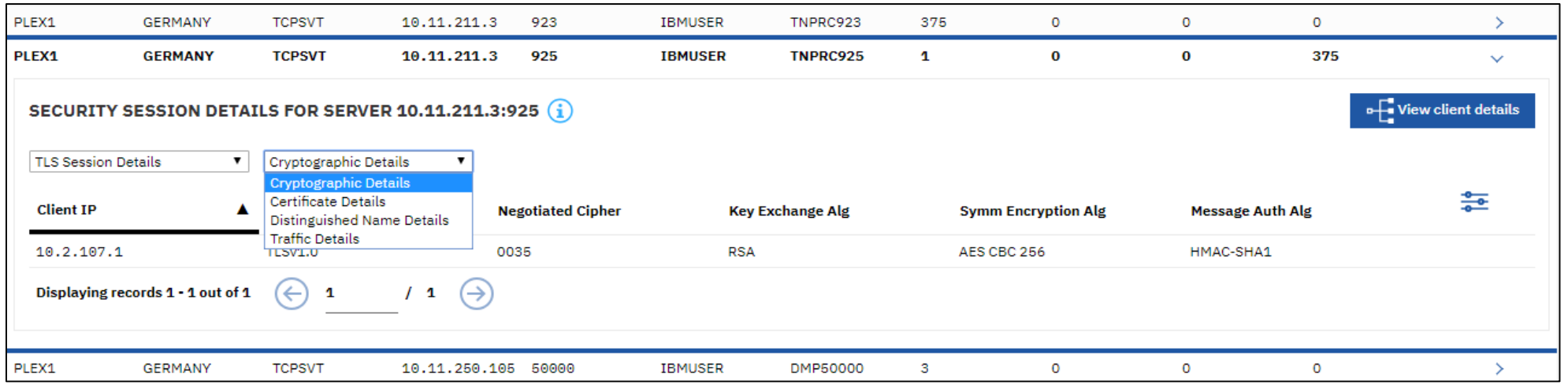


Usage & Invocation – Report (2 of 3)



Usage & Invocation – Report (3 of 3)





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

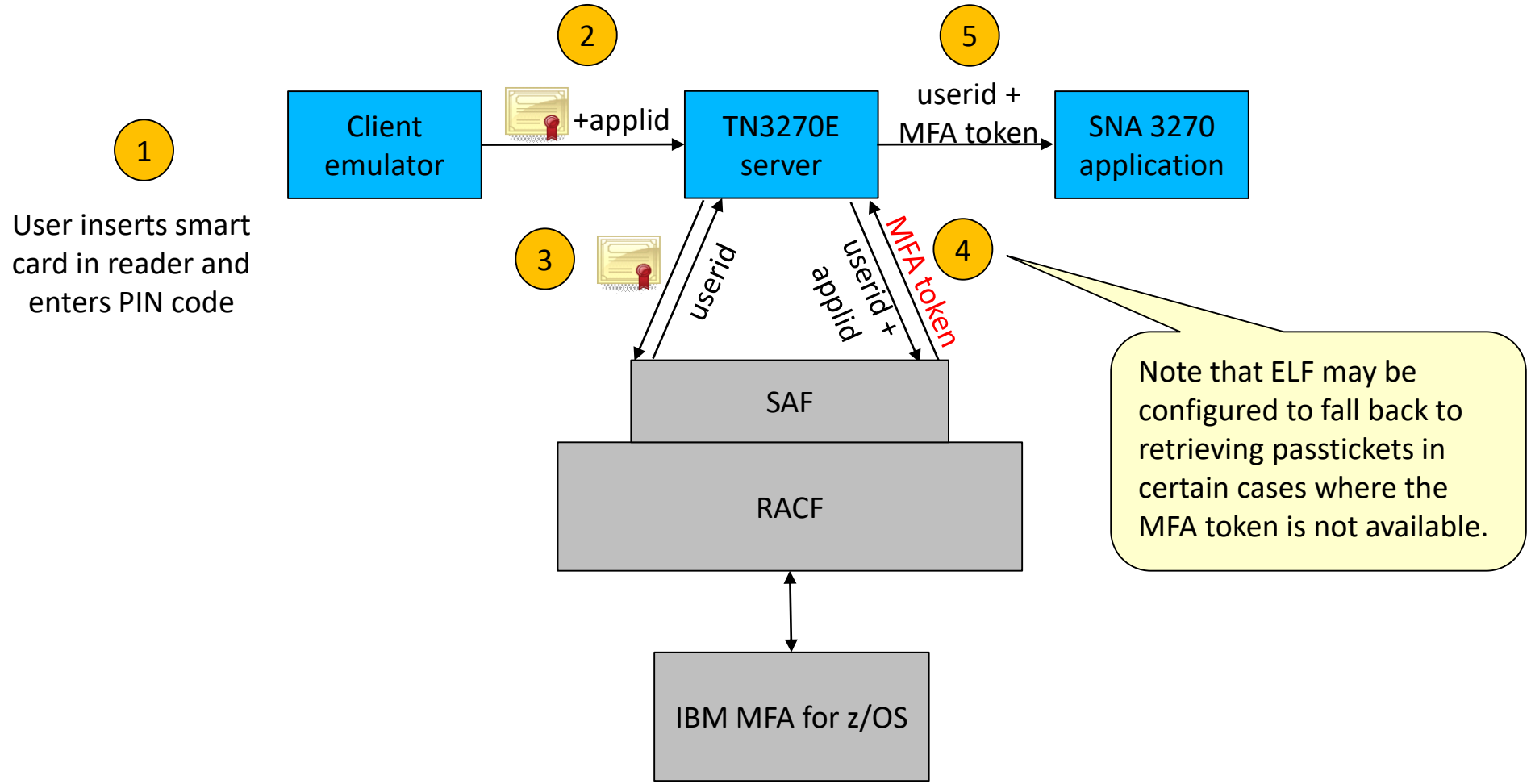
What (Solution)

- 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

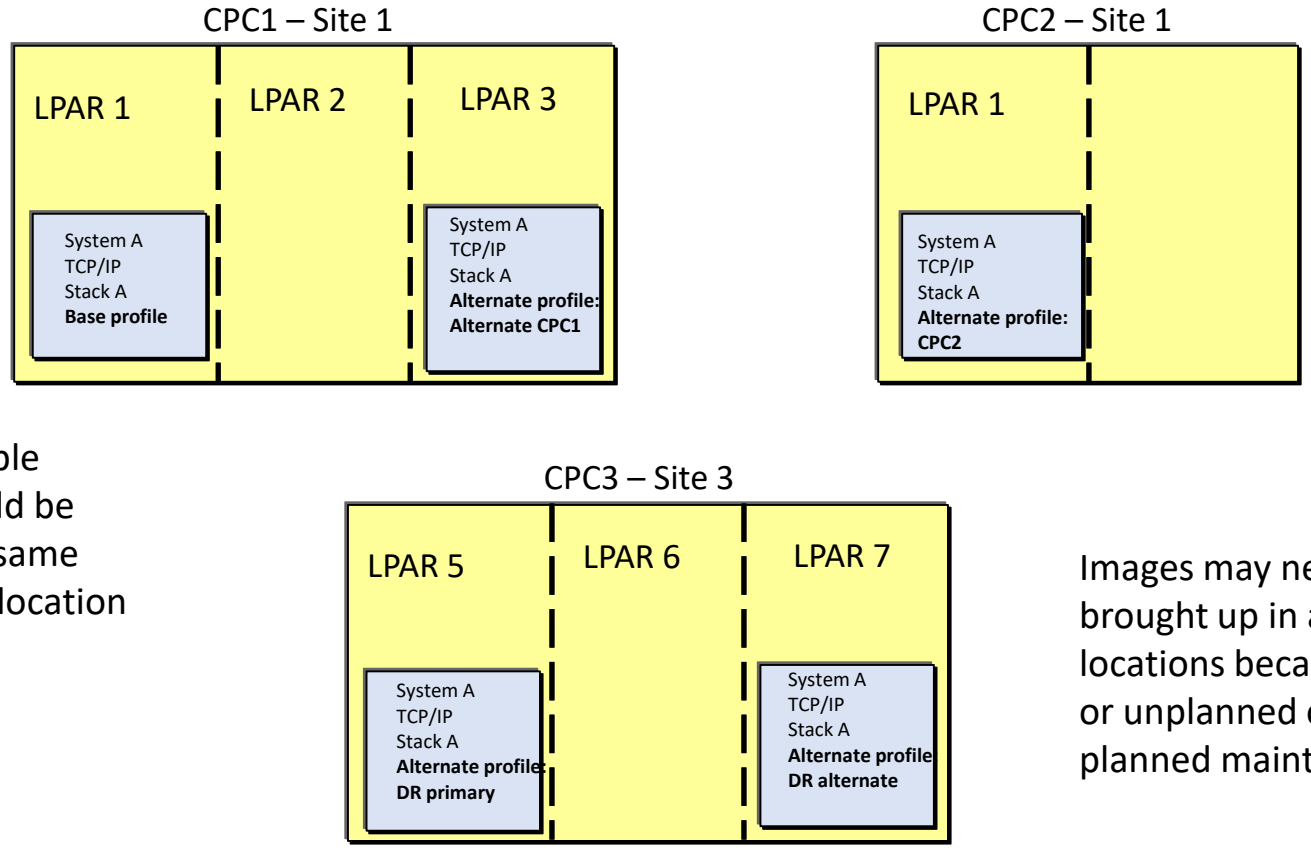
- Support also provided for z/OS V2R3 Communications Server (in 1Q 2018) with APAR PI85185, RACF APAR OA53002, and IBM MFA for z/OS APARs PI86470 and PI93341

Dependencies

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

Network Configuration Assistant support for multiple location TCP/IP configuration

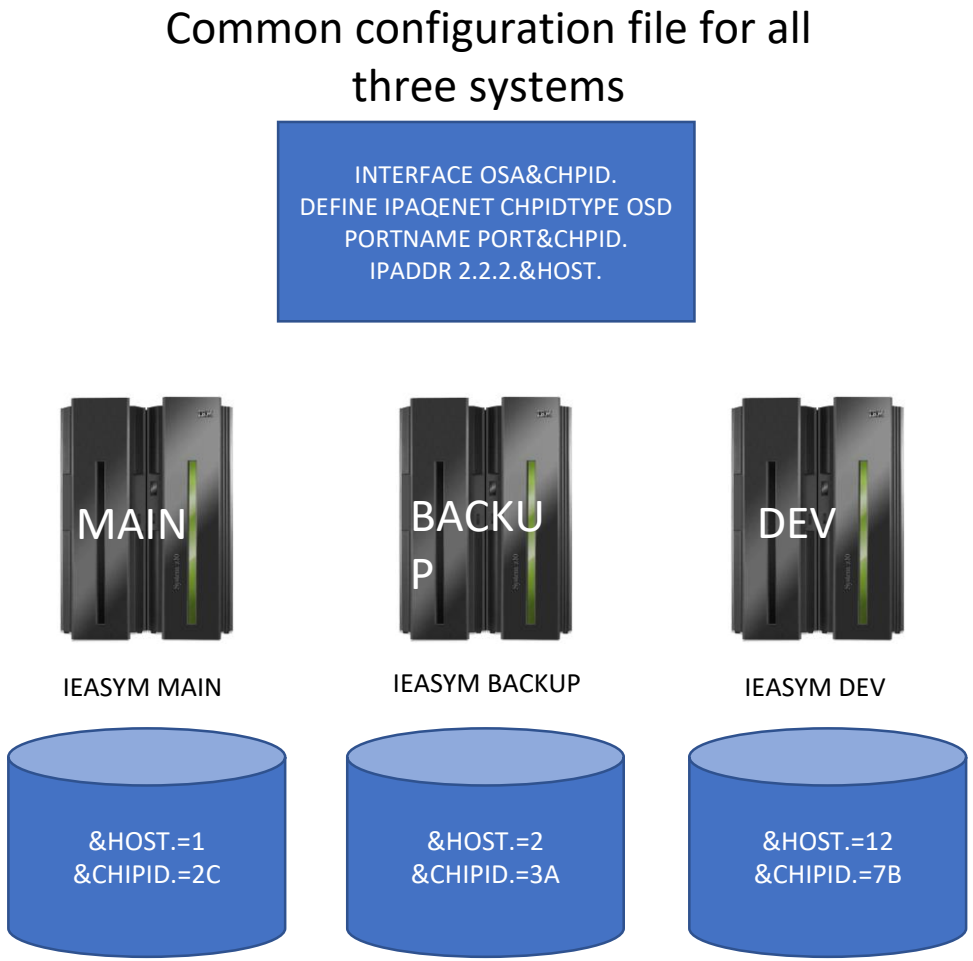
Background Information: Alternate configurations



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.)



- 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 speadsheets, etc.
  - This is tedious and error-prone

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

Overview

Who (Audience)

- z/OS network administrators

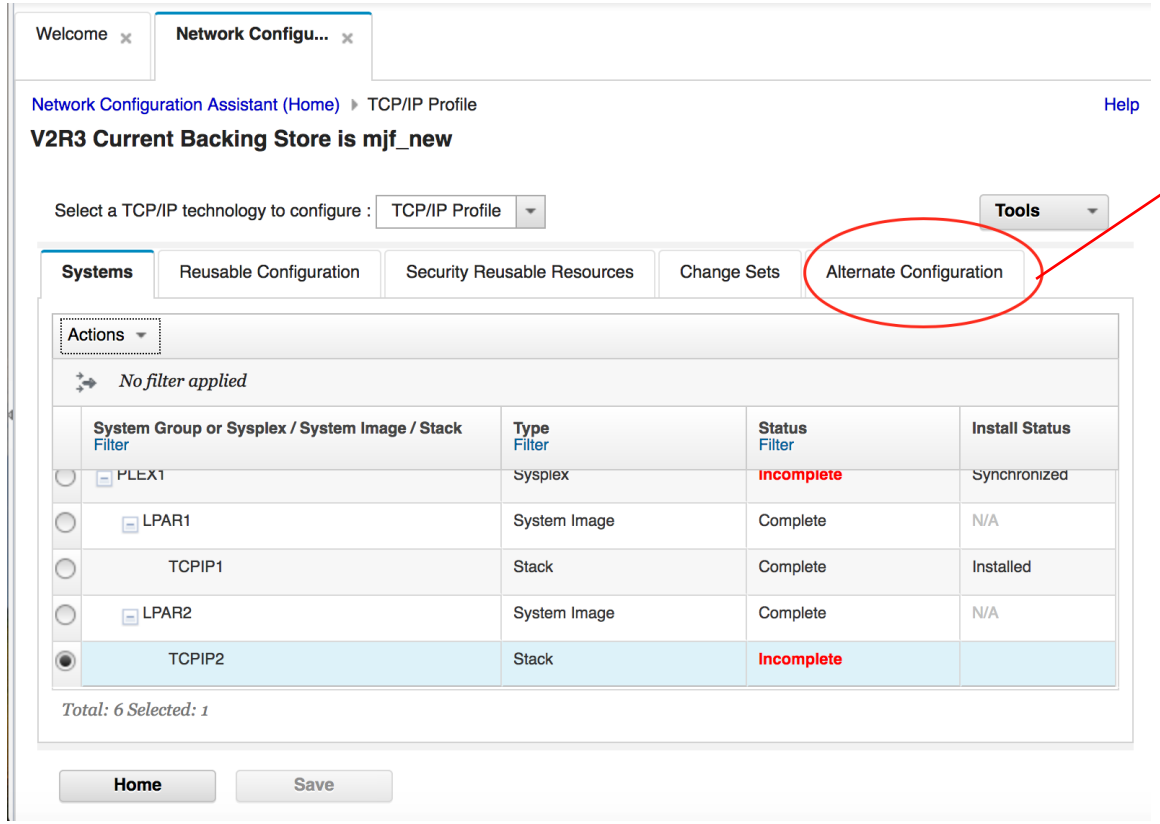
What (Solution)

- 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

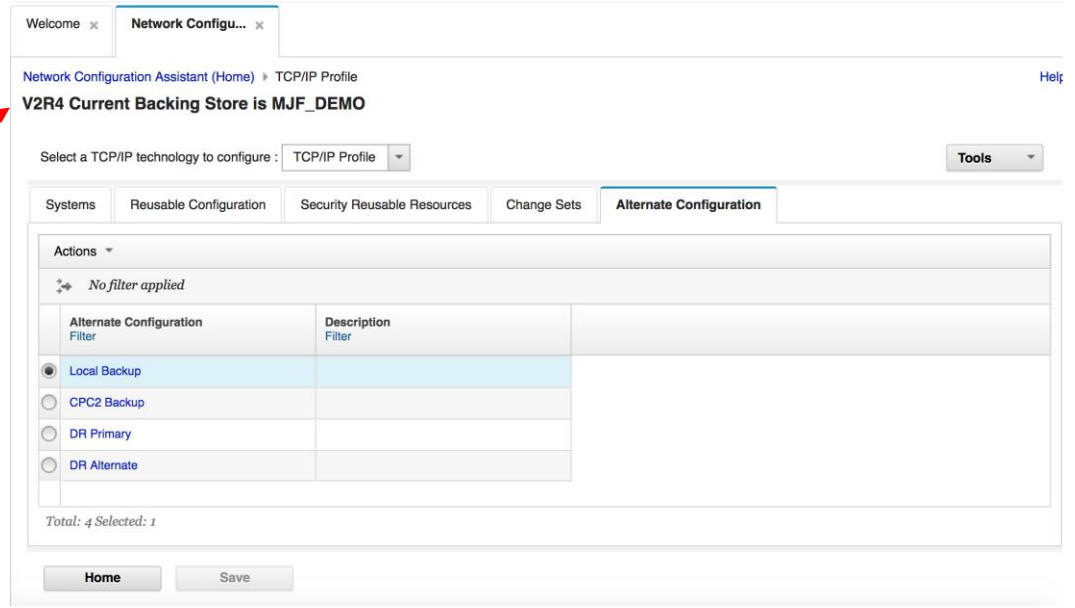
Wow (Benefit / Value, Need Addressed)

- 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!

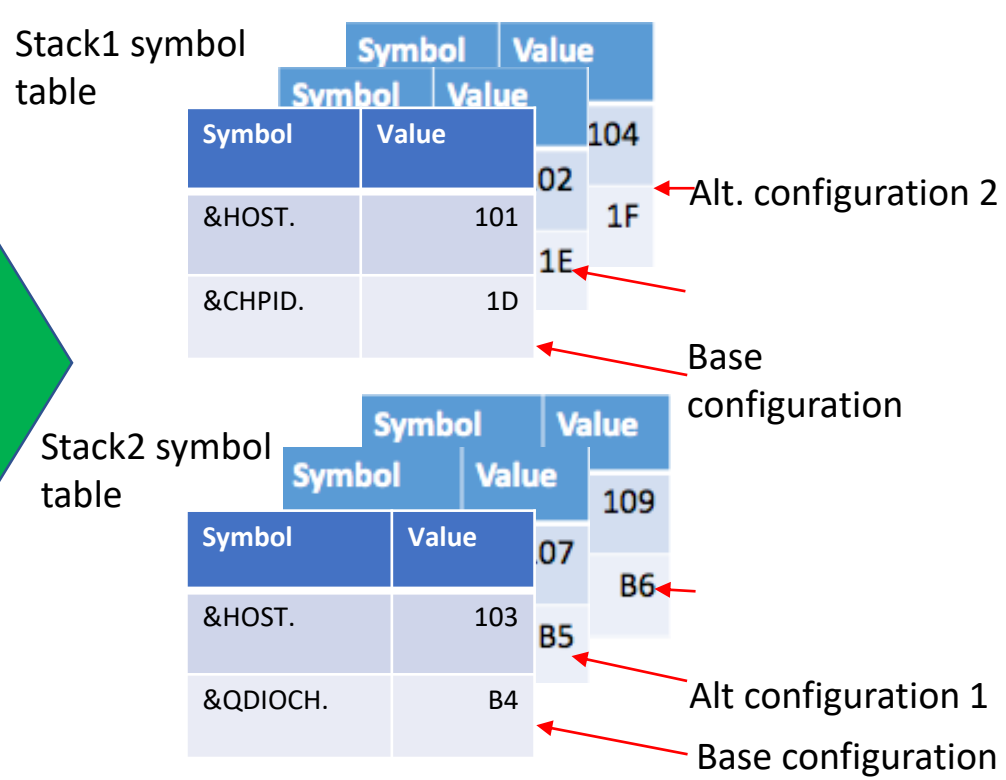
Stack1 symbol table

Symbol	Value
&HOST.	101
&CHPID.	1D

Stack2 symbol table

Symbol	Value
&HOST.	103
&QDIOCH.	B4

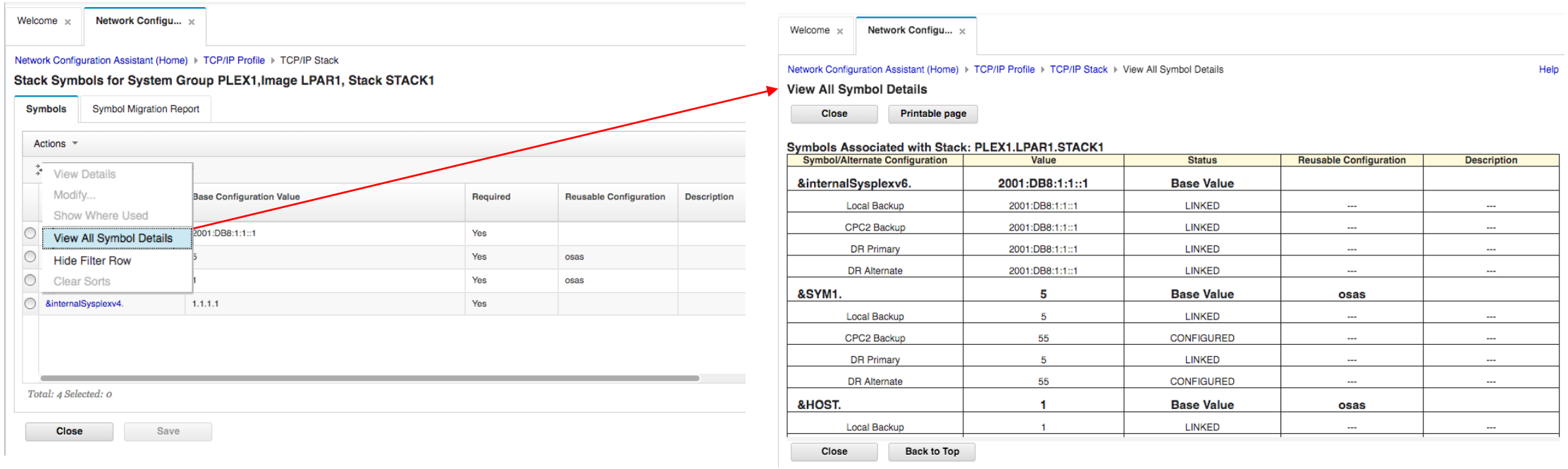
Add a new dimension to stack symbol tables for Alternate Configurations



- 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



- 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

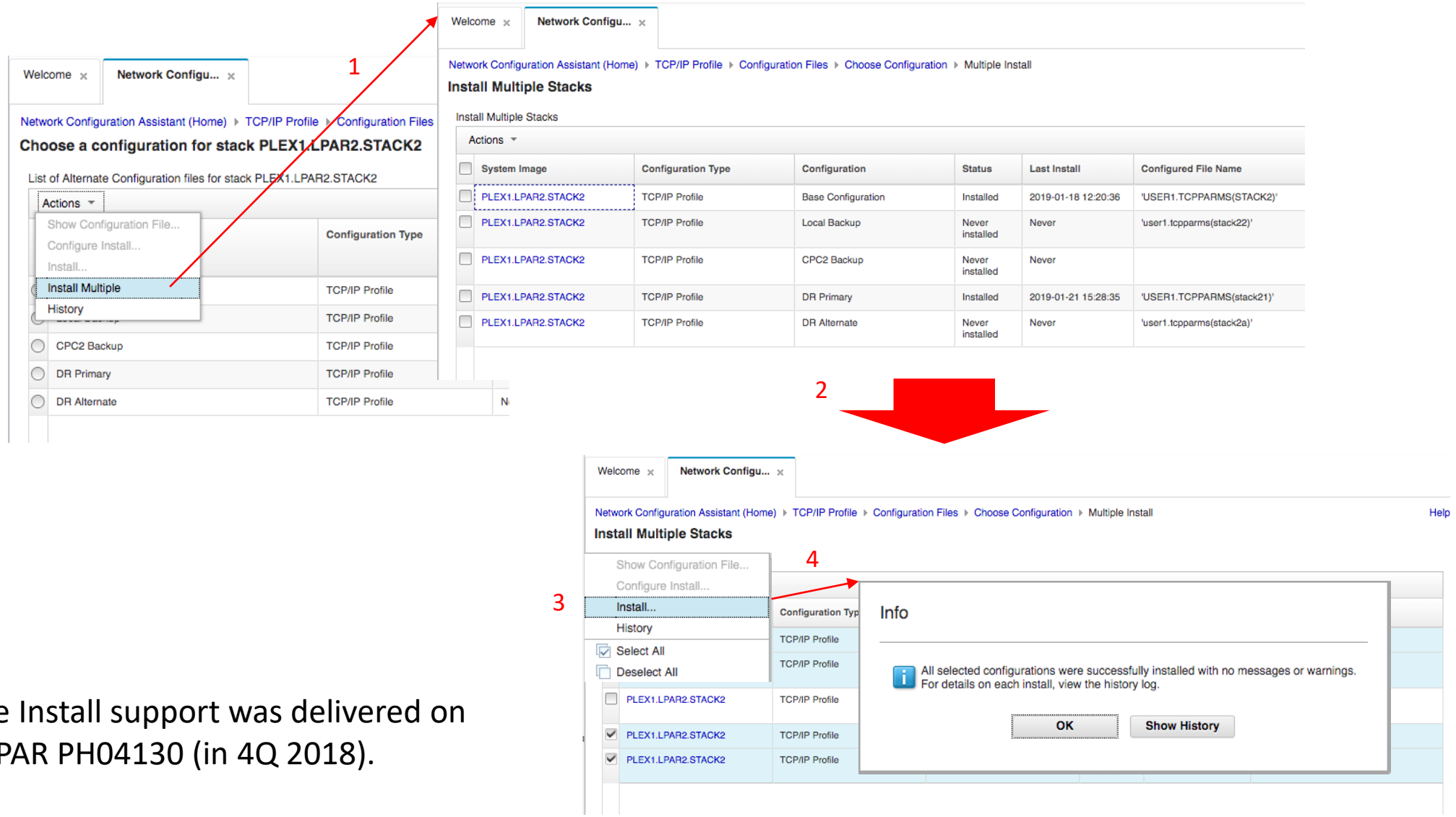
What (Solution)

- 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

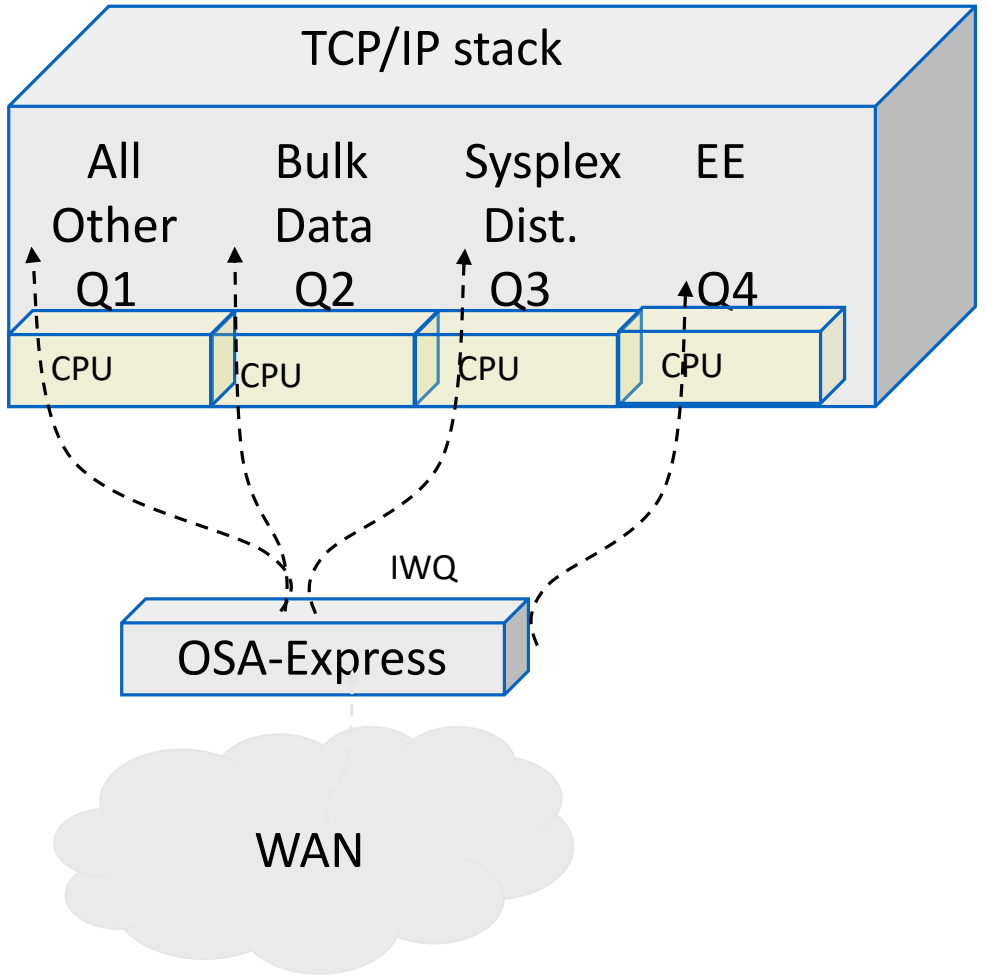


NCA Multiple Install support was delivered on V2R3 with APAR PH04130 (in 4Q 2018).

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)

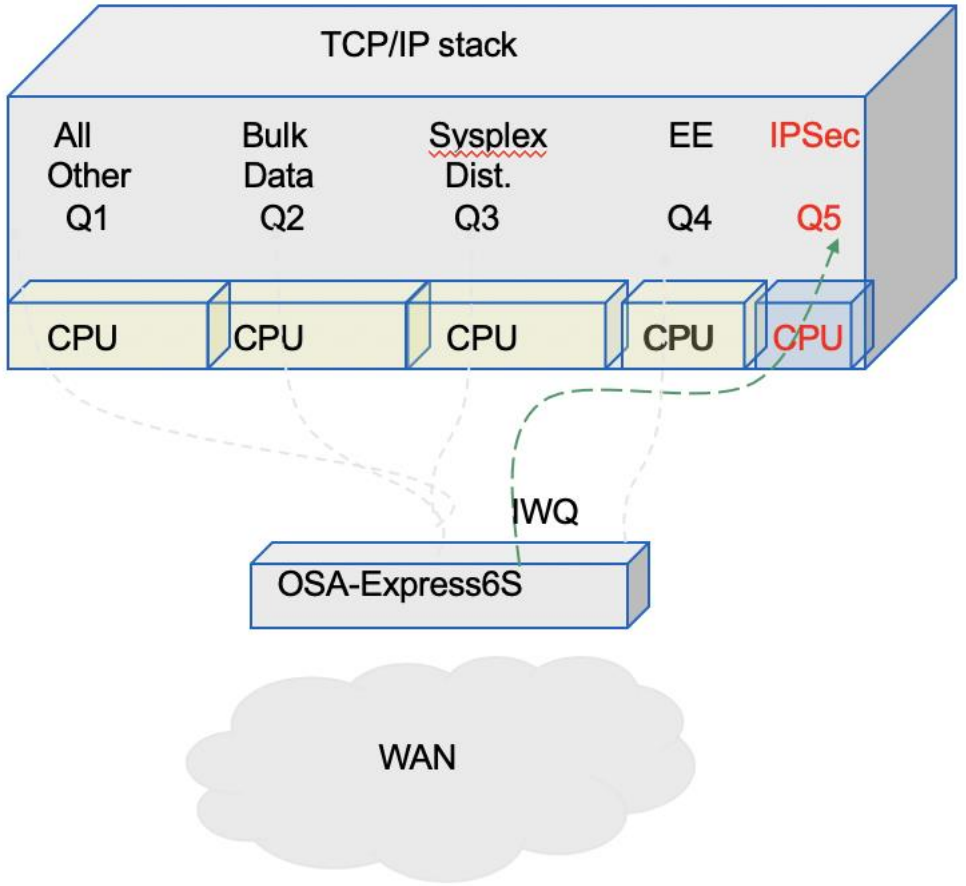
- z/OS network administrators

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

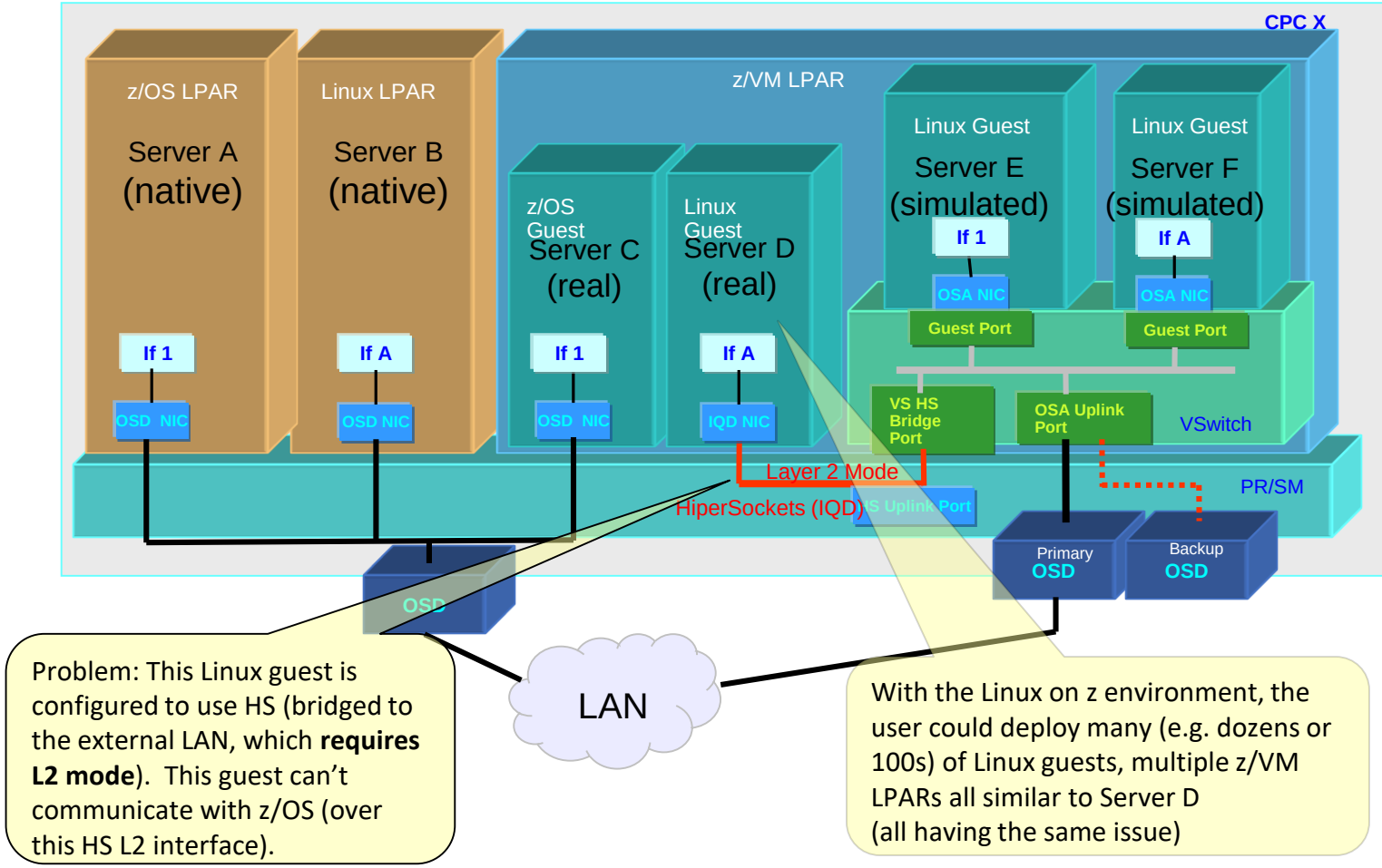
    See z/OS Migration book for details

  - 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)

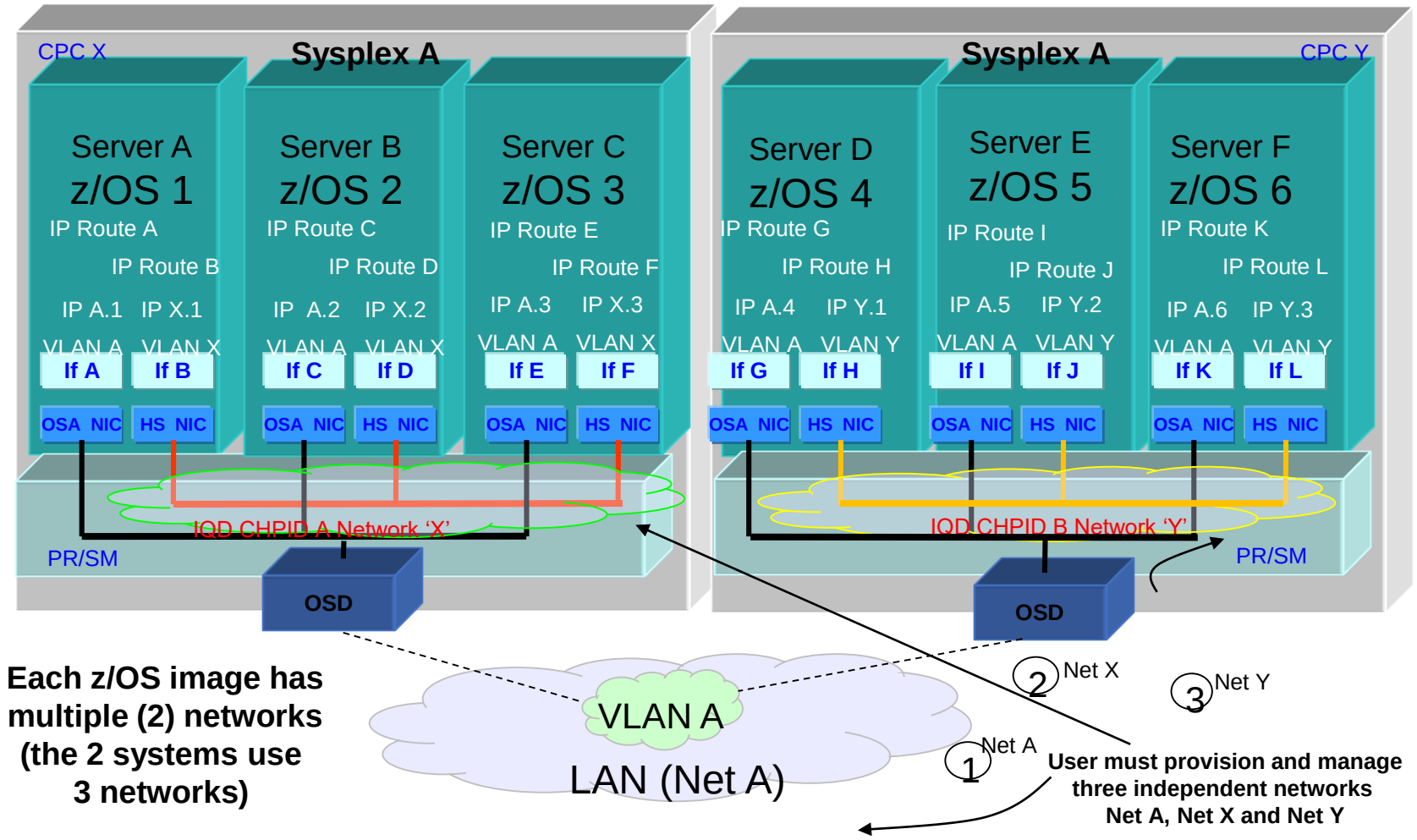
HiperSockets Converged Interface Support

Background Information: Incompatibility issue

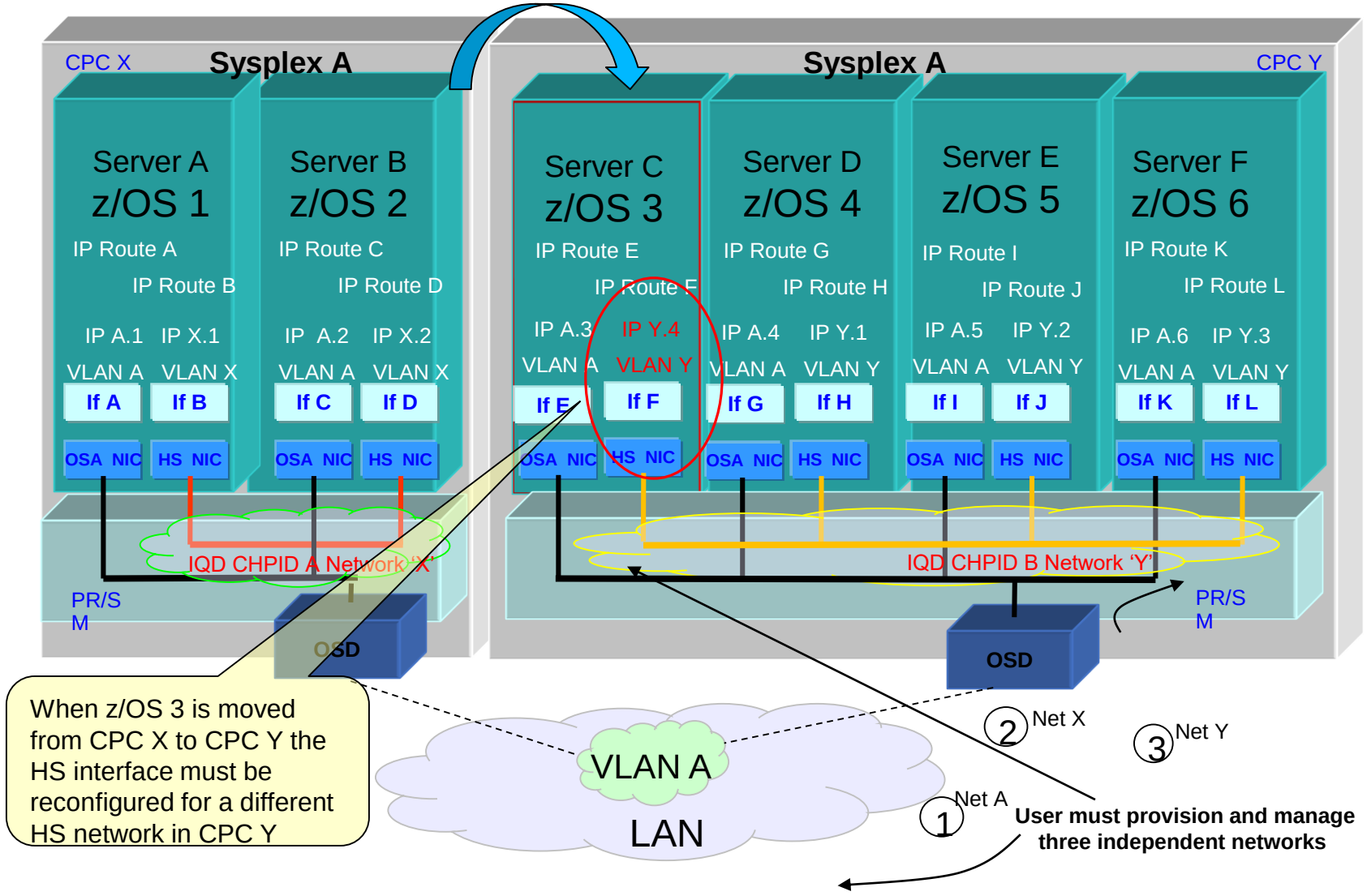
- OSA/HiperSockets (QDIO) architecture defines two "transport" modes of adapter connectivity:
  - Layer 3 mode (IP address routing) or
  - Layer 2 mode (MAC routing)
- LPARs using HiperSockets in Layer 2 mode **can not** communicate with LPARs in Layer 3 mode (note. OSA can bridge L2 to L3 hosts sharing 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)

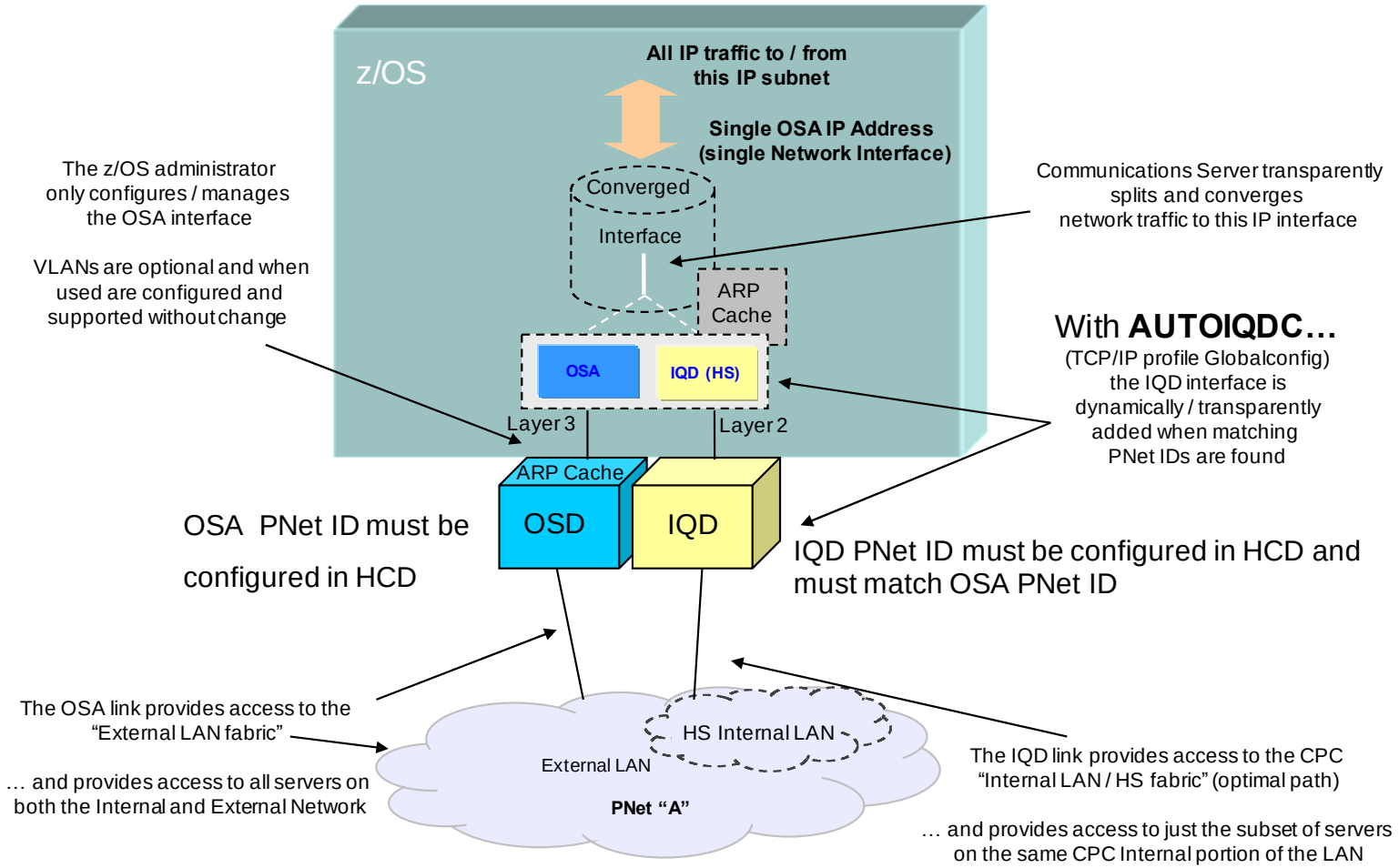
- HiperSockets converged interface support for z/VM bridge Layer 2 environment
- Allows configuration of HiperSockets on z/OS without defining additional network interfaces/networks

Wow (Benefit / Value, Need Addressed)

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

Usage & Invocation

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

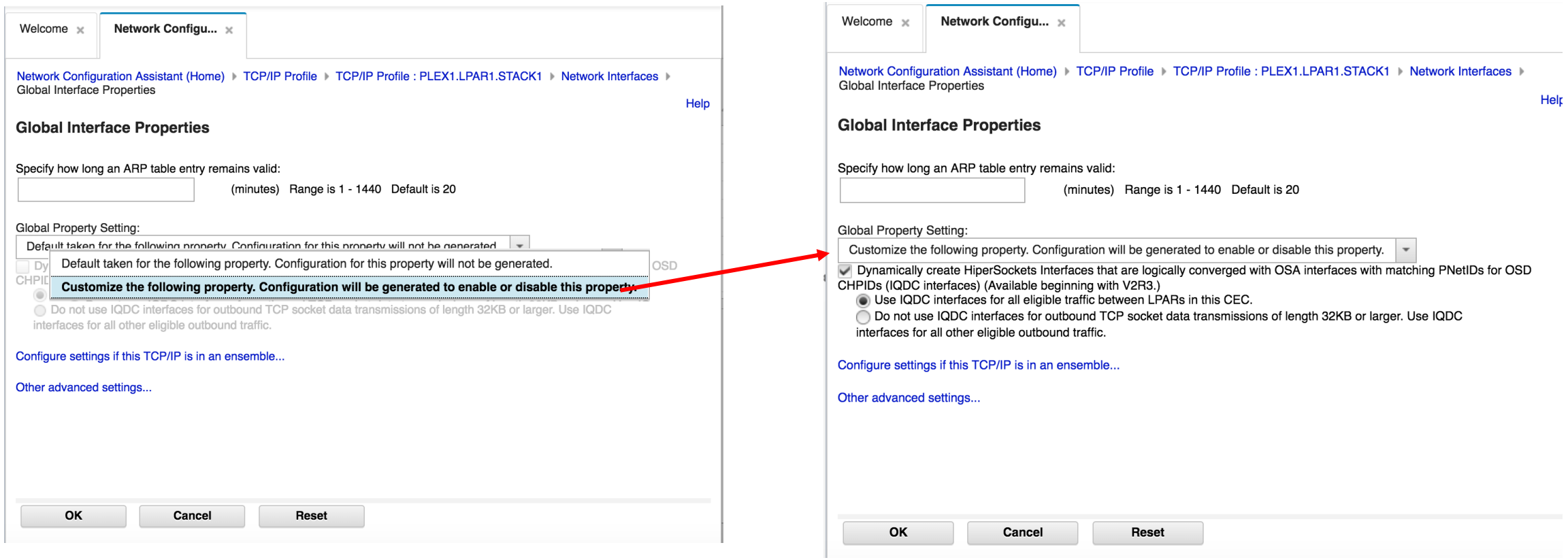
- New parameters on the GLOBALCONFIG statement: AUTOIQDC | NOAUTOIQDC
  - Sub-parameter on AUTOIQDC ALLTRAFFIC | NOLARGEDATA

    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

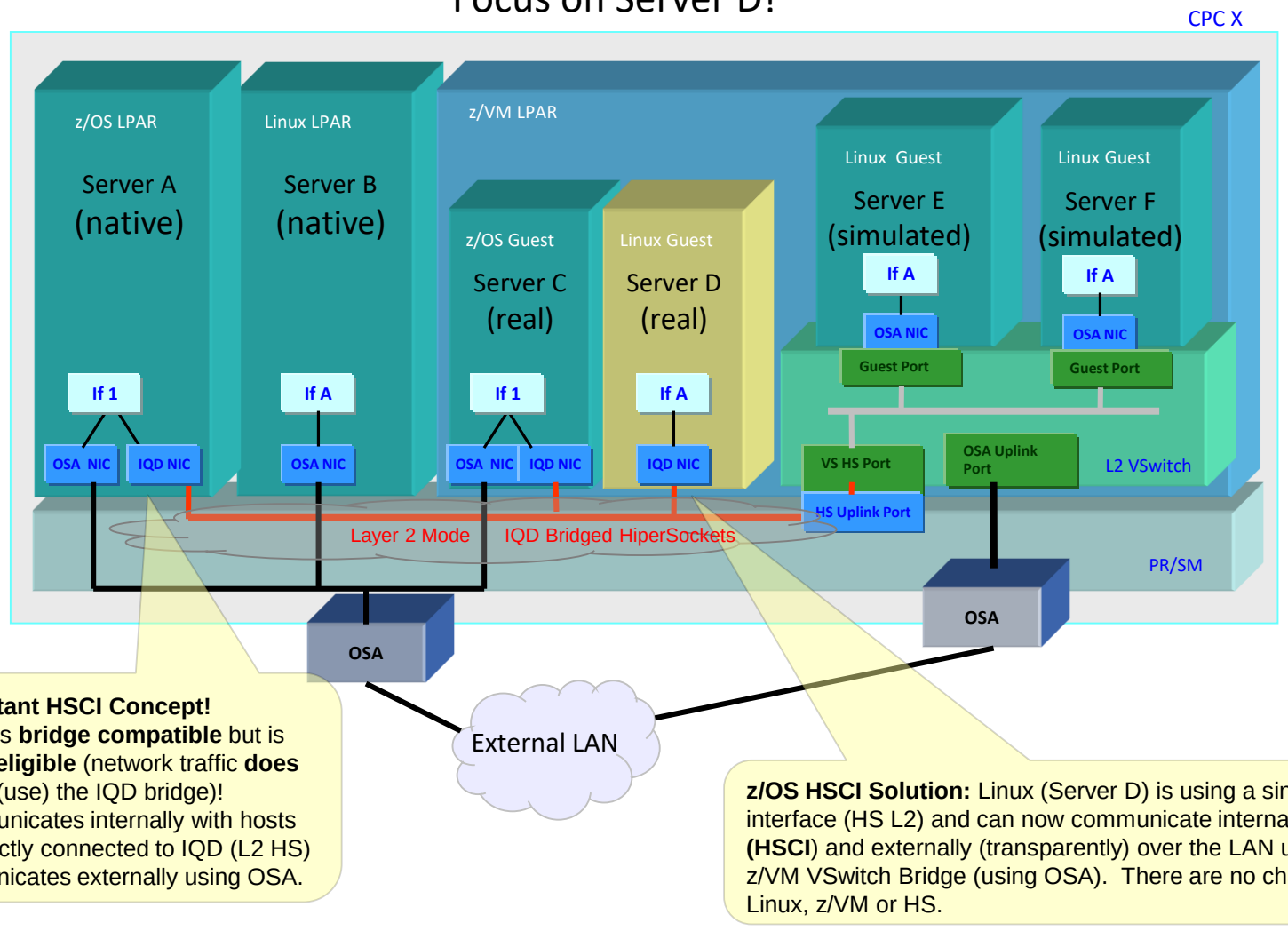
Usage & Invocation (contd.)

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



Usage & Invocation (contd.)

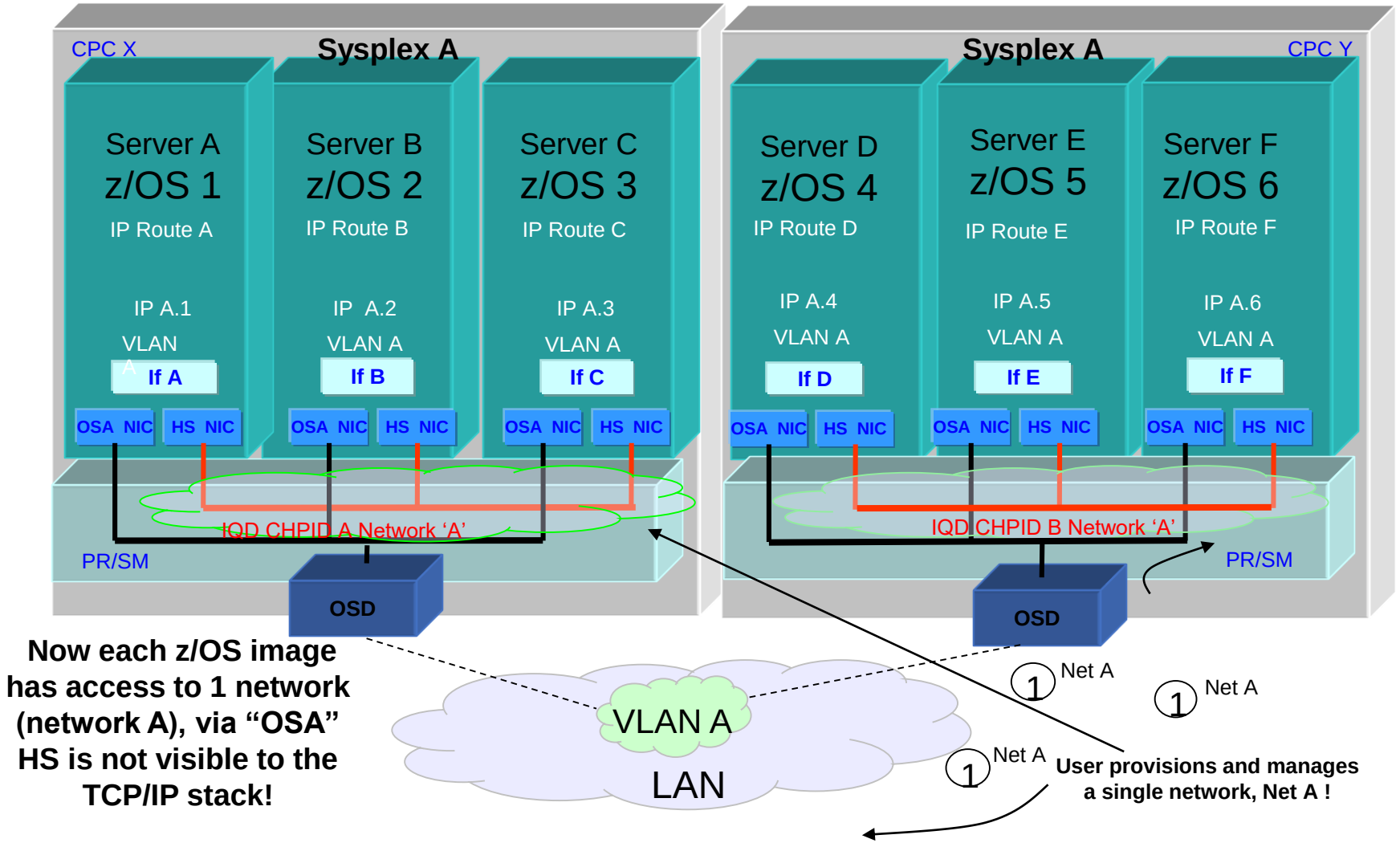
Focus on Server D!



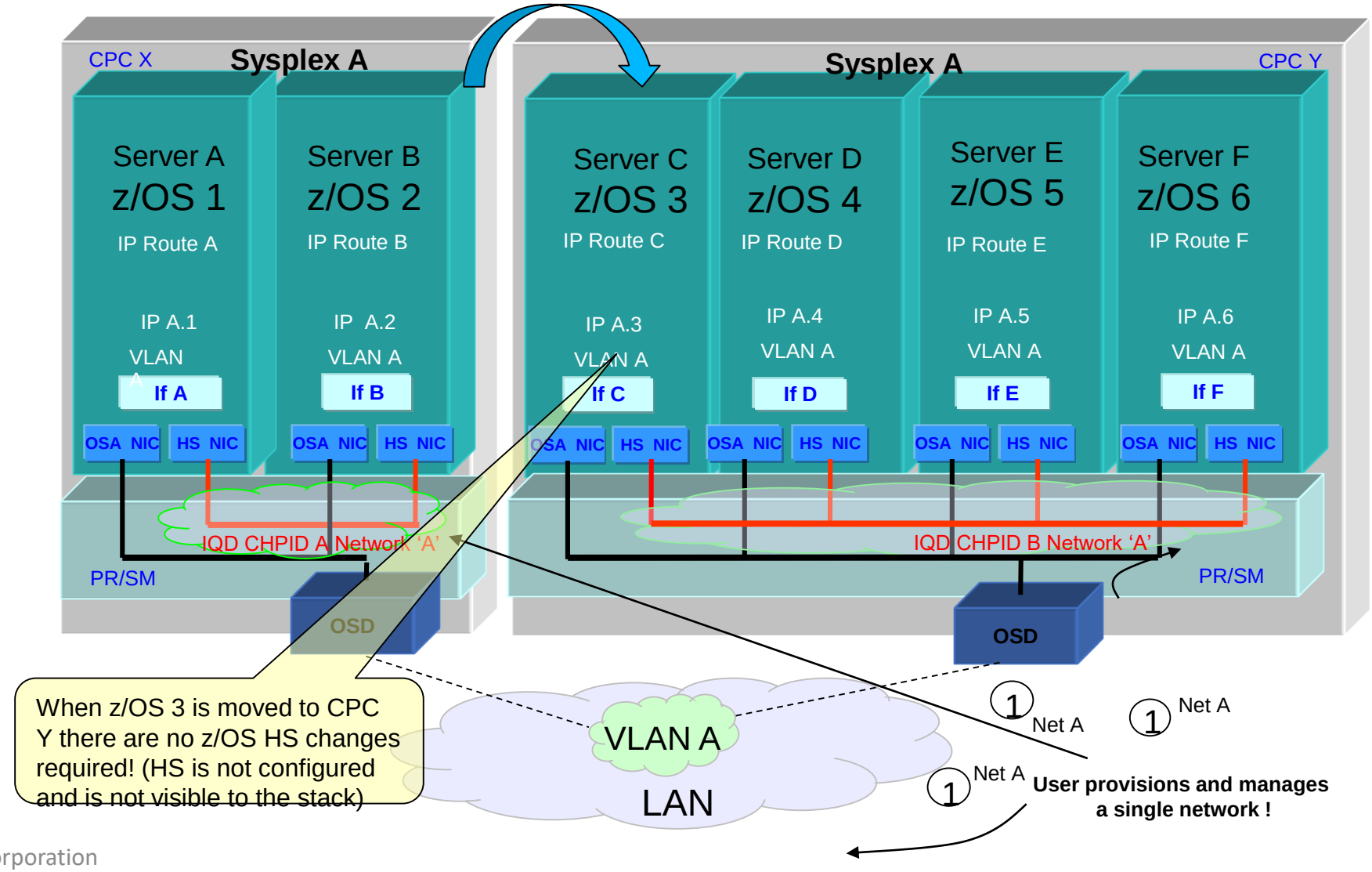
Very Important HSCI Concept!
z/OS HSCI is **bridge compatible** but is **not bridge eligible** (network traffic **does not** go thru (use) the IQD bridge)!
z/OS communicates internally with hosts that are directly connected to IQD (L2 HS) and communicates externally using OSA.

z/OS HSCI Solution: Linux (Server D) is using a single IP interface (HS L2) and can now communicate internally with **z/OS (HSCI**) and externally (transparently) over the LAN using the z/VM VSwitch Bridge (using OSA). There are no changes to Linux, z/VM or HS.

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.

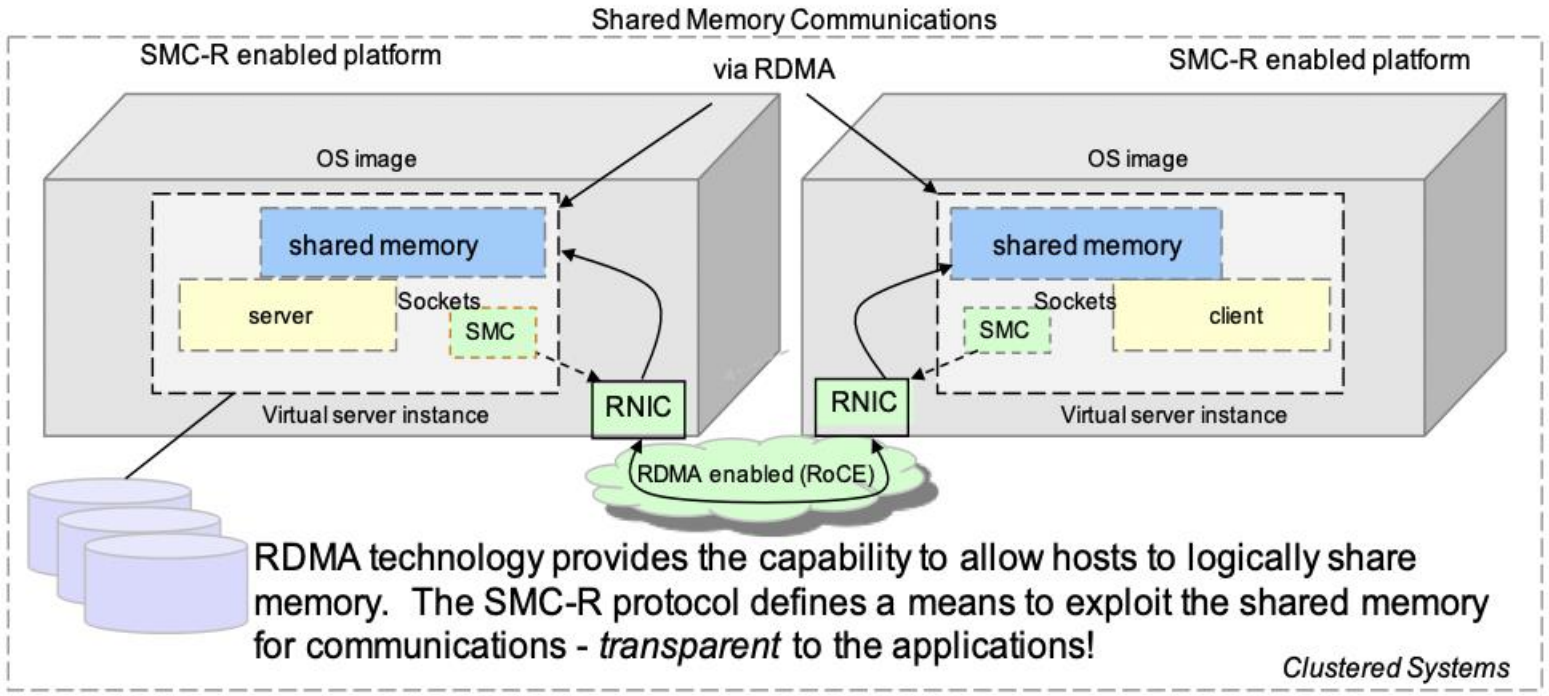
  - Hardware configuration
    - IQD CHPID:
      - Must have a PNetID[1] and External Bridge configured
      - The number of required IQD channel devices per TRLE: Two devices (read/write) are required for control + one additional device per TCP/IP stack, up to 8 stacks for a total of 10 devices per TRLE. A TRLE is created for each IP version (up to 2 TRLEs). TRLEs are created for each unique IQD CHPID (PNetID)[1].
      - IQD Max Frame Size **Recommendation**: Use (at least) 24k (16k MTU)
    - OSD CHPID(s) must have a PNetID[1] 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)

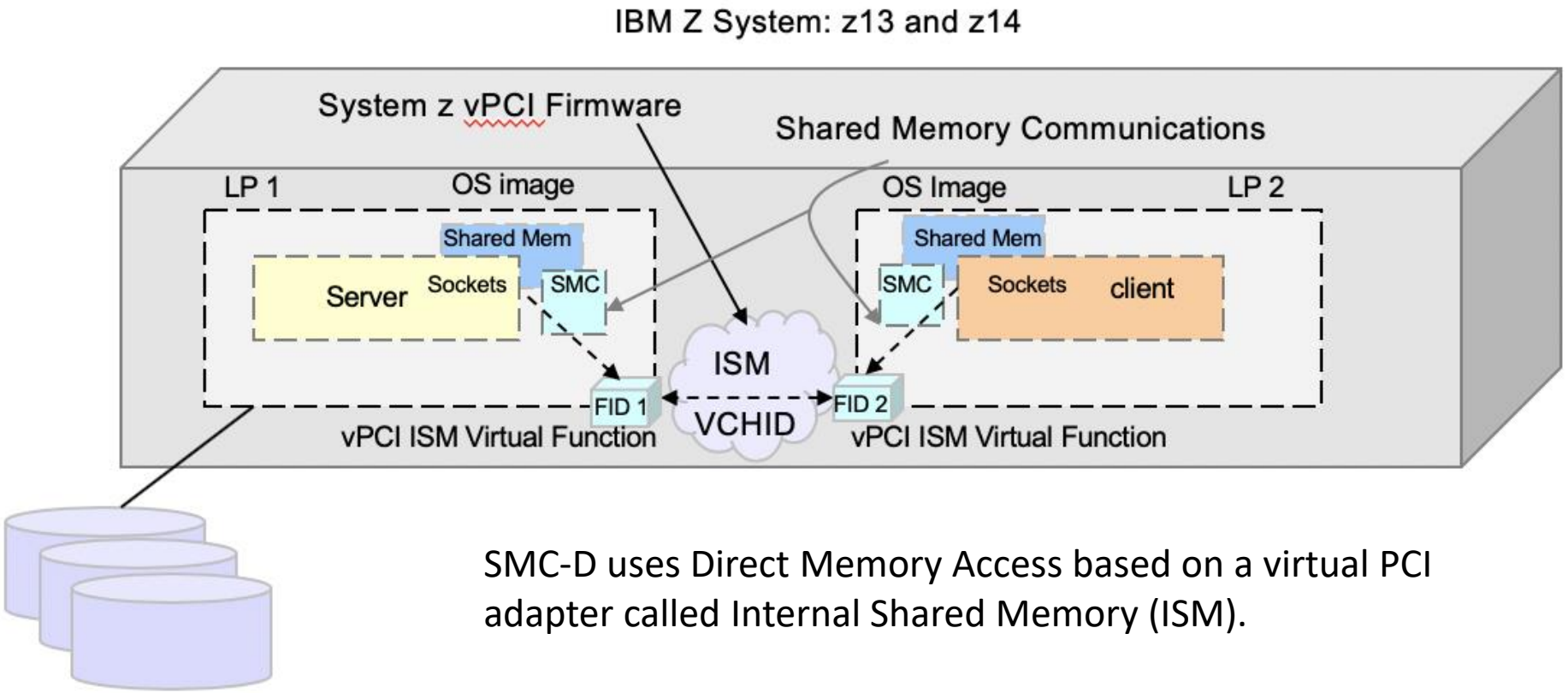


SMC-R is an *open* sockets over RDMA protocol that provides transparent exploitation of RDMA (for TCP based applications) while preserving key functions and qualities of service from the TCP/IP ecosystem that enterprise level servers/network depend on!

IETF RFC for SMC-R:

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

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



SMC-D uses Direct Memory Access based on a virtual PCI adapter called Internal Shared Memory (ISM).

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: MAXNEGTTL *time-to-live*
  Example: MAXNEGTTL 200
  Default value: Same as MAXTTL (configured or defaulted)

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