

z/OS 2.4 Communications Server Technical Update

Jerry Stevens (sjerry@us.ibm.com)

IBM

November 2019

Session EB



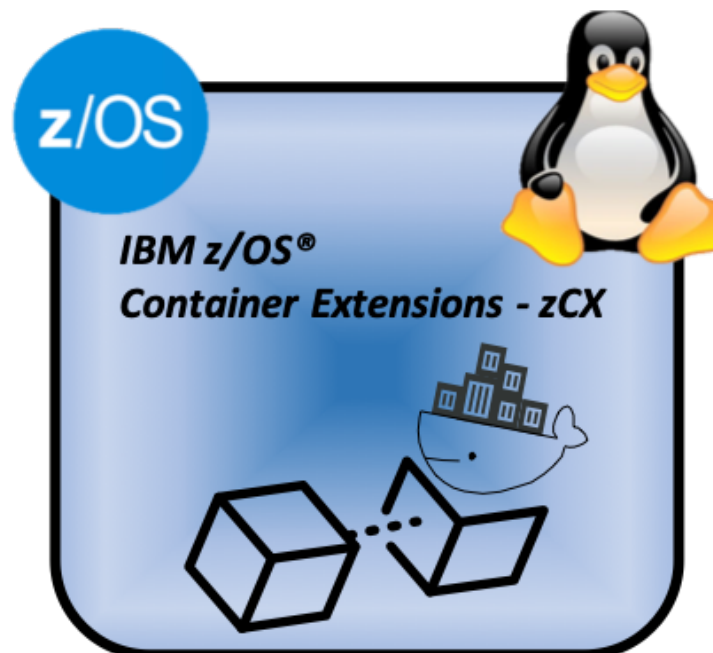
Agenda

- Networking Support for z/OS Container Extensions
- z/OS Encryption Readiness Technology (zERT)
- AT-TLS Support for TLSv1.3
- HiperSockets Converged Interface (HSCI) Support
- IWQ Support for IPSec
- Sysplex Notification of TCP/IP Stack Join or Leave
- Sysplex Autonomics for IPSec
- Network Configuration Assistant Updates
- New Function APAR Summary Web Pages
- Statements of Direction
- Miscellaneous
- Appendix

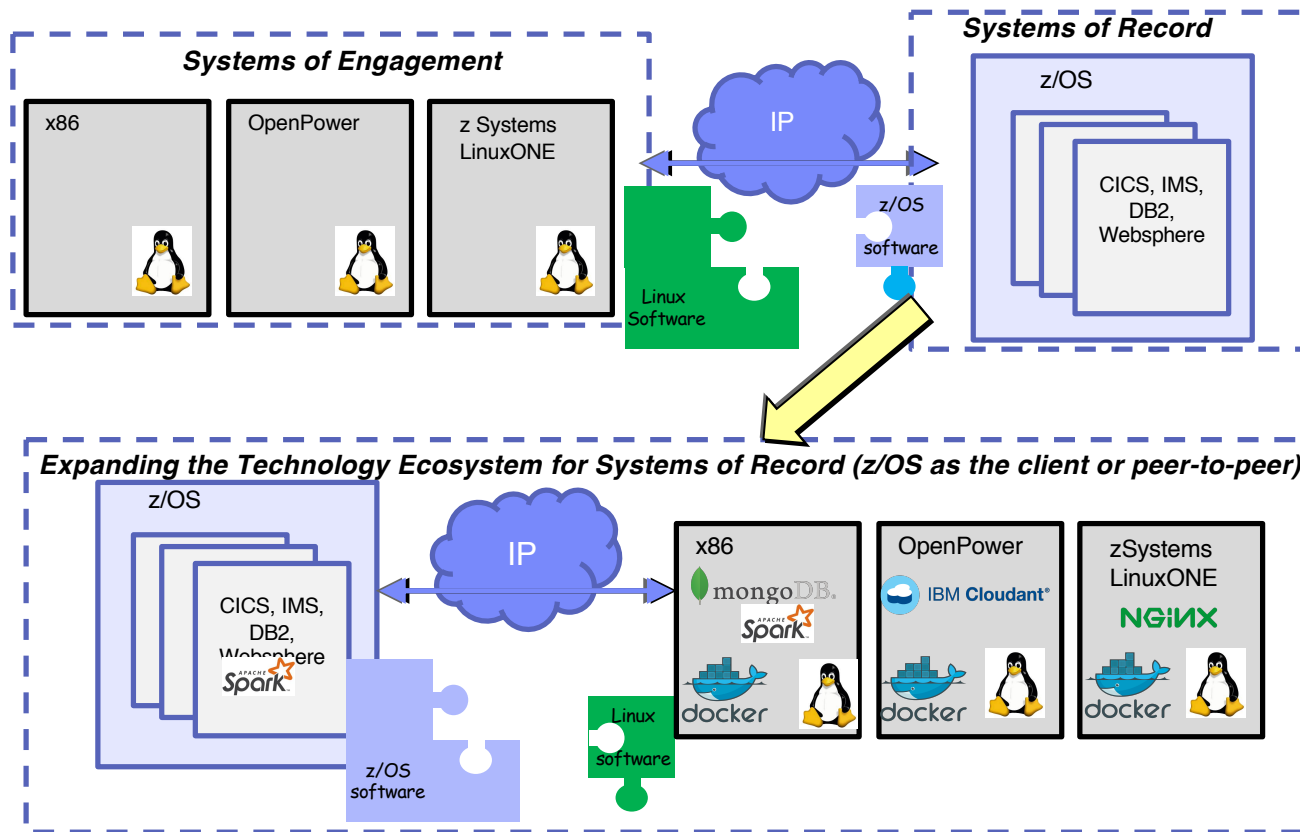
Networking Support for z/OS Container Extensions

Introduction to z/OS Container Extensions

- *What is z/OS Container Extensions (zCX)?*
- *What does it enable you to do?*
- *Overview of Networking support for zCX*



Today's z/OS and Linux composite solutions



Traditional SoE tier interacting with SoR tier

- Proven, understood model of deployment
- Loosely coupled management model
- Not the focus of this technology

Expanding the Technology Ecosystem for traditional Systems of Record

- When the needed technologies are not available natively on z/OS you could deploy them on a virtual Linux based server
- z/OS becomes dependent (acting as a client or consumer) of software deployed on Linux
- This introduces a set of complex management issues – how do ensure that the SoR SLAs and QoS are not compromised?
- The focus of the z/OS Container Extensions on is to significantly simplify these management issues

What Is IBM z/OS Container Extensions (zCX)?

A new function in z/OS 2.4 that enables clients to:

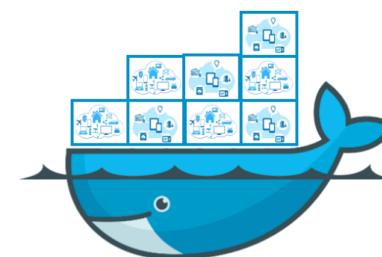
- ✓ Deploy Linux on Z software components as Docker Containers in a z/OS system, in direct support of z/OS workloads
- ✓ Without requiring a separately provisioned Linux server
- ✓ While maintaining overall solution operational control within z/OS and with z/OS Qualities of Service
- ✓ Requires IBM z14 based server with Container Hosting Foundation (feature code 0104)

Design Thinking Hill Statement:

A **solution architect** can **create a solution to be deployed on z/OS based on components available as Docker containers** in the Linux on Z ecosystem transparently exploiting z/OS QoS, **without requiring z/OS development skills**.

What is Docker?

- A Packaging standard for software
 - Think of it like a shipping container
 - Makes moving, stacking, unstacking of compliant software easier
 - Common in the application world on Linux and cloud
- Dockerhub
 - Contains many popular docker packages
 - s390x packages support Linux on z
 - <https://hub.docker.com/search?q=&type=image&architecture=s390x>
- By focusing on Docker
 - We reduce the complexity of installation and configuration for the user
 - We reduce the service footprint on Linux to what Docker supports
 - We gain access to a large number of packages out of the box



zCX – A turn-key Virtual Docker Server Software Appliance

Pre-packaged Linux Docker appliance

- Provided and maintained by IBM
- Provisioned using z/OSMF workflows

Provides standard Docker interfaces

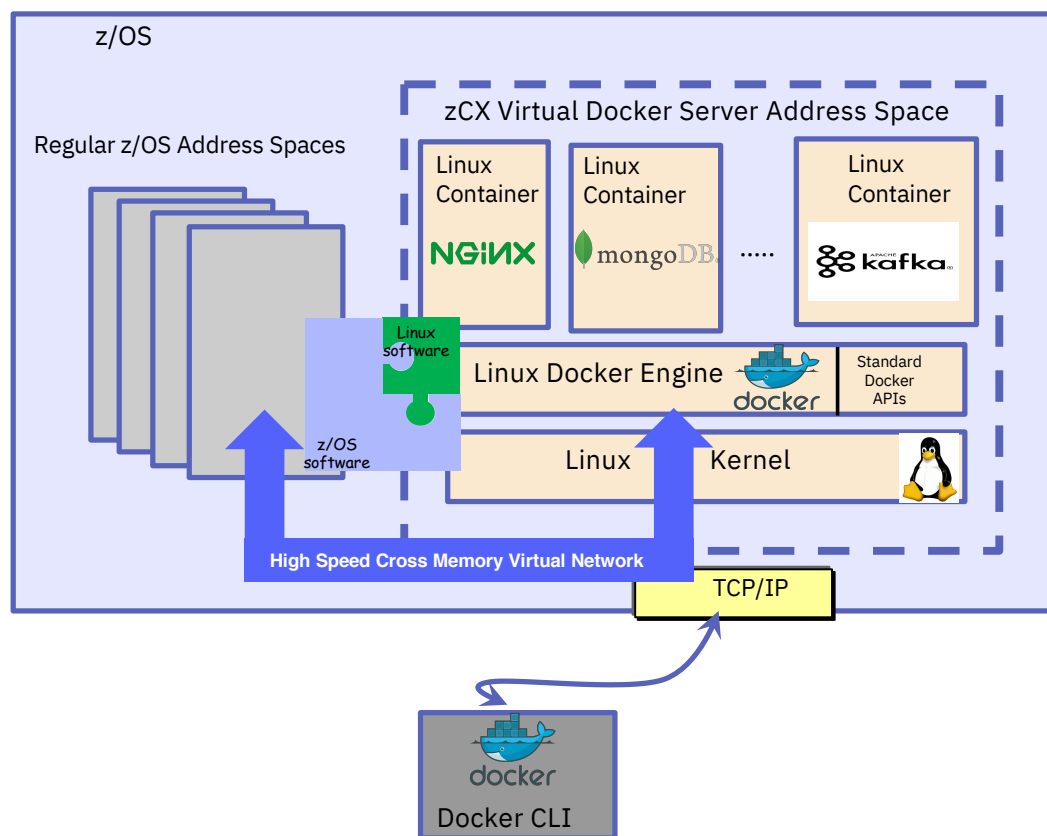
- Supports deployment of any software available as a Docker image for Linux on Z
- Communications with native z/OS applications over high speed virtual IP network
- No z/OS skills required to develop and deploy Docker Containers

No Linux system administration skills required

- Interfaces limited to Docker CLI
- No direct access to underlying Linux kernel

Managed as a z/OS process

- Multiple instances can be deployed in a z/OS system
- Managed using z/OS Operational Procedures
- zCX workloads are zIIP eligible



IBM zCX - Goals & Qualities of Service

Integrated Disaster Recovery & Planned Outage Coordination

Using z/OS DR/GDPS to cover storage used by Linux automatically, integrated restart capabilities for site failures, etc.

Integrated Planned Outage Coordination

No need to coordinate with non-z/OS administrators when planning a maintenance window, moving workloads to alternate CECs, sites, etc.

z/OS Storage Resilience

Eliminate single points of failure

Exploit z/OS VSAM which offers transparent encryption, and failure detection with HyperSwap

Configuration validation, I/O health checks,

Automatic exploitation zHyperLink and future z/OS Storage enhancements

z/OS Workload Management, Capacity Planning & Chargeback

WLM: Service Class goals, Business Importance levels, ability to cap resource consumption (CPU and memory)

Capacity Provisioning Manager (CPM) support

SMF support for accounting and chargeback

z/OS Networking Virtualization, Security & Availability

Support for VIPAs, Dynamic VIPAs allowing for non-disruptive changes, failover, and dynamic movement of the workload.

High speed and secure communications with Cross-Memory Virtual Network Interface (SAMEHOST)

Use Cases

Expanding the z/OS software ecosystem for z/OS applications

- Latest Microservices (logstash, Etcid, Wordpress, etc.)
- Non-SQL databases (MongoDB, IBM Cloudant, etc.)
- Analytics frameworks (e.g. expanding the z/OS Spark ecosystem)
- Messaging frameworks (example: Apache Kafka)
- Web server proxies (example: nginx)
- Emerging Programming languages and environments

System Management components

- System management components in support of z/OS that are not available on z/OS
- Centralized data bases for management
- Centralized UI portals for management products – Examples:
 - Tivoli Enterprise Portal (TEPS)
 - Service Management Unite (SMU)

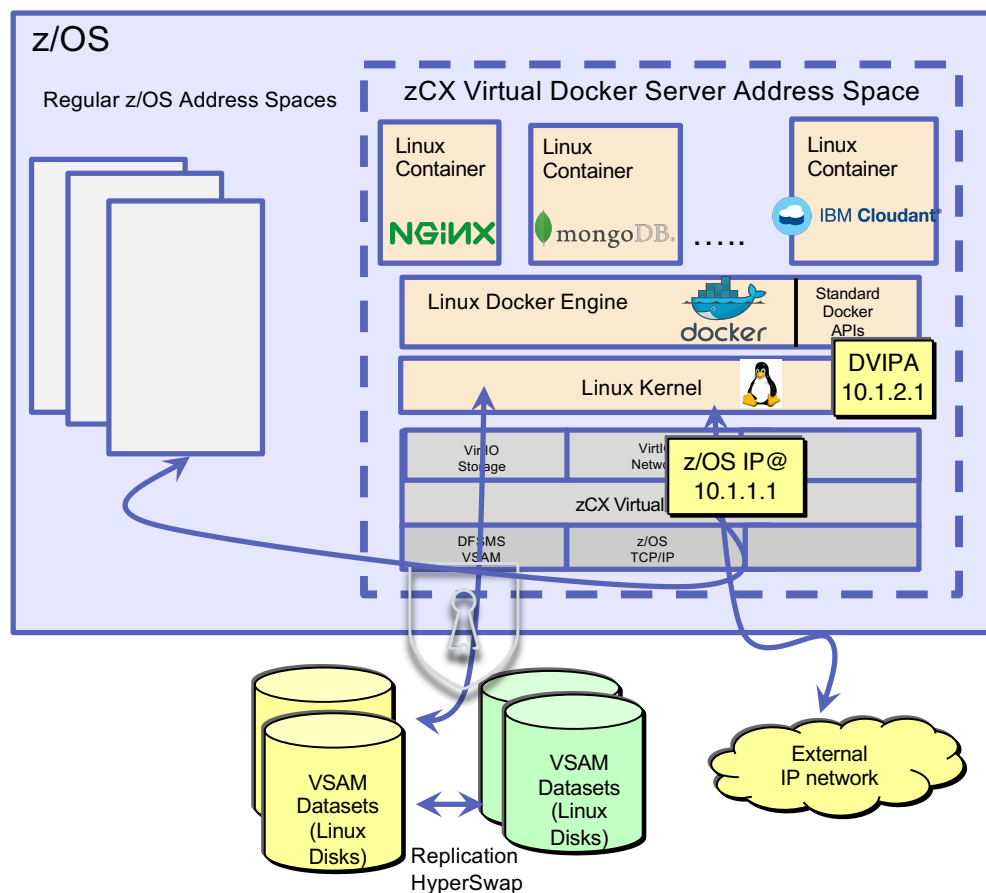
Open Source Application Development Utilities

- Complement existing z/OS ecosystem and Zowe and DevOps tooling
- Gitlab/Github server
- Linux based development tools
- Linux Shell environments
- Apache Ant, Apache Maven

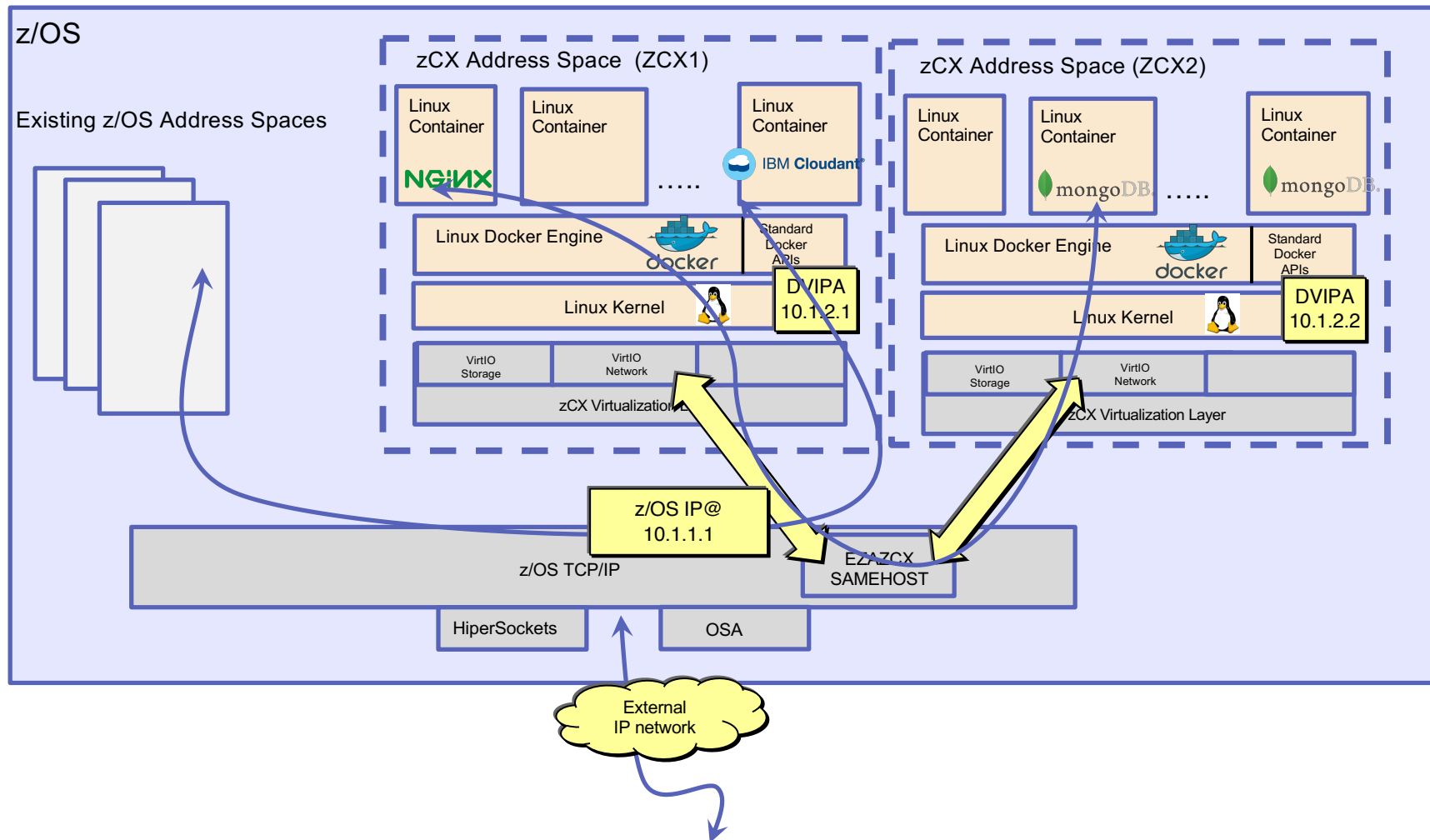
Note: The use cases depicted reflect the types of software that could be deployed in IBM zCX in the future. They are not a commitment or statement of software availability for IBM zCX

IBM zCX – z/OS Network Integration

- z/OS Linux Virtualization Layer:
 - Allows virtual access to z/OS Storage and Network
 - Using virtio Linux interfaces
 - Stable, well defined interfaces used to virtualize Linux
 - Allows us to support unmodified, open source Linux for z kernels
- Linux network access via high speed virtual *SAMEHOST* link to z/OS TCP/IP protocol stack
 - Each Linux Docker Server represented by a z/OS owned, managed and advertised Dynamic VIPA (DVIPA)
 - Allows restart of a CX instance in another system in the Sysplex
 - A new “application instance” DVIPA type “zCX” is introduced (created with the VIPARange statement)
 - Provide high performance network access across z/OS applications and Linux Docker containers – leveraging cross memory
 - External network access via z/OS TCP/IP
 - z/OS IP filters to restrict external access

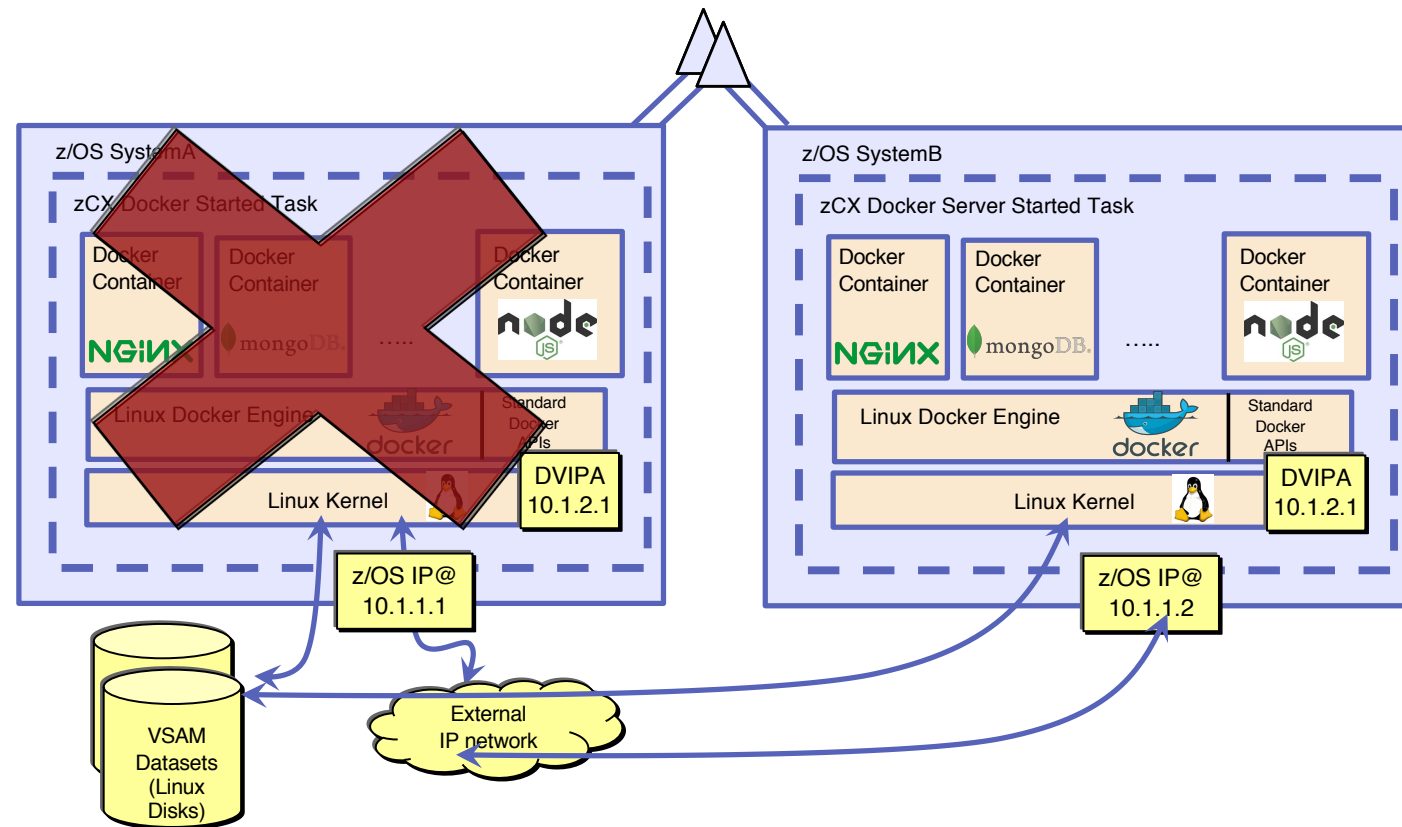


IBM zCX – High Speed Virtual IP Network - SAMEHOST



z/OS Container Extensions Operations and Disaster Recovery Integration

- Started using z/OS Start Command
 - Support for Start, Stop, Modify
- Automated Operations using z/OS facilities
 - ARM policy
 - System Automation
 - Other z/OS Automation framework/product
- Planned and Unplanned Outage and Disaster Recovery coordination
 - zCX Docker Server failure (restart in place)
 - LPAR failure (restart on other LPAR in the sysplex)



Usage and Invocation - zCX Network Configuration Steps

1. zCX Network Parameters (z/OSMF Workflows), for each server:
 - Configure zCX Server IP address (DVIPA)
 - DNS Name/IP Address
 - MTU (optional, default = 1492, suitable for most environments)

2. z/OS TCP/IP profile:
 1. zCX DVIPA(s)
Using VIPARange, configure DVIPA ZCX
The DVIPA must match zCX server configuration! (Must match the z/OSMF Workflow configuration, step 1 above).

 2. EZAZCX interface is created when the EZASAMEMVS (samehost) interface is created.

 Note. When using DynamicXCF or have enabled IUTSAMEH for Enterprise Extender both EZASAMEMVS (samehost) and EZAZCX interfaces are dynamically created and started. If you're not using Dynamic XCF or Enterprise Extender, then you must manually define (dev/link/home) IUTSAMEH (which will also create EZAZCX)

3. OMPROUTE configuration:
 - Define Dynamic VIPAs for zCX, advertise as hosts route (use of wildcarding suggested) – similar to existing DVIPA definitions

4. IPsec Policy:
 - If you have IP Filters defined you need to ensure that you permit ROUTED and LOCAL traffic for these DVIPAs

VIPARange ZCX (syntax and definition)

```

•          .-DEFINE- .-MOVEable NONDISRUPTive--.
• >>-VIPARange-----address_mask--ipv4_addr-----
----->
•          '-DELEte-' | '-MOVEable DISRUPTive-----'          'SAF resname'
|
•          | .-MOVEable NONDISRUPTive--. |
•          |'-----ipv6_intfname--ipv6_addr/prefix_len--
|
•
•
• >-----X
•          '---ZCX---'

```

Notes:

- zCX DVIPAs are defined with VIPARANGE with a new keyword “ZCX”.
- The MOVEABLE keyword is ignored on a ZCX VIPARANGE (i.e. a zCX DVIPA can't be activated if already active).
- An expected use case is that a zCX VIPARANGE may exist on multiple hosts so it should remain in sysplex VIPARange configuration.
- Support will also be available in the z/OSMF Network Configuration Assistant for defining zCX DVIPAs under the Configure Sysplex Networking actions

Modernize and Extend your
z/OS® Applications with

IBM z/OS® Container Extensions(zCX)

Resource	Link
Content Solutions Page	http://ibm.biz/zOSContainerExtensions
Open Z Systems Exchange	http://ibm.biz/openzsx
zCX FAQ	http://ibm.biz/zcx_FAQ

z/OS Encryption Readiness Technology (zERT)



IBM z Systems Pervasive Encryption

Enabled through tight platform integration



Integrated Crypto Hardware



Data at Rest



Clustering



Network



Secure Service Container

Background: Encrypting TCP/IP network traffic on z/OS

z/OS provides 4 mechanisms to protect TCP/IP traffic:

1 TLS/SSL direct usage

- Application is explicitly coded to use these
- Configuration and auditing is unique to each application
- Per-session protection
- TCP only

2 Application Transparent TLS (AT-TLS)

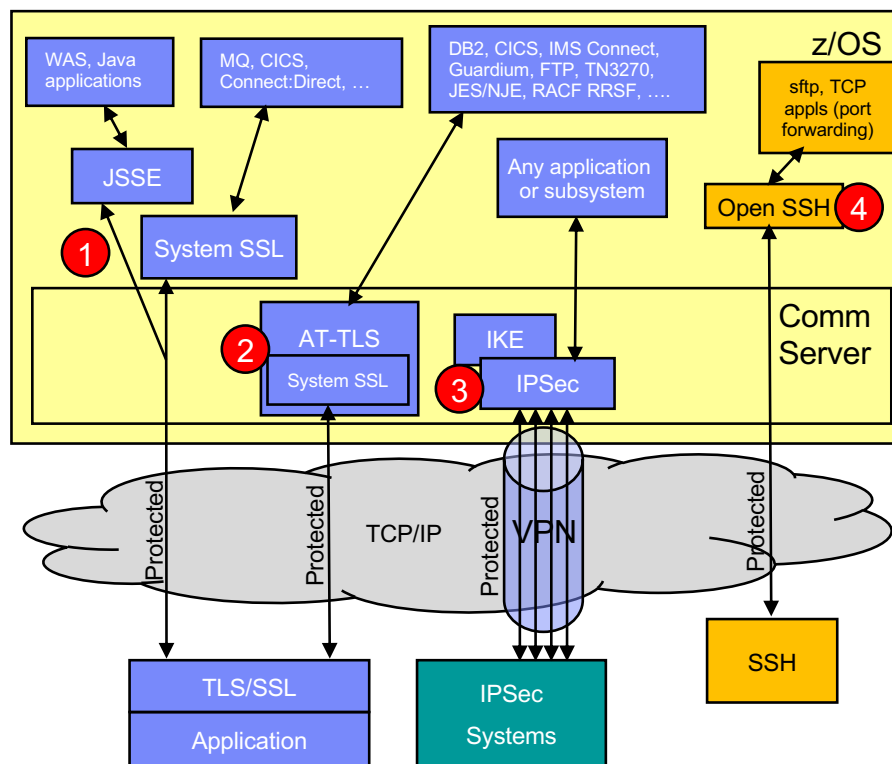
- TLS/SSL applied in TCP layer as defined by policy
- Configured in AT-TLS policy via Network Configuration Assistant
- Auditing through SMF 119 records
- Typically transparent to application
- TCP/IP stack is user of System SSL services

3 Virtual Private Networks using IPSec and IKE

- “Platform to platform” encryption
- IPSec implemented in IP layer as defined by policy
- Auditing via SMF 119 records at tunnel level only
- Completely transparent to application
- Wide variety (any to all) of traffic is protected
- IKE negotiates IPSec tunnels dynamically

4 Secure Shell using z/OS OpenSSH

- Mainly used for sftp on z/OS, but also offers secure terminal access and TCP port forwarding
- Configured in ssh configuration file and on command line
- Auditing via SMF 119 records
- TCP only

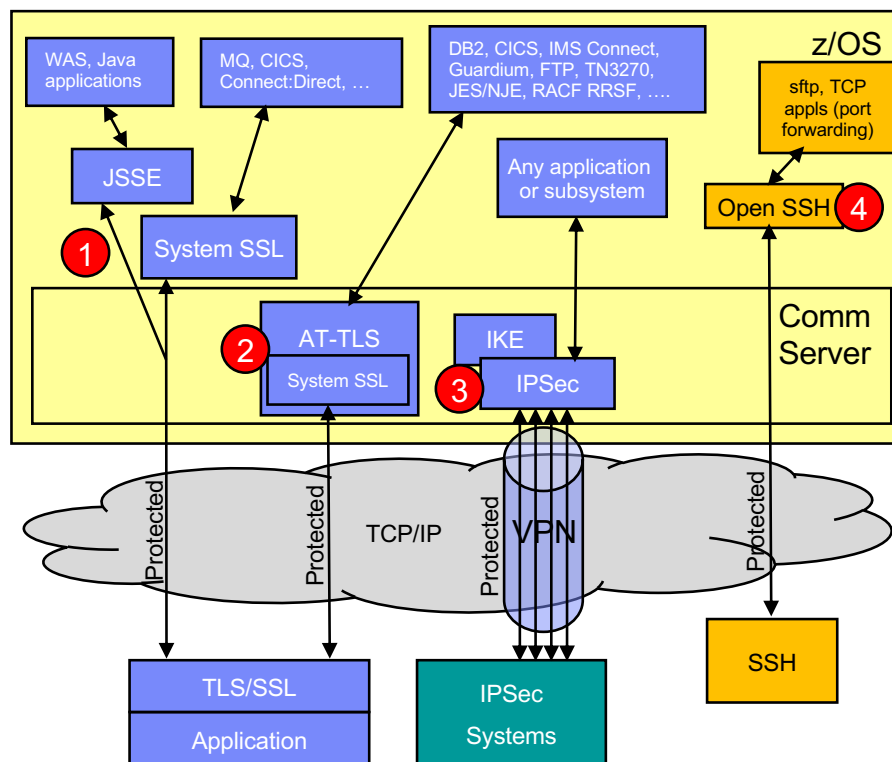


Background ...

Given all these mechanisms, configuration methods and variation in audit detail...

▪ **How can I tell...**

- **Which traffic** is being protected (and which is not)?
 - **How** is that traffic being protected?
 - Security protocol?
 - Protocol version?
 - Cryptographic algorithms?
 - Key lengths?
 - ...and so on
 - **Who** does on the traffic belong to in case I need to follow up with them?
- How can I ensure that new configurations adhere to my company's security policies?
- Once I've answered the above questions, how can I provide the information to my auditors or compliance officers?
- Many factors driving these questions:
- Regulatory compliance (corporate, industry, government)
 - Vulnerabilities in protocols and algorithms
 - Internal audits
 - ...and so on



Introducing z/OS Encryption Readiness Technology (zERT)

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

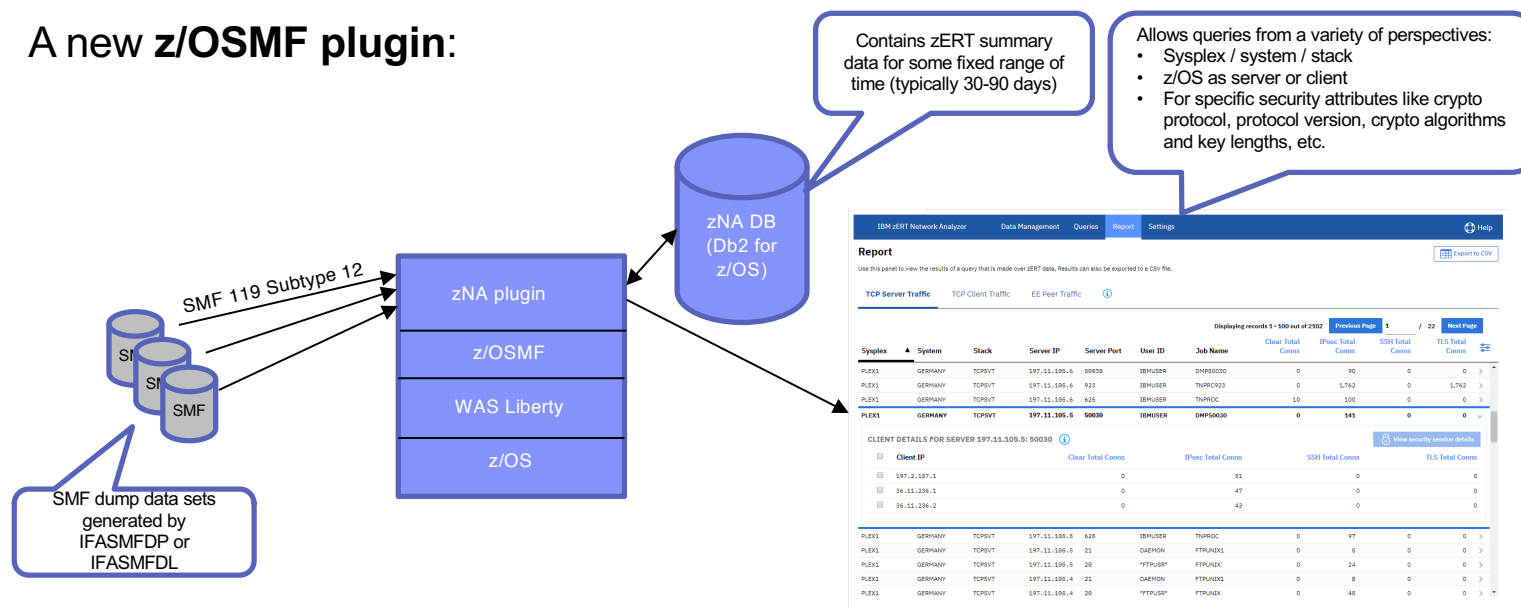
- zERT positions the TCP/IP stack as a central collection point and repository for cryptographic security attributes for:
 - TCP connections that are protected by TLS, SSL, SSH, IPsec or are unprotected
 - Enterprise Extender connections that are protected by IPsec or are unprotected
- Two methods for discovering the security sessions and their attributes:
 - Stream observation (for TLS, SSL and SSH) – the TCP/IP stack observes the protocol handshakes as they flow over the TCP connection
 - Advice of the cryptographic protocol provider (System SSL, OpenSSH, TCP/IP's IPsec support)
- Attributes are collected on a per-connection basis
- Reported through a new SMF 119 record (subtype 11, 12) via:
 - SMF and/or
 - New SYSTCPER and SYSTCPES real-time NMI services

z/OS Encryption Readiness Technology

- zERT Discovery – **available in base V2R3**
 - Attributes are collected and recorded at the connection level
 - SMF 119 subtype 11 “zERT Connection Detail” records
 - These records **describe the cryptographic protection history of each TCP and EE connection**
 - Measures are in place to minimize the number of subtype 11 records, but they could still be very voluminous
- zERT Aggregation – **provided in March, 2018 via new function APAR PI83362**
 - Attributes collected by zERT discovery are aggregated by security session
 - SMF 119 subtype 12 “zERT Summary” records
 - These records **describe the repeated use of security sessions over time**
 - **Aggregate connection data from repeated connections between a TCP client and server**
 - Aggregation can greatly reduce the volume of SMF records while maintaining the fidelity of the information – well suited for reporting applications

zERT Network Analyzer (zNA)

- A new **z/OSMF** plugin:



- **Web UI** makes zERT data consumable for **z/OS network security administrators** (typically systems programmers)
- Used primarily to investigate specific network encryption questions (but could also be used for periodic report generation)
- Additional zNA screenshots in appendix
- Provided in December, 2018 via new function APAR PH03137
 - Refer to the [New Function APAR Summary](#) page for more details

Summary

- There is a growing need to be able to identify and enumerate the cryptographic protection attributes for network traffic for key workloads on z/OS systems
- With zERT, a z/OS network administrator can discover and audit the network encryption attributes associated with TCP and Enterprise Extender traffic by analyzing new SMF records.
- zERT positions the z/OS TCP/IP as a central collection point and repository for those attributes. The attributes can be written as SMF 119 subtypes 11 and 12 records to one or both of:
 - SMF
 - SYSTCPER and SYSTCPES real-time NMI services
- The zERT Network Analyzer plug-in for z/OSMF provides an easy-to-use UI for querying data reported in SMF 119 subtype 12 records
- With zERT discovery, aggregation and reporting in place, more advanced capabilities for analyzing z/OS network cryptographic protection become possible
- For much more on zERT:

***session: EF: Pervasive Encryption: Get a Grip on Your z/OS Network Encryption with zERT
 Tuesday, Nov 5, 2019: 16:45 PM - 17:45 PM
 Stowe
 Speaker: Jerry Stevens (IBM Corporation)***

z/OS Encryption Readiness Technology

Functions and performance



Discovery (available at V2R3 general availability)

Discover the network encryption attributes for all TCP and Enterprise Extender traffic and record them in SMF format.



Aggregation (available in V2R3 with APAR PI83362/UI54759)

Use zERT to **summarize** high volumes of granular zERT SMF records into a condensed SMF representation.



IBM zERT Network Analyzer

(available in V2R3 with z/OSMF APAR PH03137)

A **web-based GUI** for analyzing the SMF data that zERT records.

zERT Discovery and Aggregation performance overview

- Enabling zERT has **little to no impact** on latency or CPU consumption.
- The CPU results reflect networking related CPU costs **only which are a small fraction** of the overall system CPU costs.
- Results obtained using applications with no application logic (micro-benchmarks).
- In a real workload the percent of CPU increases or decreases would be much smaller compared to the overall system CPU utilization.
- All zERT storage obtained from **64-Bit private** (minimize footprint).
- Aggregation **minimizes** SMF records created.

For more details, see [z/OS Communications Server V2R3 Performance Summary report](#).

z/OS Encryption Readiness Technology

Useful materials



zERT documentation

- [zERT discovery documentation](#)
- [zERT aggregation documentation](#)
- [IBM zERT Network Analyzer documentation](#)
- [IBM zERT Network Analyzer tutorial](#)



zERT social posts

- [Things you should know about zERT – zERT all-in-one page \(http://ibm.biz/thingsaboutzert\)](http://ibm.biz/thingsaboutzert)



zERT webinar

- [Getting a grip on your z/OS network encryption \(http://ibm.biz/zertwebinar\)](http://ibm.biz/zertwebinar)

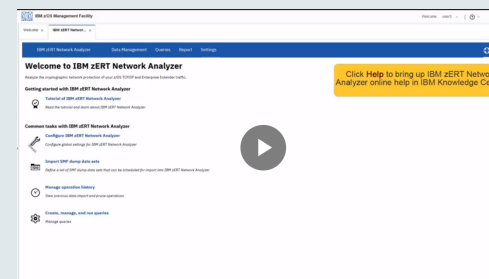


zERT video

- [zERT overview introductory video](#)



- [IBM zERT Network Analyzer overview demo video](#)



Pervasive Encryption Fast Start for IBM Z – Badge requirements

To earn a badge for this track, you must do the following:

1. Enroll in Pervasive Encryption Fast Start (send email to tpearson@us.ibm.com)

2. Attend at least 9 of 12 lectures listed here (name and signature on sign-in sheet or badge scan)

3. Complete all required lab exercises. You will be assigned to one of 3 lab time slots. Lab instructors will record your name after you show them you have completed those exercises.

z109203 E4S: Pervasive Encryption: Get a Grip on Your z/OS Network Encryption with zERT

z109372 E4S: The encryption pyramid - Choosing the level that works for you

z109374 E4S: z/OS cryptographic key management fundamentals (Part 1)

z109375 E4S: z/OS cryptographic key management fundamentals (Part 2)

z109376 E4S: Pervasive encryption: Protecting the keys to the kingdom

z109377 E4S: A guided tour of policy-based data set encryption

z110021 E4S: The new and improved IBM Z Batch Network Analyzer (zBNA)

z110272 E4S: z/OS data set encryption - Implementation best practices

z110273 E4S: Pervasive encryption: Protect your data at rest with z/OS data set encryption

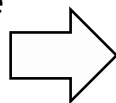
z110331 E4S: Protecting data through encryption of Coupling Facility structures

z110349 E4S: Pervasive encryption for z/VM and Linux on Z

z110404 E4S: IBM Z and LinuxONE pervasive encryption: Putting data protection into practice

z109369 E4S: Pervasive Encryption Fast Start -- All lab exercises (Part 1)

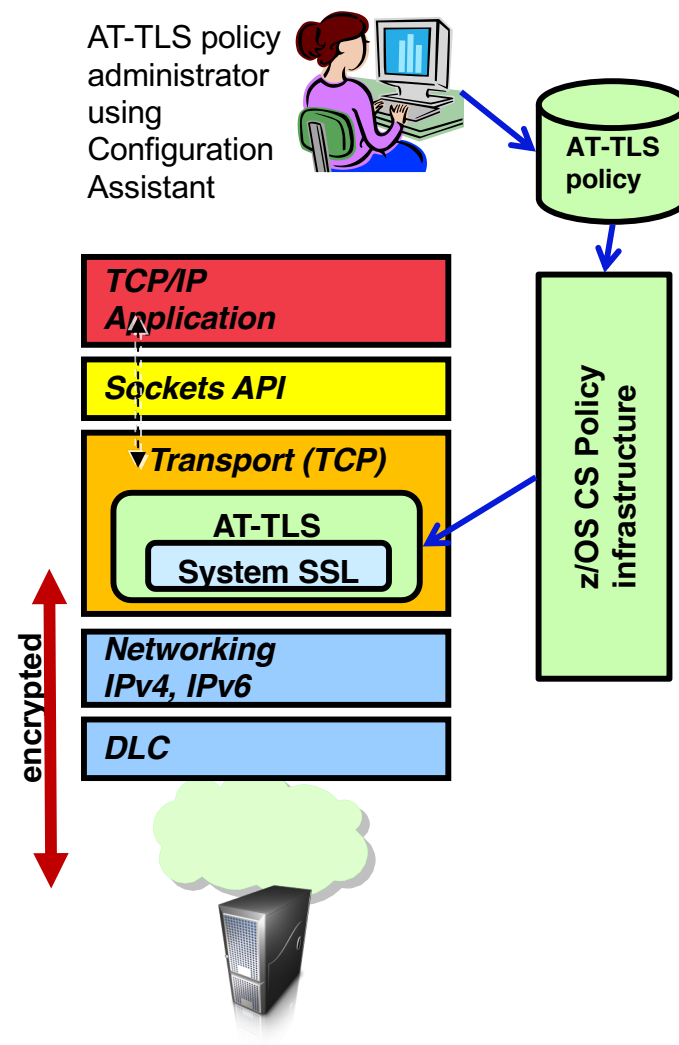
z109371 E4S: Pervasive Encryption Fast Start -- All lab exercises (Part 2)



AT-TLS Support for TLSv1.3

Application Transparent Transport Layer Security (AT-TLS)

- Stack-based TLS
 - TLS process performed in TCP layer (via System SSL) without requiring any application change (transparent)
 - AT-TLS policy specifies which TCP traffic is to be TLS protected based on a variety of criteria
- Application transparency
 - Can be fully transparent to application
 - An optional API allows applications to inspect or control certain aspects of AT-TLS processing – “application-aware” and “application-controlled” AT-TLS, respectively
- Uses System SSL for TLS protocol processing
 - Remote endpoint sees an RFC-compliant implementation
 - Interoperates with other compliant implementations



What's new in AT-TLS?



Basic TLSv1.3 protocol support

- **RFC 8446** - The Transport Layer Security (TLS) Protocol Version 1.3
 - Adopted as a standard August 2018
 - This is a **significantly different protocol** than SSLv2-TLSv1.2
-
- Let's take a quick look at TLSv1.3 vs. its predecessors and how System SSL and AT-TLS implement it...

TLSv1.3 focus: Better security, protocol efficiency

Cipher suites:

- New format – **key exchange algorithm now specified separately** from the cipher suite
- Only using Authenticated Encryption with Associated Data (AEAD) or “combined mode” encryption
- Only 5 cipher suites defined – System SSL only supports 3 of these (TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256)

Several new cryptographic algorithms:

- RSASSA-PSS signature algorithm. This **MUST** be used whenever RSA certificates are used for authentication
- x25519 and x448 “Edwards curves”
- ChaCha20-Poly1305 symmetric encryption algorithm
- Uses HKDF key derivation algorithm

Key Exchange:

- Only uses ephemeral Diffie-Hellman key exchange – System SSL only supports ECC variants (ECDHE)
- Guarantees perfect forward secrecy
- Eliminates fixed RSA key exchange

In general, more cryptographically intensive than predecessors:

- Multiple key derivation operations per handshake
- Exclusive use of ephemeral Diffie-Hellman (DHE/ECDHE) makes key generation mandatory (DHE/ECDHE is optional in prior versions)

zERT and the zERT Network Analyzer include support for TLSv1.3 in z/OS V2R4.

HiperSockets Converged Interface (HSCI) Support

Problem Statement

There are two main issues:

1. z/VM Bridge, SSI and LGR and Linux (Layer 2) Incompatibility:

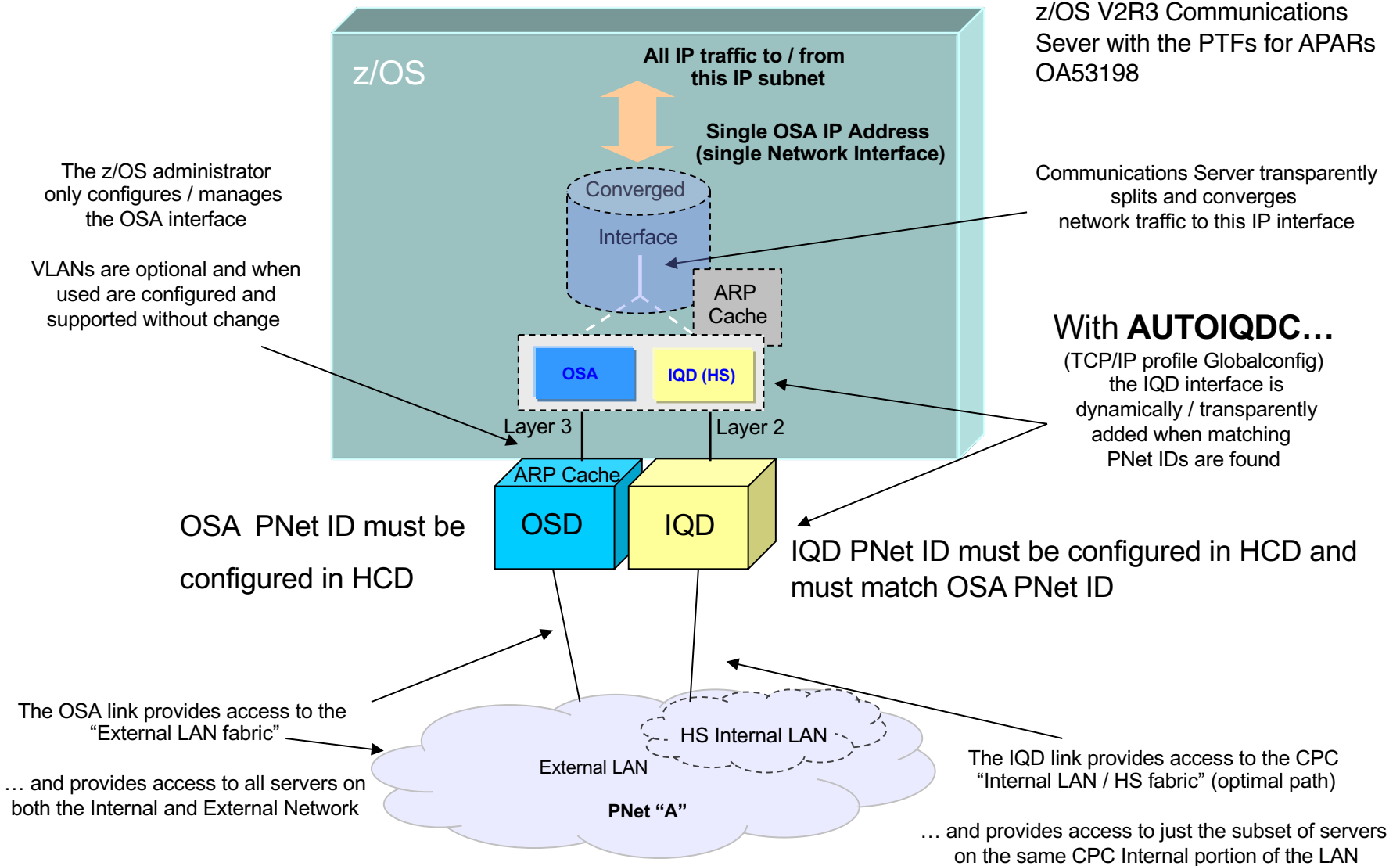
The z/VM Bridge support provides a very competitive and seamless solution for the overall System z networking landscape for Linux on z clients. There are many advantages (e.g. allows single IP interface per Linux guest) to the z/VM bridge model and enables Live Guest Relocation in a z/VM SSI environment. However, z/OS does not support (L2) connectivity to Linux in this configuration. The missing z/OS support creates a gap in the overall value of the z System solution (Layer 2 Linux compatibility, HS, z/VM Bridge, VSwitch etc.)

2. z/OS HiperSockets usability:

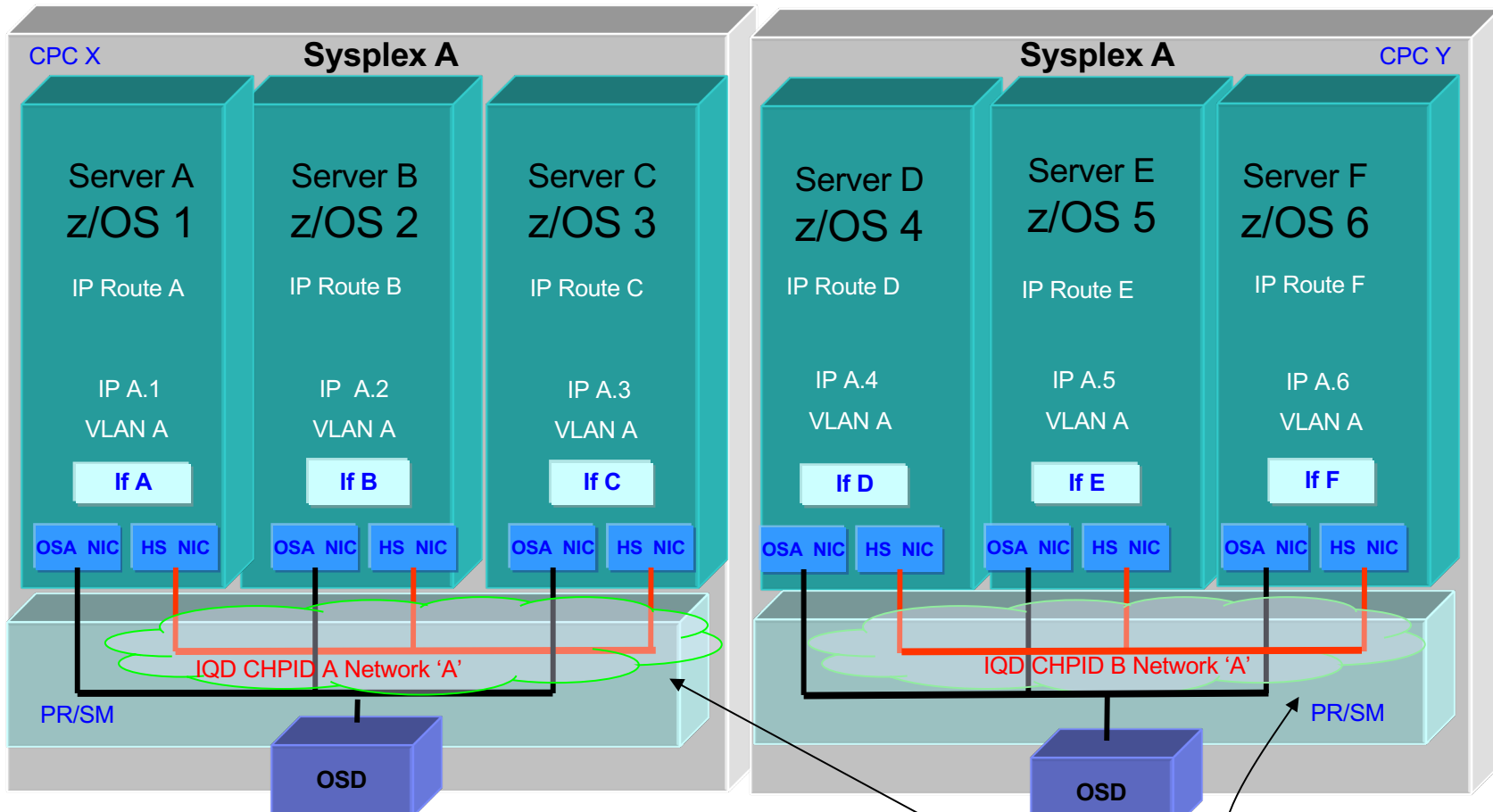
When moving a z/OS instance to another CPC, it requires manual administrative actions to reconfigure the HS interfaces to match the new IP subnet(s) on the new CPC. This applies to all z/OS environments (even in z/OS only environments). Some customers regularly / frequently move their z/OS instances. Customers have expressed concerns about this issue (i.e. how this manual step impacts their day to day operations causing some customers to rethink or stop using HS).

z/OS HiperSockets Converged Interface (HSCI)

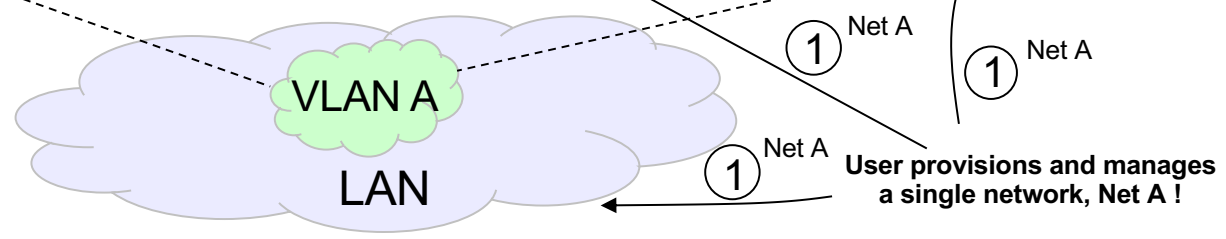
HiperSockets Converged Interface (HSCI) support is provided on z/OS V2R3 Communications Server with the PTFs for APARs OA53198




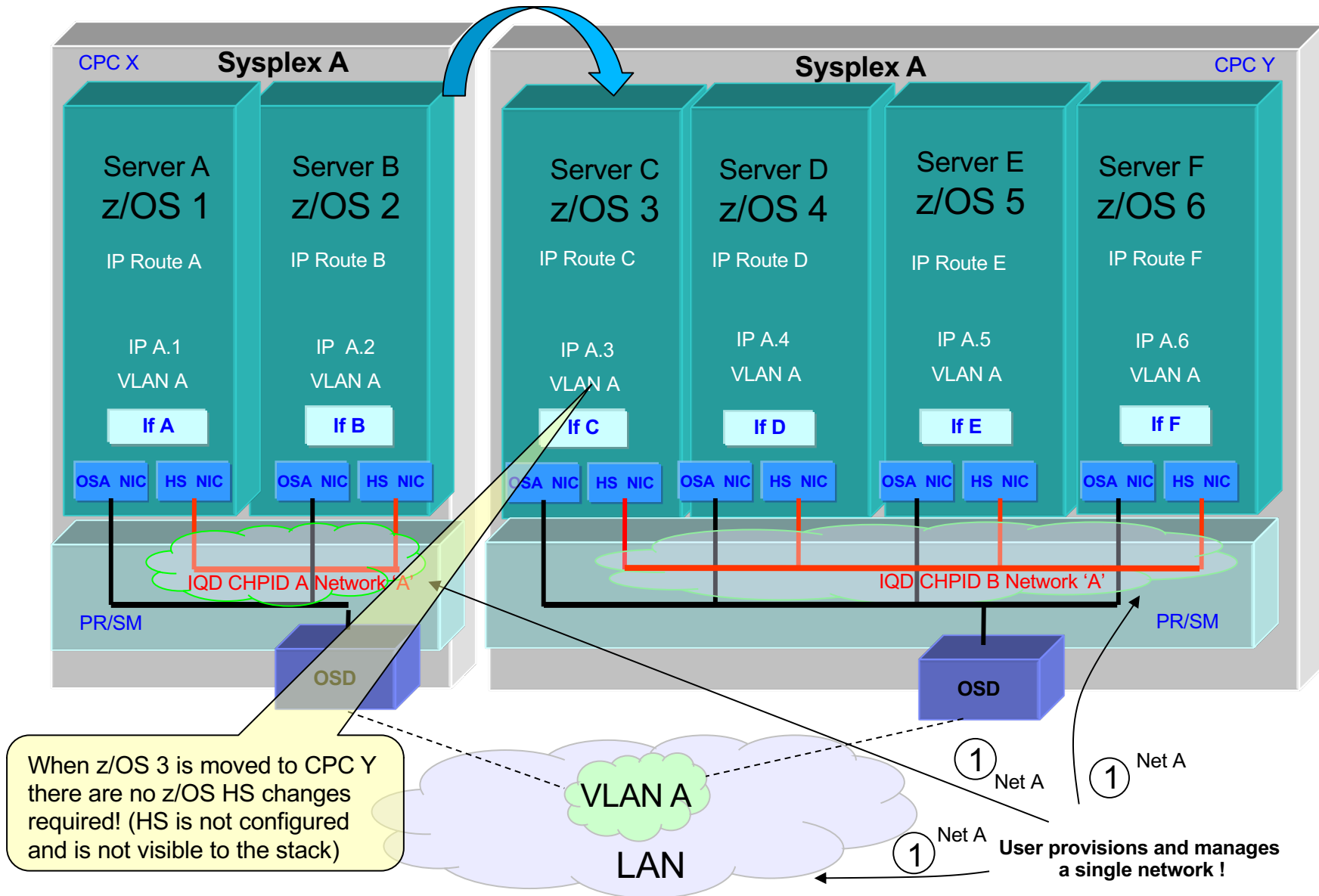
z/OS-only with HSCI: Each host now sees a single IP network (subnet A)



Now each z/OS image has access to 1 network (network A), via "OSA" HS is not visible to the TCP/IP stack!



z/OS-only with HSCI: Moving a z/OS instance with no HS configuration changes! 



For additional information



- Additional details in appendix
- Screencast on the z/OS CS YouTube channel:

Screencast of a presentation on Hipersockets Converged Interface Support:

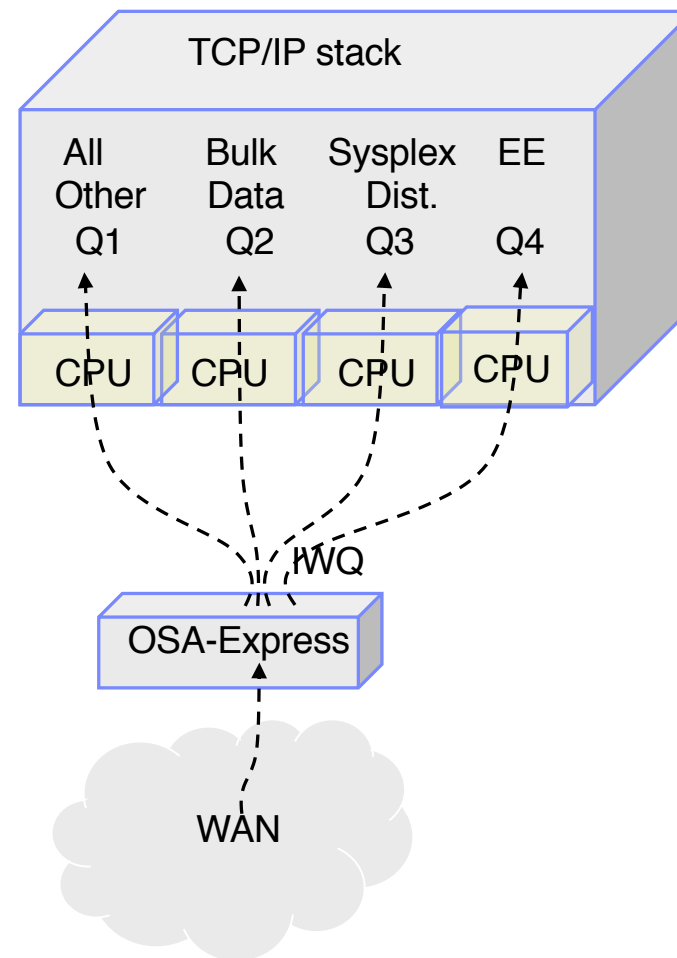
<https://www.youtube.com/watch?v=o0jK5walPoQ>

IWQ Support for IPSec

Background information: Inbound workload queueing (IWQ)

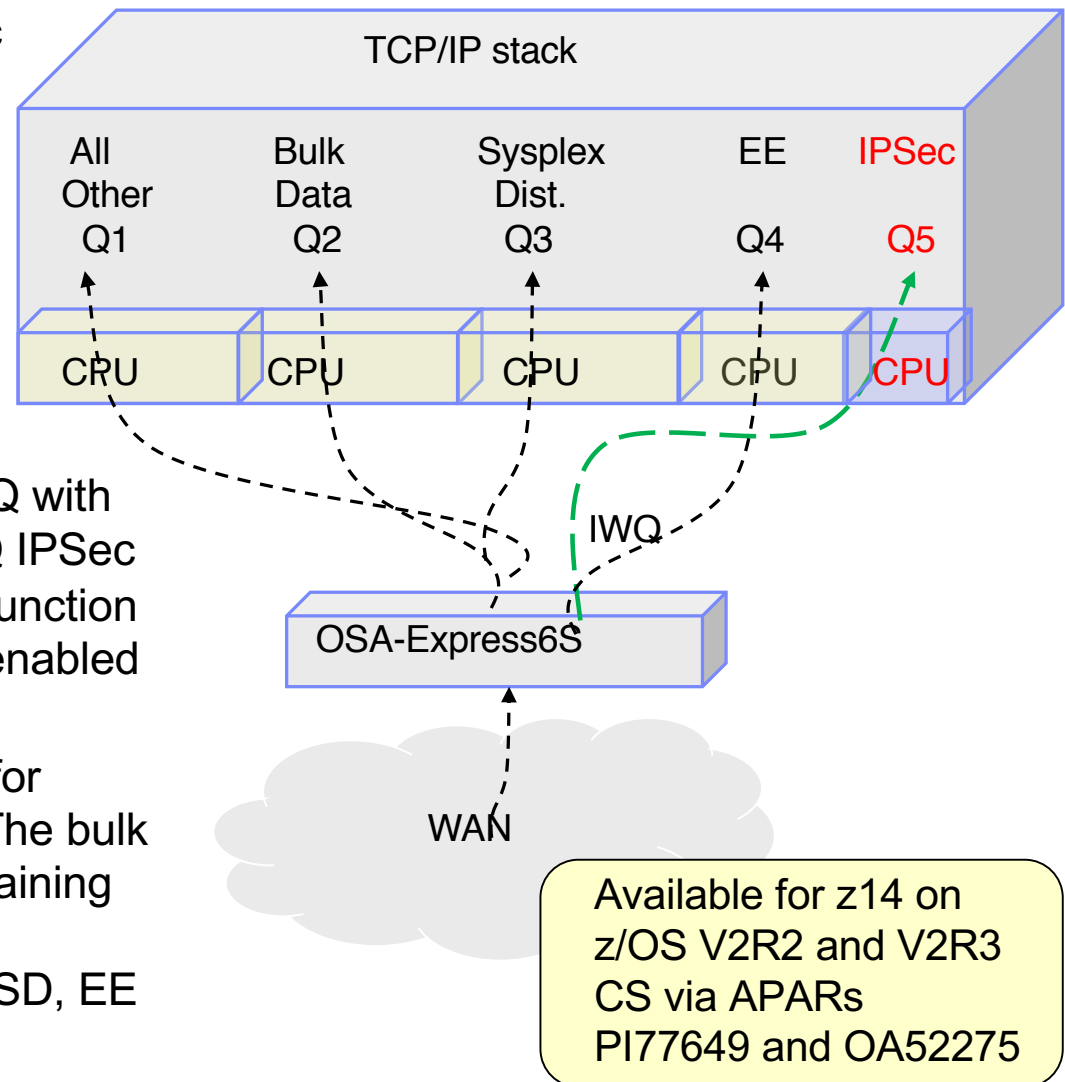
- OSA separates inbound packets and routes them over four different ancillary input queues on the same interface
 - Bulk data (such as FTP)
 - Sysplex Distributor (SD)
 - Enterprise extender (EE)
 - All other traffic (primary)

- z/OS can service each queue concurrently using separate processors
- Stack receives pre-sorted packets
- Enabled via:
 INBPERF DYNAMIC WORKLOADQ on
 IPAQNET and IPAQNET6 INTERFACE
 statements (only)



QDIO inbound workload queueing for IPSec (2Q2018)

- New ancillary input queue for IPSec
- IPSec traffic serviced on its own processor
- Processing of IPSec queue is optimized since the only traffic on the queue is IPSec
- IPSec-protected bulk, SD, or EE traffic uses IPSec queue
- For customers who already use IWQ with OSA-Express6S and apply the IWQ IPSec enablement PTFs, the IWQ IPSec function (input queue) will automatically be enabled (input queue is defined).
- There are no configuration options for controlling each input queue type. The bulk queue is always active and the remaining input queues are used when the corresponding function is enabled (SD, EE and IPSec).

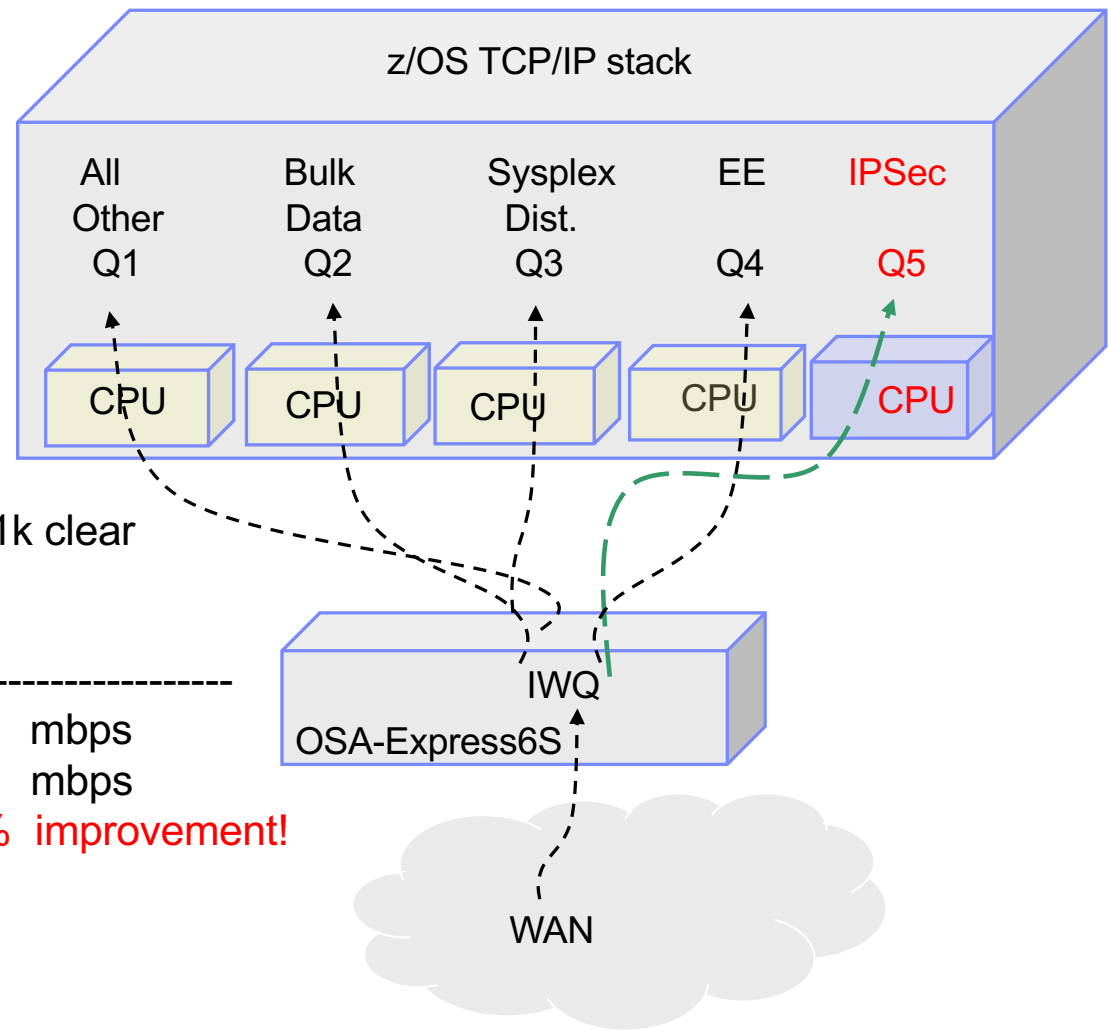


IWQ for IPsec: Performance Summary

Performance testing shows the following throughput improvement:

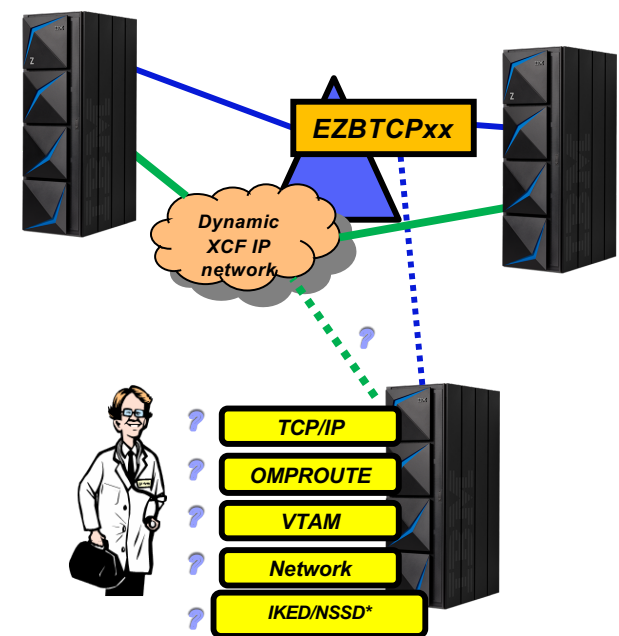
RR10 1k encrypted mixed with RR10 1k clear

	encrypted / clear	
Without IWQ:	59 mbps	53 mbps
With IWQ:	74 mbps	81 mbps
	25 %	52 % improvement!



Sysplex Notification of TCP/IP Stack Join or Leave

Sysplex autonomics: Background information



Sick? Better remove myself from the IP Sysplex!



Feeling better? Maybe it's time to rejoin the IP Sysplex

- Monitoring:
 - Monitor CS health indicators
 - Storage usage critical condition (>90%) - CSM, TCPIP Private & ECSA
 - Monitor dependent networking functions
 - OMPROUTE availability
 - VTAM availability
 - XCF links available
 - Monitor for abends in Sysplex-related stack components
 - Selected internal components that are vital to Sysplex processing
 - Selected network interface availability and routing
 - Monitor for repetitive internal abends in non-Sysplex related stack components
 - 5 times in less than 1 minute
- Actions:
 - Remove the stack from the IP Sysplex (manual or automatic)
 - Retain the current Sysplex configuration data in an inactive state when a stack leaves the Sysplex
 - Reactivate the currently inactive Sysplex configuration when a stack rejoins the Sysplex (manual or automatic)

Sysplex autonomics: Background information ...

- Sysplex autonomics may cause a TCPIP stack to leave a sysplex group when a problem is detected.
 - Stack managed DVIPAs move to backup systems
 - Application instance DVIPAs (app-instance) are deleted and only apps using bind-activated DVIPAs are notified.
 - Apps using IOCTL-activated DVIPAs are not notified.
 - **Issue: Network processing may continue as if the deleted DVIPAs still exist.**

Sysplex autonomics: Problem statement

- Sysplex Autonomics recovery may remove a problematic TCPIP stack from a sysplex group.
 - DVIPA activated via IOCTL/MODDVIPA are deleted and applications using them are never notified
 - New connections to deleted DVIPA will timeout
- This could result in unnecessary connection slowdowns or inability to form new connections

Sysplex autonomics: Event notification facility signal

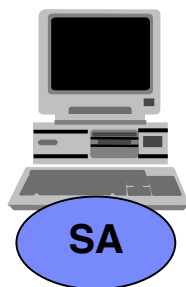


- The Event Notification Facility (ENF) allows applications to listen for specific system events
- ENF Code 80 now has a new event qualifier to represent the following TCPIP system events:
 - TCPIP leaves the Sysplex group for any reason (autonomics, manual termination, failure, etc.)
 - TCPIP joins the Sysplex group
- New mapping for this ENF signal contains the following:
 - Flag bits representing a join or a leave
 - The job name of the TCPIP stack performing the leave or join
- User can use this signal to make an appropriate decision based on whether the stack left or joined the group
- Additional details are in the appendix

Sysplex Autonomics for IPSec

Sysplex Wide Security Associations

Client (with IKED)



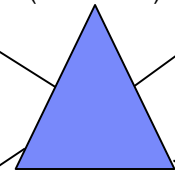
Distributor (with IKED)



Backup (with IKED)



Coupling Facility
(tunnel data)



Target



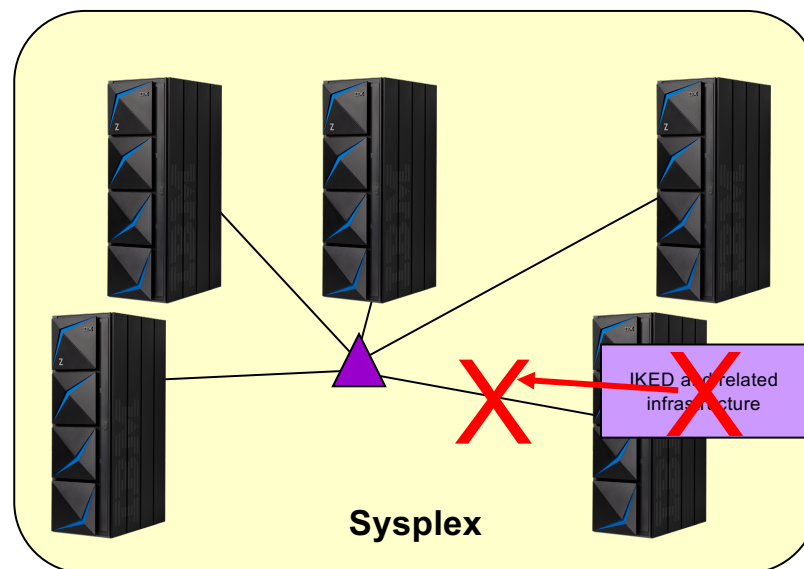
Target



- Sysplex Distributor
 - Negotiates SAs with remote Client using the Internet Key Exchange protocol
 - Sends copies of SAs (shadows) to targets
- Targets use SAs to encrypt and decrypt data
- Backup can recover SAs in case of DVIPA takeover
- Coupling Facility stores shared data
 - Tunnel data
 - AH/ESP sequence numbers

Sysplex autonomics for IPsec

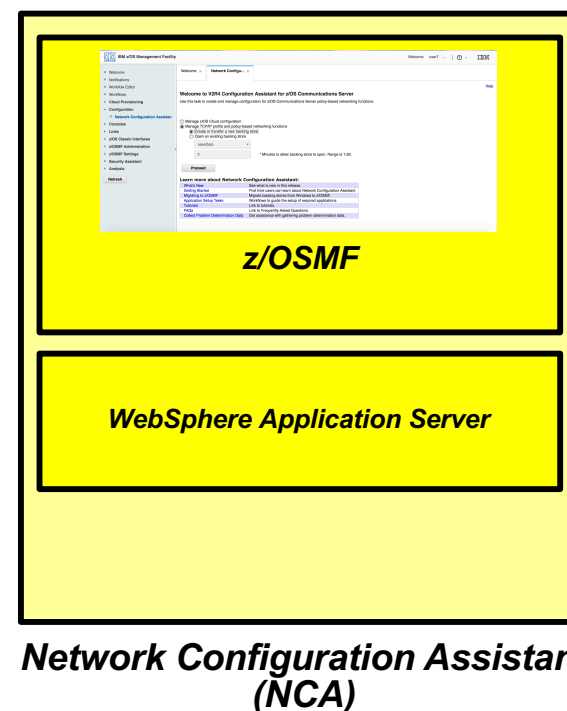
- Planned for 1Q2020 – APAR PH12788
- Sysplex autonomics support enhanced to monitor health of IPsec infrastructure relative to sysplex traffic
- For use with critical applications that depend on Sysplex-wide Security Associations (SWSA)
- Delay joining the sysplex until IPsec infrastructure is ready to go
- Ongoing monitoring once the system joins the sysplex
- Honors existing SYSPLEXMONITOR parameters like RECOVERY, AUTOREJOIN
- Additional detail in appendix



Network Configuration Assistant Updates

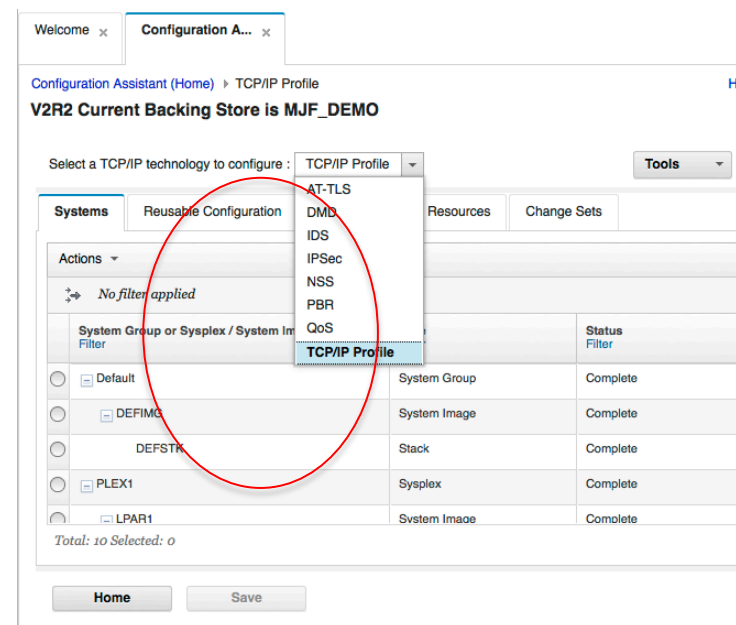
Network Configuration Assistant: TCP/IP stack configuration

- Skilled z/OS system programmers and administrators are an aging skillset, leading to concerns about future skill shortages.
- Prior to z/OS V2R2, Network Configuration Assistant (NCA) only supported configuration of z/OS CS policy-based networking functions, such as IPsec, AT-TLS, and IDS.
- While TCP/IP configuration is not that complex, some aspects are not intuitive.
- User must look through a lot of documentation.
- Some statements are not easy to configure.

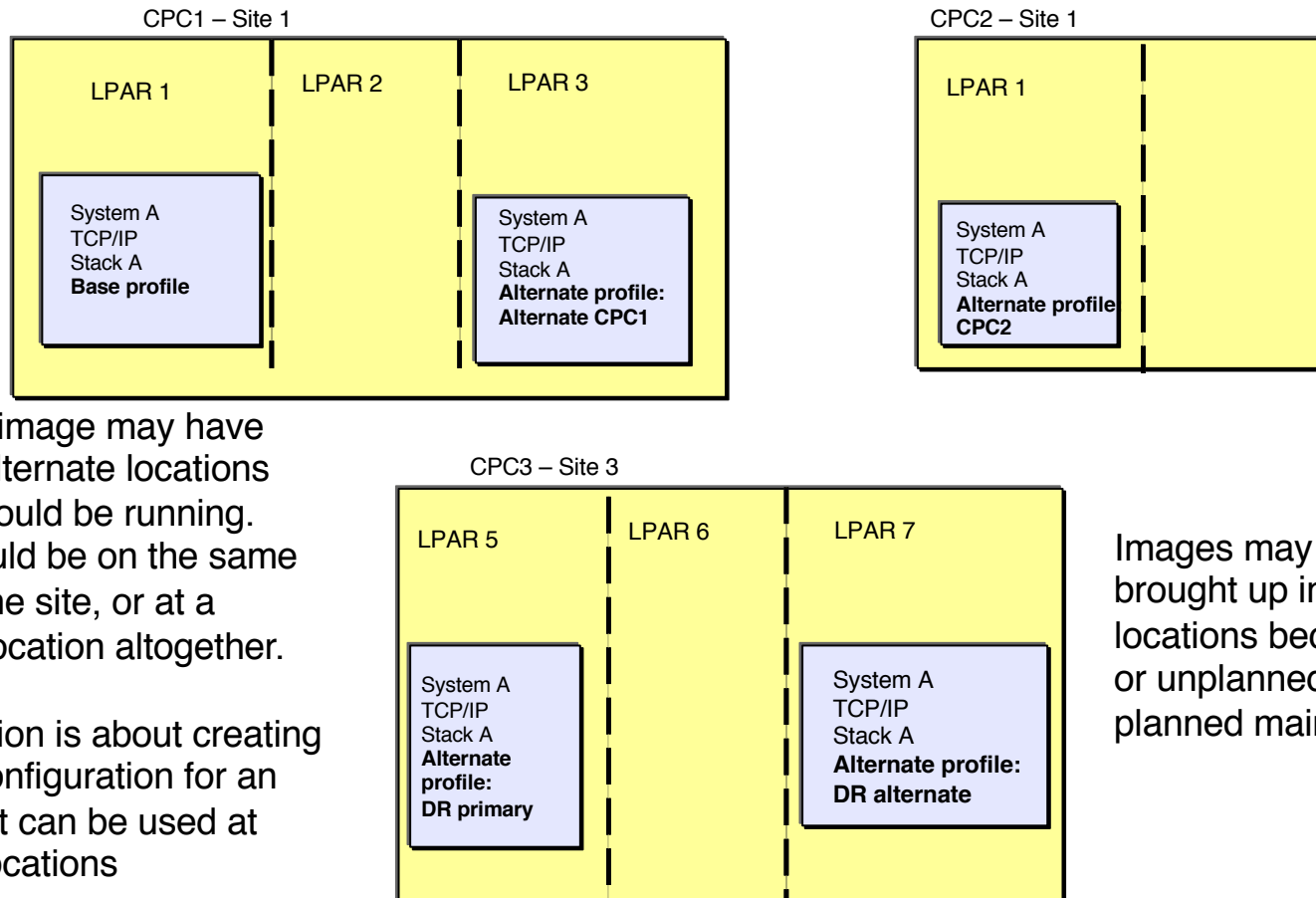


Network Configuration Assistant: TCP/IP stack configuration ...

- z/OS V2R2 provided a new “TCP/IP” configuration perspective in the NCA, with support provided for both novice and more experienced users.
- NCA allows for the import of an existing TCP/IP profile by first running the VARY TCPIP,,EXPORTPROF operator command and then importing the resulting file into NCA.
 - Requires APARs PI66143 (NCA) and PI63449 (z/OS CS) for V2R2. (Base in V2R3)
- VARY OBEY is supported in Network Configuration Assistant by introducing a new configuration object called a “Change Set”. The change set is edited to make the configuration changes you want, and then NCA will generate the VARY OBEY file necessary to put the changes into effect.
 - The VARY OBEY files must be manually applied by the operator.
 - Requires APAR PI80101 for V2R2 (Base in V2R3).



Network Configuration Assistant support for High Availability / Disaster Recovery: background



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.

This function is about creating TCP/IP configuration for an image that can be used at multiple locations

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

Network Configuration Assistant alternate configurations function

Network Configuration Assistant (Home) > TCP/IP Profile

V2R3 Current Backing Store is AltCfgTutorial

Select a TCP/IP technology to configure : TCP/IP Profile

Tools

Systems Reusable Configuration Security Reusable Resources Change Sets **Alternate Configuration**

Actions

No filter applied

Alternate Configuration Filter	Description Filter
<input type="radio"/> Local Backup	The system running in a different LPAR on the same CEC
<input type="radio"/> CPC2 Backup	The system running in a different CPC in this data center
<input type="radio"/> DR Primary	Primary LPAR at the DR site
<input type="radio"/> DR Alternate	Alternate LPAR at the DR site

Total: 4 Selected: 0

Home Save

- This new NCA function enables a system administrator to create TCP/IP configuration for an image that can be used in multiple locations
 - With a minimum of changes required between alternates
 - Also manages install of the alternate configurations in their locations
- This new function does not control or manage the actual failover or movement of images
 - It simply primes the alternate locations with configuration, so when the system is restarted in a different location, correct TCP/IP configuration is in place for that location

NCA Alternate Configuration support was delivered on V2R3 in **APAR PI97737**.

Network Configuration Assistant multiple install support: background

Welcome x Network Configu... x

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

Choose a configuration for stack PLEX1.LPAR2.STACK2

List of Alternate Configuration files for stack PLEX1.LPAR2.STACK2

Actions ▾					
	Configuration	Configuration Type	Status	Last Install	Co File
<input type="radio"/>	Base Configuration	TCP/IP Profile	Installed	2019-01-18 12:20:36	'US
<input type="radio"/>	Local Backup	TCP/IP Profile	Never installed	Never	
<input type="radio"/>	CPC2 Backup	TCP/IP Profile	Never installed	Never	
<input type="radio"/>	DR Primary	TCP/IP Profile	Never installed	Never	
<input type="radio"/>	DR Alternate	TCP/IP Profile	Never installed	Never	

Total: 5 Selected: 0

Close Save

NCA can configure and manage multiple configuration files. There are multiple functions where several configuration files can need installation at once including:

- Install all files for a sysplex (TCP/IP) or group (all other technologies)
- Install all alternate configurations for a stack (in TCP/IP only, example screen shot to the left)
- Some of the policy technology installs at the image level result in multiple files
 - For example, IPSEC image install if there are dynamic rules will yield an IKED configuration and a stack configuration

NCA multiple install support: background ...

1

2

3

4

Information

The save to the file system was successful.

OK

Now do it again for another file!

Each file install is a multiple-click process that can get tedious if you have to install multiple files

NCA multiple install support

1

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

Install Multiple Stacks

Install Multiple Stacks

Actions

- Show Configuration File...
- Configure Install...
- Install...
- Install Multiple**
- History

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.tcparms(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.tcparms(stack2a)'



The new “install multiple” action takes you to a panel where you can check the files to be installed, then install them all in one action.

3

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

Install Multiple Stacks

Actions

- Show Configuration File...
- Configure Install...
- Install...**
- History

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

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.tcparms(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.tcparms(stack2a)'

Multiple install support requirements

NCA Multiple Install support was delivered on V2R3 in **APAR PH04130**.

- To be eligible for multiple install a file must:
 - Represent a complete, installable configuration
 - Have installation information, either:
 - Remembered from a previous install of the file, or
 - Configured for use in multiple install

- In order to meet the last requirement above, a new “Configure Install” option was added to all install screens where multiple install is also an option.

**New Function
APAR Summary
Web Pages**

New function APAR summary web pages

- We are now maintaining web pages that provide a summary of the new function APARs available for each release
 - Includes a summary of the function, a link to the APAR, and a link to the function documentation
 - V2R2: <https://www.ibm.com/support/pages/zos-v2r2-communication-server-new-function-apar-summary>
 - V2R3: <https://www.ibm.com/support/pages/zos-v2r3-communication-server-new-function-apar-summary>
 - V2R4: <https://www.ibm.com/support/pages/zos-v2r4-communication-server-new-function-apar-summary>

New function APAR summary web pages - Example



•
•

Scalability and performance enhancement

✦IWQ support for IPSec June 2018

z/OS V2R3 Communications Server, with TCP/IP APAR PI77649, is enhanced to support inbound workload queueing for IPSec workloads for OSA-Express in QDIO mode.

Incompatibilities: This function does not support IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.

- [PI77649](#)
- [How to enable/use this function?](#)

Dependencies:

- This function is limited to OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Statements of Direction

Statement of Direction: Withdrawal of Support for CMIP (Issued February 26, 2019)

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.

Note: IBM has announced that IBM Z NetView V6.3 will be the last release to support the SNA Topology Manager (the main consumer of CMIP data).

Statement of Direction: Withdrawal of ISPF Workstation Agent (Issued February 26, 2019)

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.

Statement of Direction: Removal of native TLS/SSL support from TN3270E Telnet server, FTP server, and DCAS (Issued July 23, 2019)

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 Direction: Removal of policy data import function from the Network Configuration Assistant (Issued July 23, 2019)

z/OS V2.4 will be the last release that the Network Configuration Assistant (NCA) z/OS MF plug-in 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.

Import of TCP/IP profiles into NCA is not affected.

Statement of Direction: Removal of Sysplex Distributor support for workload balancing to IBM DataPower^(R) Gateway products (Issued July 23, 2019)

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.

Miscellaneous Topics

Additional z/OS CS sessions at GSE UK

session: EF: Pervasive Encryption: Get a Grip on Your z/OS Network Encryption with zERT

Tuesday, Nov 5, 2019: 16:45 PM - 17:45 PM

Stowe

Speaker: Jerry Stevens (IBM Corporation)

**session: EG: Introduction to z/OS Container Extensions: Running Linux Docker on Z
Docker Containers inside z/OS**

Wednesday, Nov 6, 2019: 10:15 PM - 11:15 PM

Stowe

Speaker: Jerry Stevens (IBM Corporation)

session: EB z/OS 2.4 CS Technical Update – Repeat of this session

Wednesday, Nov 6, 2019: 13:45 AM - 14:45 AM

Stowe

Speaker: Jerry Stevens (IBM Corporation)

**session: EL: Shared Memory Communications (SMC) with IBM z/OS Communications Server
and Linux on Z**

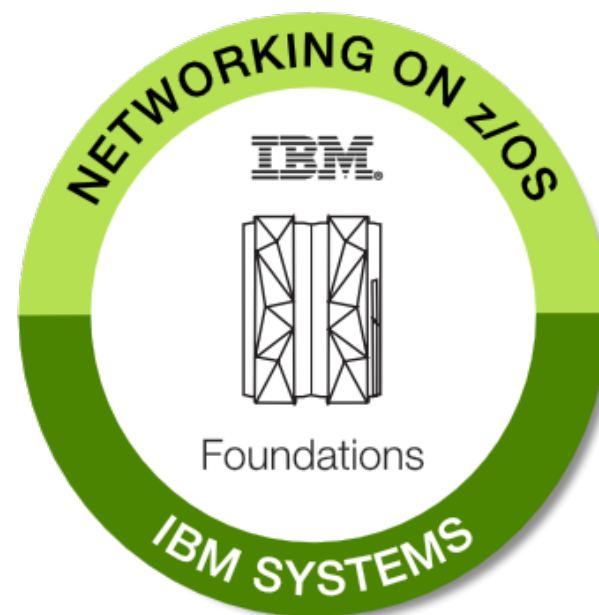
Wednesday, Nov 6, 2019: 16:30 PM - 17:30 AM

Stowe

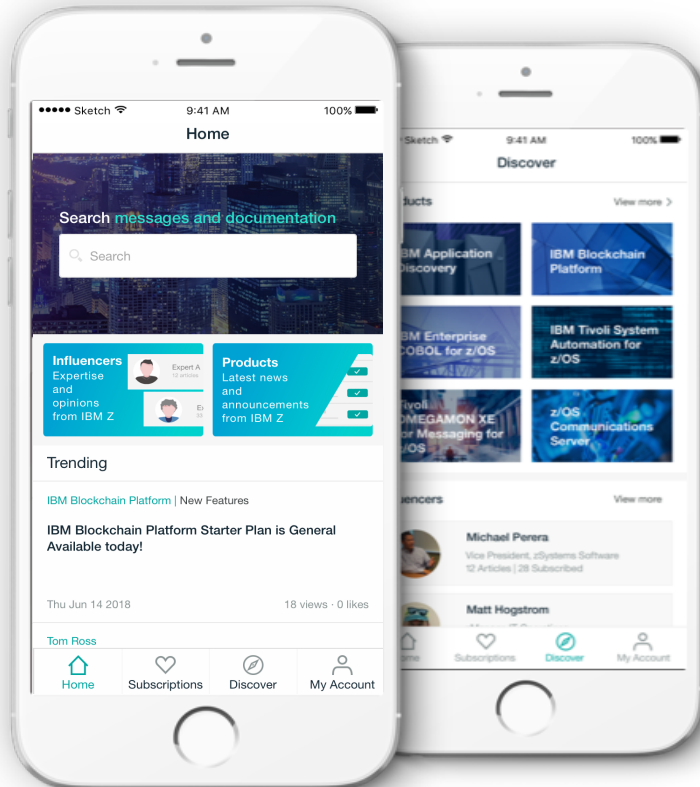
Speaker: Jerry Stevens (IBM Corporation)

IBM Open Badge for Networking on z/OS - Foundations

- To earn the IBM Open Badge for Networking on z/OS Foundations, you need to complete a digital course and pass the final assessment.
- The Networking on z/OS – Foundations course is tailored for novice users of z/OS Communications Server to learn networking on z/OS. After completing this course, you will have foundational understanding of networking on z/OS, including general networking concepts, TCP/IP and SNA communication protocols, network security, and network operations.
- Audience: New technical professional with no or little experience in z/OS Communications Server
- Purpose: Provide foundational knowledge in networking on z/OS that is needed for on-the-job expertise
- Duration: 6 hours and 50 minutes
- IBM Open Badge - Networking on z/OS foundations:
<https://www.youracclaim.com/org/ibm/badge/networking-on-z-os-foundations>
- Networking on z/OS foundations digital course:
<https://www.onlinedigitallearning.com/course/view.php?id=4529>
- Badge final assessment:
<https://www.onlinedigitallearning.com/course/view.php?id=5241>



IBM Doc Buddy – Your one-stop Z mobile content portal



- **Find mainframe documentation in no time**
Integrate mainframe product docs and error messages for 66 products from 141 releases, including z/OS Communications Server
- **Gain insights from best technical and business leaders**
Latest presentations and white papers for important mainframe products and trending IT business insights
- **Share great content to peers**
Connect with your peers via technical content sharing
- **Support 7800+ IBM Z users**
- **Review rating: 4.21/5**



iOS



Android

Notices and disclaimers

- ©2019 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights – use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Appendix

zERT Network Analyzer (zNA) Screenshots

zERT Network Analyzer Overview: Sneak peek: Welcome page and layout

The screenshot shows the IBM zERT Network Analyzer interface. At the top is a dark blue navigation bar with the following items: "IBM zERT Network Analyzer", "Data Management", "Queries", "Report", "Settings", and a "Help" icon. Below the navigation bar is the main content area with the following structure:

- Welcome to IBM zERT Network Analyzer**
Analyze the cryptographic network protection of your z/OS TCP/IP and Enterprise Extender traffic.
- Getting started with IBM zERT Network Analyzer**
 - Configure IBM zERT Network Analyzer**
Configure global settings for IBM zERT Network Analyzer
- Common tasks with IBM zERT Network Analyzer**
 - Import SMF dump data sets**
Define a set of SMF dump data sets that can be scheduled for import into zERT
 - Manage operation history**
View previous data import and prune operations
 - Create, manage, and run queries**
Manage queries

Four callout boxes provide additional information:

- Top-left: "Click here to import SMF dump data sets and to prune old data out of the database" (points to the "Import SMF dump data sets" link).
- Top-middle: "Click here to create, modify, and run queries over the imported data" (points to the "Create, manage, and run queries" link).
- Top-right: "Click here to view the query results (more on this in the following slides)" (points to the "Report" menu item).
- Bottom-right: "Click here to modify application and database settings" (points to the "Settings" menu item).

zERT Network Analyzer Overview: Sneak peek: Report summary view (1 of 2)

TCP Server Traffic: Summary of all the traffic connecting in to servers running on local z/OS systems

TCP Client Traffic: Summary of all the traffic connecting out to servers running on other systems

EE Peer Traffic: Summary of all EE traffic connected to local z/OS systems

Exports the query results and all related details to a comma separated value file

IBM zERT Network Analyzer
Management Queries Report Settings

Report

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 Traffic
TCP Client Traffic
EE Peer Traffic

Export to CSV

Displaying records 1 - 100 out of 5344 Previous Page 1 / 54 Next Page

Sysplex	System	Stack	Server IP	Server Port	User ID	Job Name	Clear Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
LOCAL	MVS202	TCPCS8	10.83.8.2	52030	USER3	USER35	3	0	0	0
LOCAL	MVS202	TCPCS8	10.84.8.1	52030	USER3	USER35	0	3	0	0
PLEX1	GERMANY	TCPSVT	0:0:0:0:0:0:0:1	50000	IBMUSER	DMP50000	22	0	0	0
PLEX1	GERMANY	TCPSVT	127.0.0.1	1024	DAEMON	OMPROUTE	1	0	0	0
PLEX1	GERMANY	TCPSVT	127.0.0.1	50000	IBMUSER	DMP50000	21	0	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	20	*FTPUSR*	FTPUNIX	26	171	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	21	DAEMON	FTPUNIX1	4	22	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	23	OMVSKERN	INETD001	2	0	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	80	SVTWSRV	WEBSERV1	5,994	0	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	175	IBMUSER	JES2S001	1	0	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	512	IBMUSER	REXECD	0	0	0	10
PLEX1	GERMANY	TCPSVT	197.11.105.1	620	*FTPUSR*	FTPANON	549	0	0	0
PLEX1	GERMANY	TCPSVT	197.11.105.1	621	IBMUSER	FTPANON1	550	0	0	0

Each row summarizes traffic for one server (TCP) or local peer (EE)

zERT Network Analyzer Overview: Sneak peek: Report summary view (2 of 2)

Report

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 Traffic | TCP Client Traffic | EE Peer Traffic

COLUMN OPTIONS

- Endpoint Attributes**
 - Sysplex
 - System
 - Stack
 - Server IP
 - Server Port
 - User ID
 - Job Name
- Segments In**
 - Clear Segments In
 - IPsec Segments In
 - SSH Segments In
 - TLS Segments In
- Total Connections**
 - Clear Total Connections
 - IPsec Total Connections
 - SSH Total Connections
 - TLS Total Connections
- Segments Out**
 - Clear Segments Out
 - IPsec Segments Out
 - SSH Segments Out
 - TLS Segments Out
- Partial Connections**
 - Clear Partial Connections
 - IPsec Partial Connections
 - SSH Partial Connections
 - TLS Partial Connections
- Bytes In**
 - Clear Bytes In
 - IPsec Bytes In
 - SSH Bytes In
 - TLS Bytes In
- Bytes Out**
 - Clear Bytes Out
 - IPsec Bytes Out
 - SSH Bytes Out
 - TLS Bytes Out

Export to CSV

Displaying records 1 - 100 out of 5344 | Previous Page 1 / 54 | Next Page

Sysplex	System	Stack	Server IP	Server Port	User ID	Job Name	Clear Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
LOCAL	MVS202	TCPCS8	10.83.8.2	52030	USER3	USER35	3	0	0	0
LOCAL	MVS202	TCPCS8	10.84.8.1	52030	USER3	USER35	0	3	0	0

zERT Network Analyzer Overview: Sneak peek: Client detail view for a given server

Report

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 Traffic | TCP Client Traffic | EE Peer Traffic

Showing records 1 - 100 out of 5344 | Previous Page 1 / 54 | Next Page

Client IP	Stack	Server IP	Clear Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
197.11.105.1	TCPSVT	197.11.105.1	3	0	0	0
197.11.105.1	TCPSVT	197.11.105.1	0	0	0	979
197.11.105.1	TCPSVT	197.11.105.1	0	0	0	769
197.11.105.1	TCPSVT	197.11.105.1	2,313	0	0	979
197.11.105.1	TCPSVT	197.11.105.1	486	0	0	1,161

CLIENT DETAILS FOR SERVER 197.11.105.1: 2221

Client IP	Clear Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
<input type="checkbox"/> 197.2.107.1	0	0	0	117
<input checked="" type="checkbox"/> 197.23.123.1	0	0	0	562
<input type="checkbox"/> 197.26.126.1	486	0	0	482

Displaying records 1 - 3 out of 3 | Previous Page | Next Page

[View security session details \(1\)](#)

zERT Network Analyzer Overview: Sneak peek: Security session details view

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

Report | Export to CSV

00 out of 5344 | Previous Page 1 / 54 | Next Page

Clear Total Conns | IPsec Total Conns | SSH Total Conns | TLS Total Conns

Sysplex	System	Stack	Server IP	User ID	Job Name	Clear Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERM	TCPSVT	197.11.105.1	IBMUSER	FTPATTA1	486	0	0	1,161

SECURITY SESSION DETAILS FOR SERVER 197.11.105.1:2

TLS Session Details | Certificate Details | View client details

COLUMN OPTIONS

TLS Cryptographic Details

- Client IP
- Session ID
- Protocol Version
- Negotiated Cipher
- Key Exchange Algorithm
- Symmetric Encryption Algorithm
- Message Authentication Algorithm
- ETM
- Source

COLUMN OPTIONS

TLS Certificate Details

- Client IP
- Session ID
- Server Certificate Signature Method
- Server Certificate Asymmetric Encryption Algorithm
- Server Certificate Digest Algorithm
- Server Certificate Key Length
- Server Certificate Key Type
- Client Certificate Signature Method
- Client Certificate Asymmetric Encryption Algorithm
- Client Certificate Digest Algorithm
- Client Certificate Key Length
- Client Certificate Key Type

TLS Session Details | Distinguished Name Details

COLUMN OPTIONS

TLS Distinguished Name Details

- Client IP
- Session ID
- Server Certificate Issuer Distinguished Name
- Server Certificate Subject Distinguished Name
- Client Certificate Issuer Distinguished Name
- Client Certificate Subject Distinguished Name

Client IP	Protocol Version	Negotiated Cipher	Key Exchange Alg	Symm Encryption Alg	Message Auth Alg
197.23.123.1	TLSv1.1	0035	RSA	AES CBC 256	HMAC-SHA1

PLEX1 | GERMANY | TCPSVT | 197.11.105.1 | 9000 | IBMUSER | MAPSRV1 | 15 | 0 | 0 | 0

zERT Network Analyzer Overview: Sneak peek: TCP Client Traffic report

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

Report
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 - 78 out of 78 | Previous Page 1 / 1 | Next Page

Client Sysplex	Client System	Client Stack	Foreign Server IP	Foreign Server Port	Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	2000:197:2:187:0:0:b	50006	0	8	0	0
PLEX1	GERMANY	TCPSVT	197.2.187.11	50006	0	7	0	0
LOCAL	MVS202	TCPCS2	10.84.8.1	52030	5	5	0	0

Click on a foreign server row to expand the list of all the local clients

CLIENT DETAILS FOR FOREIGN SERVER 10.84.8.1: 52030 ⓘ [View security session details](#)

<input type="checkbox"/> Client IP	<input type="checkbox"/> Job Name	<input type="checkbox"/> User ID	Clear Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
<input type="checkbox"/> 10.84.2.1	USER23	USER2	1	1	0	0
<input type="checkbox"/> 10.84.2.1	USER24	USER2	1	1	0	0
<input type="checkbox"/> 10.84.2.1	USER25	USER2	1	1	0	0
<input type="checkbox"/> 10.84.2.1	USER26	USER2	1	1	0	0
<input type="checkbox"/> 10.84.2.1	USER27	USER2	1	1	0	0

Client details include the job name and user ID of each local client

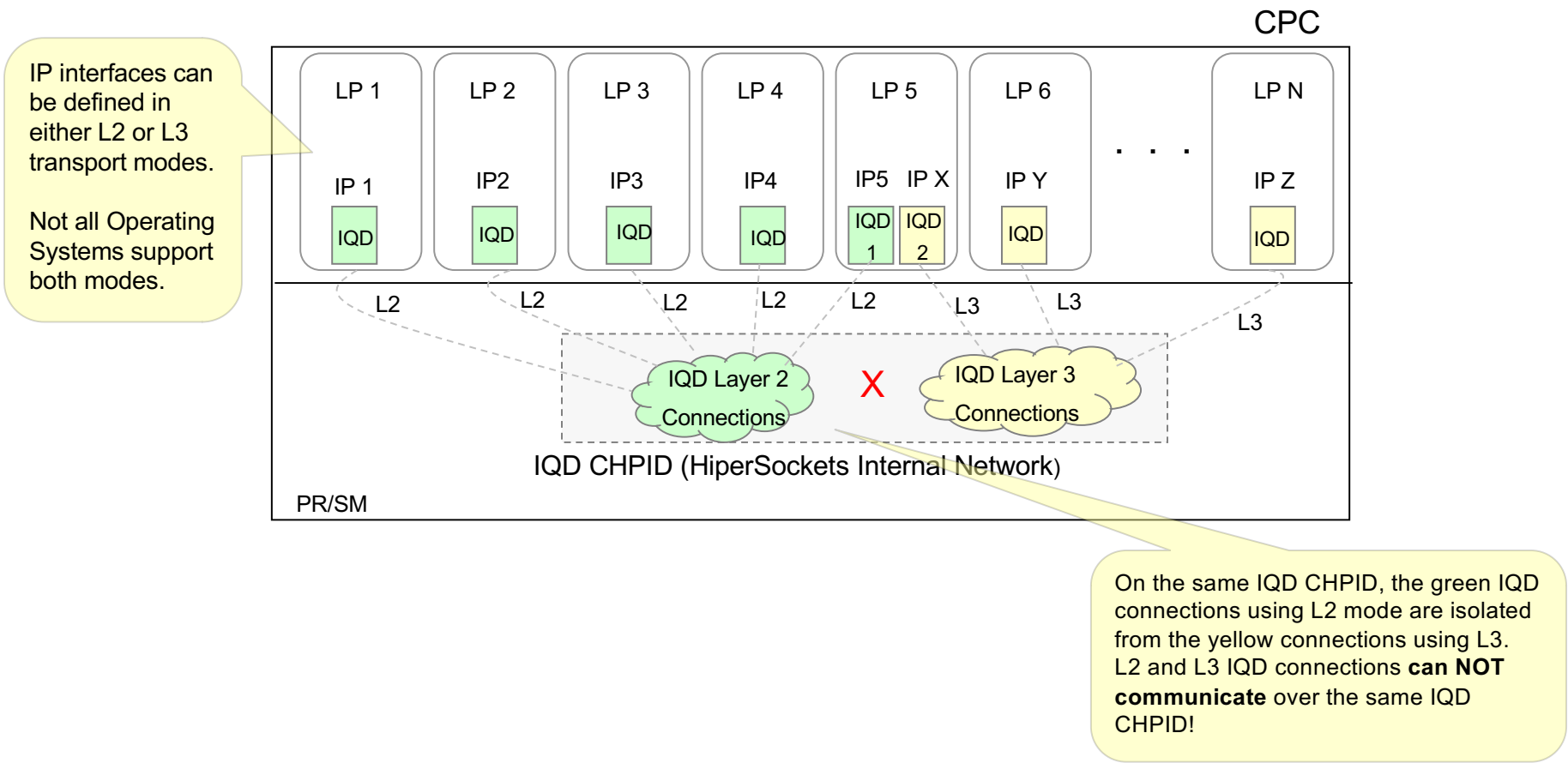
PLEX1	GERMANY	TCPSVT	0:0:0:0:0:0:1	50000	12	0	0	0
PLEX1	GERMANY	TCPSVT	127.0.0.1	1924	1	0	0	0
PLEX1	GERMANY	TCPSVT	127.0.0.1	50000	13	0	0	0

HiperSockets Converged Interface(HSCI) (Additional Detail)

System z HiperSockets Connectivity Background / Problem

- System z Operating Systems can connect to HS using 2 modes:
 - Layer 3 mode (IP address routing) or
 - Layer 2 mode (MAC routing)
- In order to communicate over HiperSockets, Operating Systems must use the same mode (note. OSA can bridge L2 to L3 hosts sharing the same OSA)
- z/OS only supports L3 mode, Linux supports both modes.

System z IQD Architecture: HiperSockets Mixing Layer 2 and Layer 3 Modes



LPARs using HiperSockets in Layer 2 mode **can not** communicate with LPARs in Layer 3 mode.

Problem Statement

There are two main issues:

1. z/VM Bridge, SSI and LGR and Linux (Layer 2) Incompatibility:

The z/VM Bridge support provides a very competitive and seamless solution for the overall System z networking landscape for Linux on z clients. There are many advantages (e.g. allows single IP interface per Linux guest) to the z/VM bridge model and enables Live Guest Relocation in a z/VM SSI environment

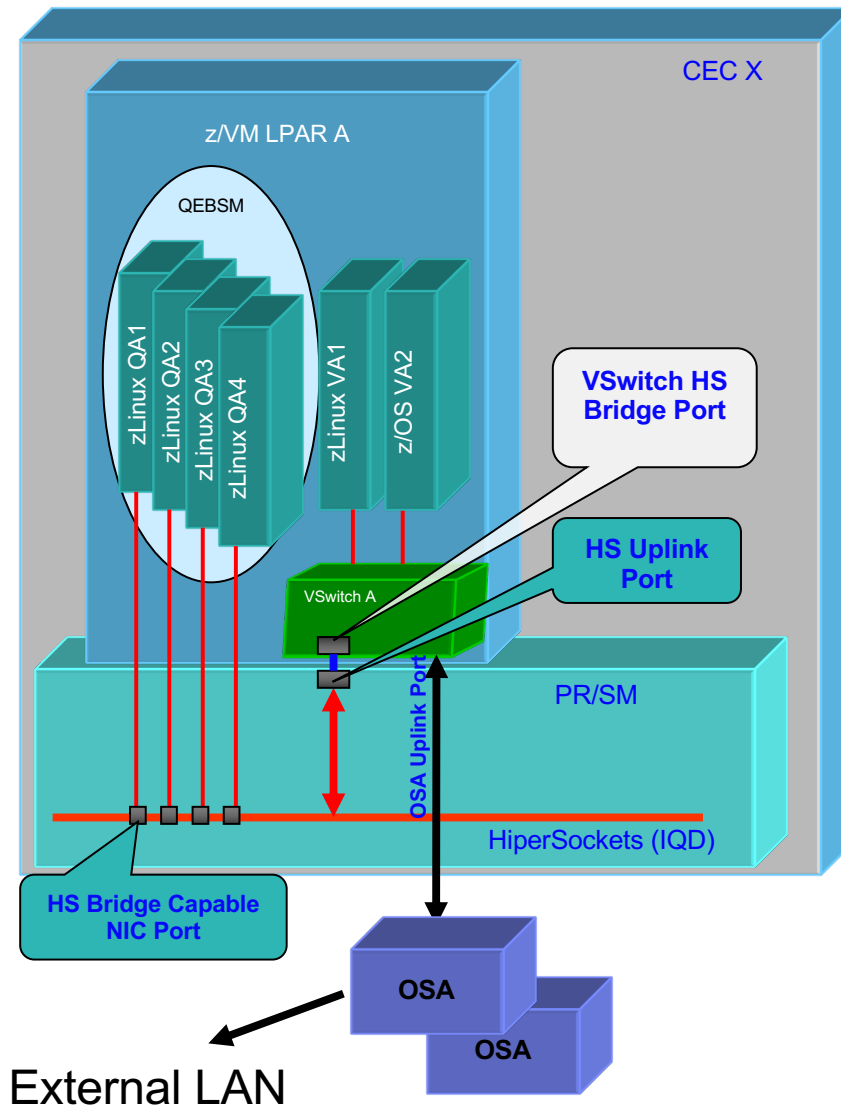
However, z/OS does not support (L2) connectivity to Linux in this configuration.

The missing z/OS support creates a gap in the overall value of the z System solution (Layer 2 Linux compatibility, HS, z/VM Bridge, VSwitch etc.)

2. z/OS HiperSockets usability:

When moving a z/OS instance to another CPC, it requires manual administrative actions to reconfigure the HS interfaces to match the new IP subnet(s) on the new CPC. This applies to all z/OS environments (even in z/OS only environments). Some customers regularly / frequently move their z/OS instances. Customers have expressed concerns about this issue (i.e. how this manual step impacts their day to day operations causing some customers to rethink or stop using HS).

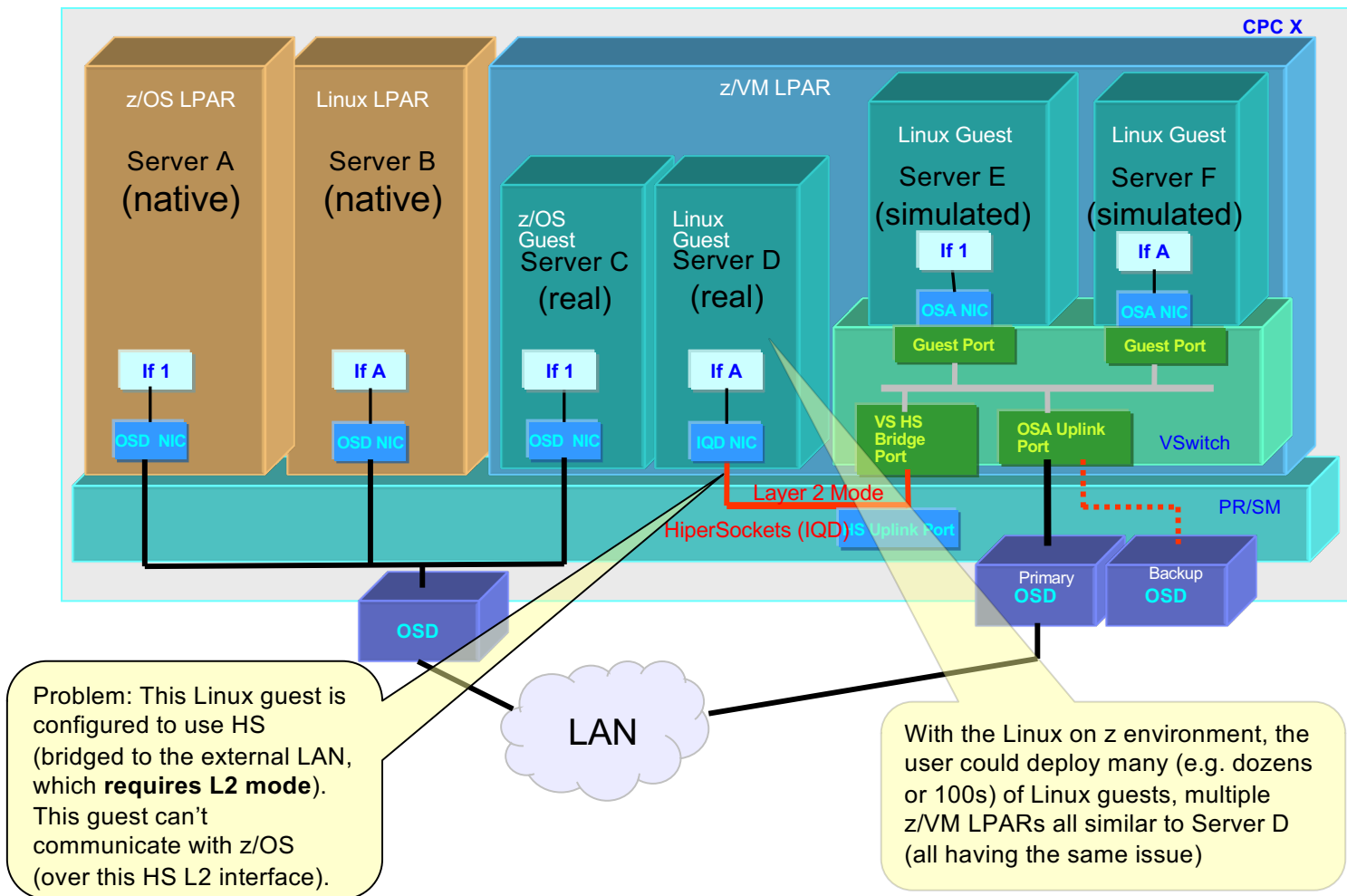
z/VM VSwitch HS Bridge Overview



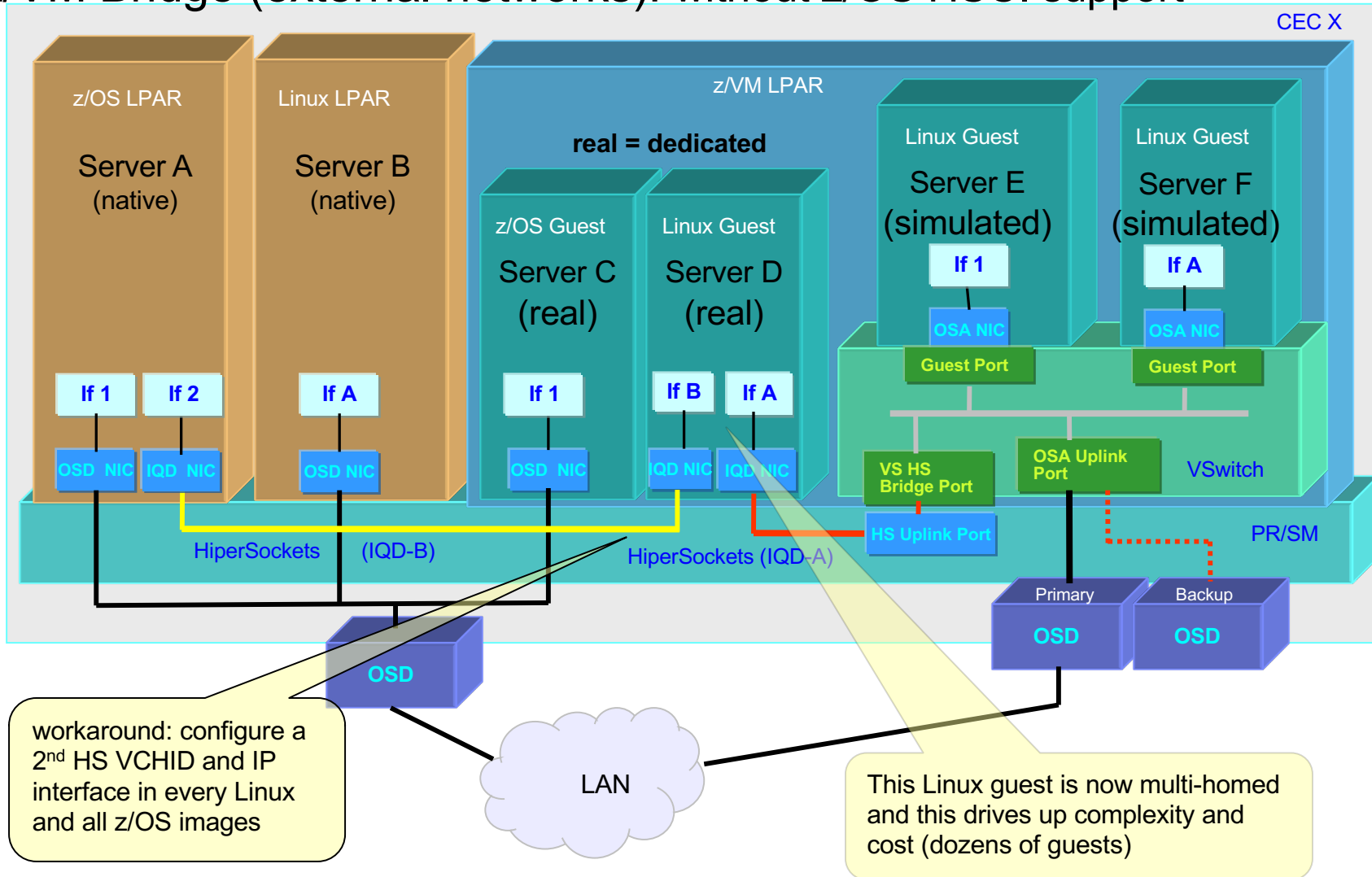
- The z/VM VSwitch and HS **must be operating in the L2 transport mode (i.e. the Bridge requires L2)**
- No transport mode conversions
- Guests QA1, QA2, QA3 and QA4 have real (*dedicated*) QEBSM connections to HS PCHID.
 - Optimum performance configuration requiring almost no z/VM involvement
 - Bridged by default when using QDIO Assist (QEBSM, which provides connectivity to both HS and the external LAN segments)
- Guests VA1 and VA2 have virtual (NIC) connections through VSwitch A
 - Optimum performance config for guests that are not deployed with QEBSM on z/VM. Eliminates “shadow” queue overhead
 - Connectivity to HS and external LAN segments
- OSA uplink port BAU no changes in current support

z/VM VSwitch Bridge Issue: z/OS and Linux HS L2

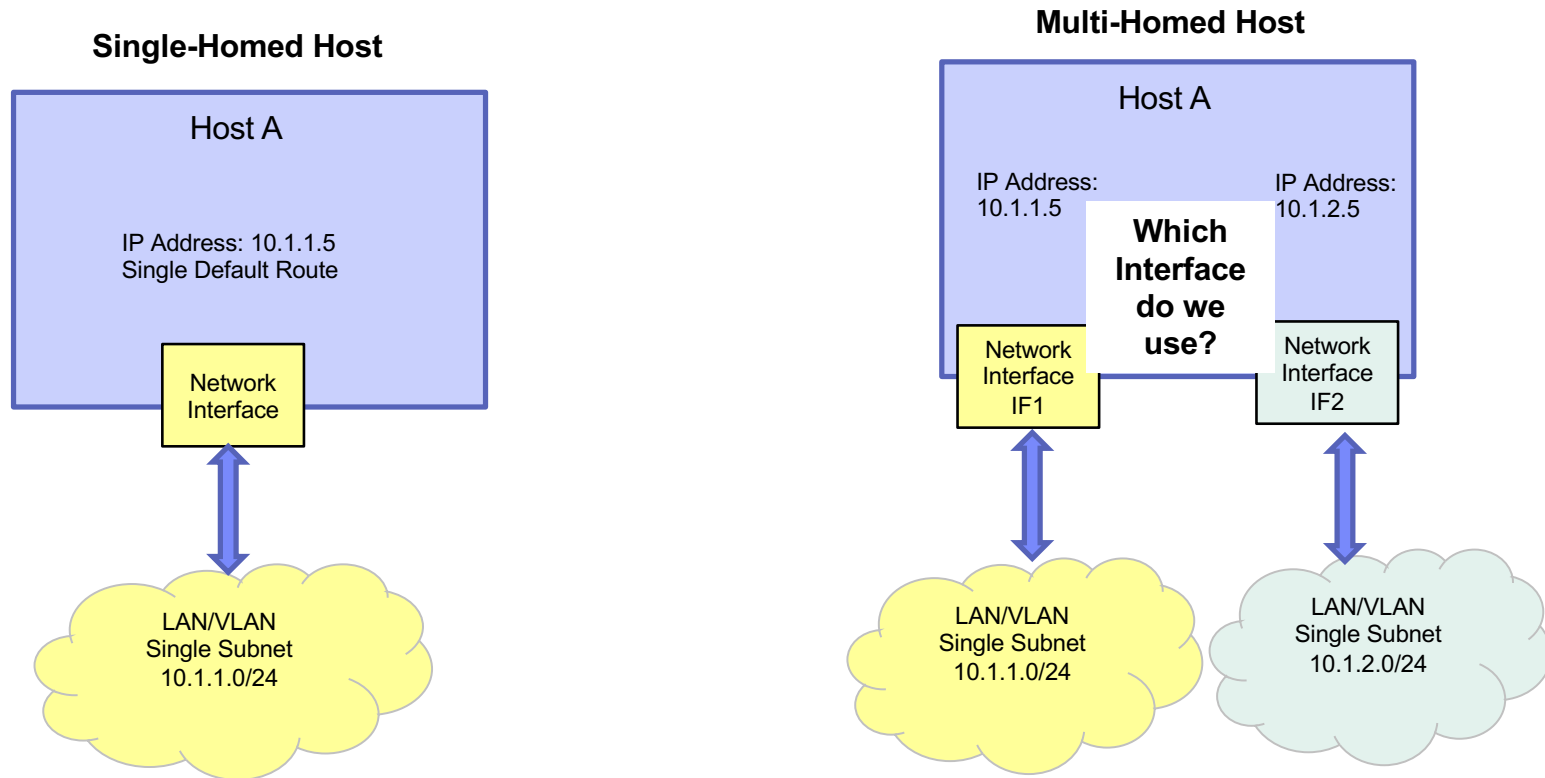
Focus on Server D!



z/VM Bridge (external networks): without z/OS HSCI support



High level review – Single-homed vs Multi-homed hosts

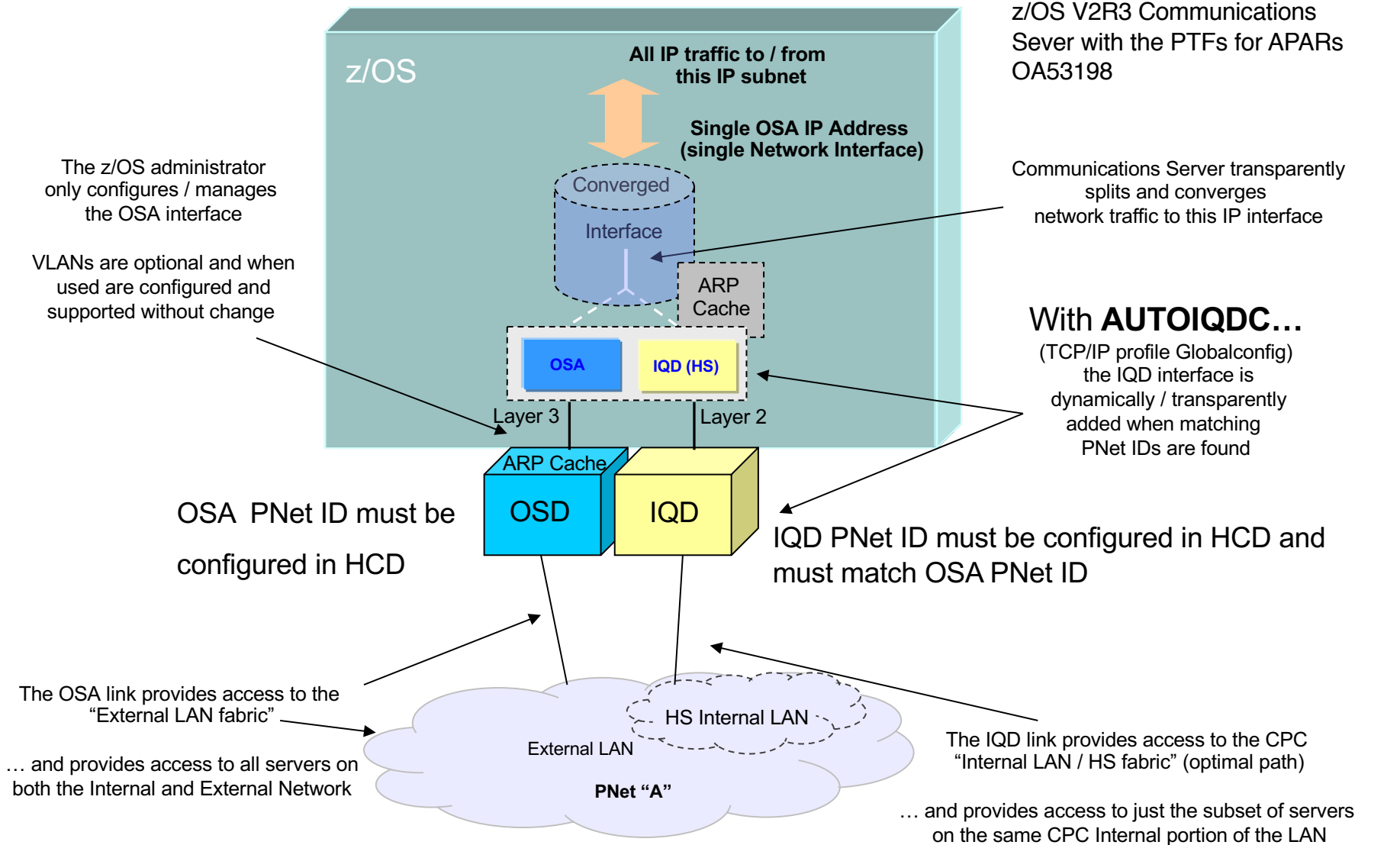


Which Interface do we use for outbound traffic?
 Which interface is used for inbound traffic?
 What network route entries are needed?
 What if an interface fails?
 Can I transparently fall over to the alternate interface?



z/OS HiperSockets Converged Interface (HSCI)

HiperSockets Converged Interface (HSCI) support is provided on z/OS V2R3 Communications Server with the PTFs for APARs OA53198



Communications Server transparently splits and converges network traffic to this IP interface

With AUTOIQDC...
(TCP/IP profile Globalconfig) the IQD interface is dynamically / transparently added when matching PNet IDs are found

The z/OS administrator only configures / manages the OSA interface

VLANs are optional and when used are configured and supported without change

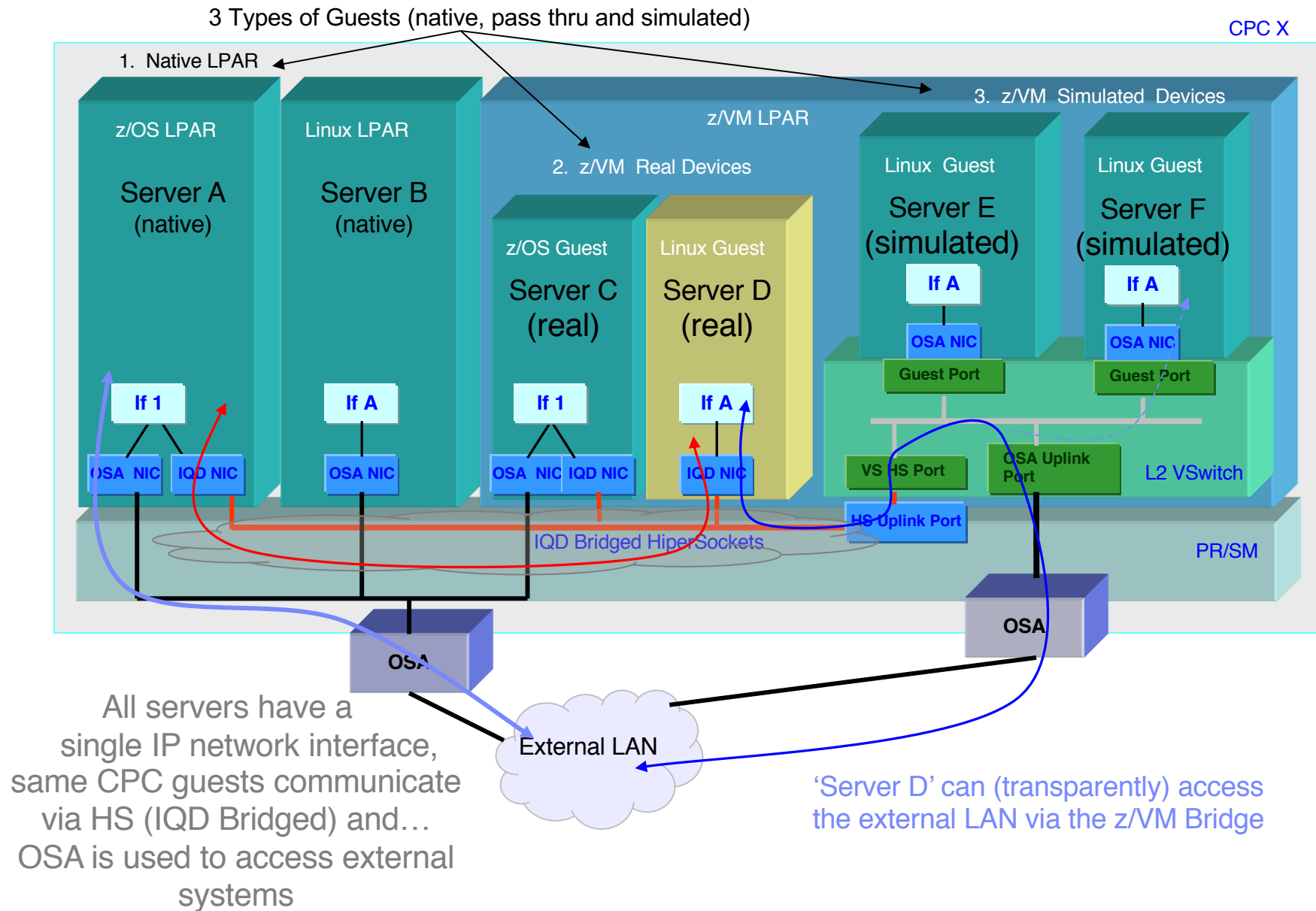
OSA PNet ID must be configured in HCD

IQD PNet ID must be configured in HCD and must match OSA PNet ID

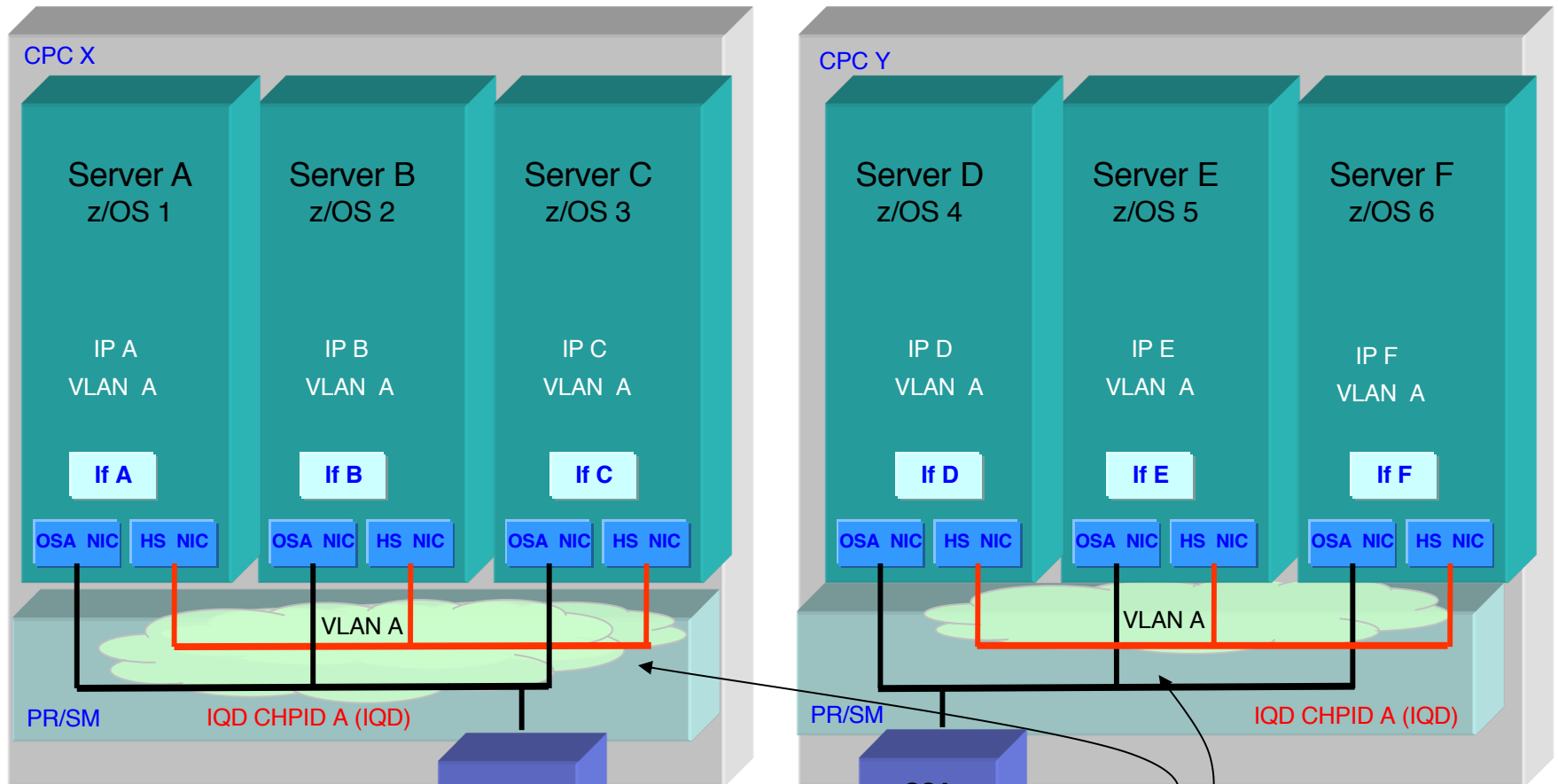
The OSA link provides access to the "External LAN fabric" ... and provides access to all servers on both the Internal and External Network

The IQD link provides access to the CPC "Internal LAN / HS fabric" (optimal path) ... and provides access to just the subset of servers on the same CPC Internal portion of the LAN

z/OS Converged HS and z/VM Bridge



z/OS only Configurations (single IP interface)

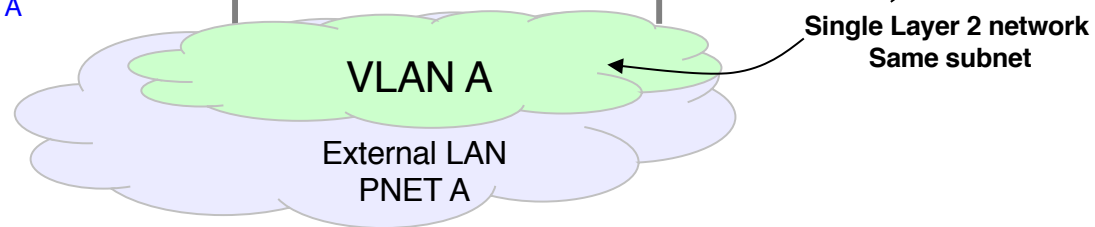


Each z/OS image has a single network...

PNet A

... single IP route, IP Address & VLAN...

the system has 2 networks



Sysplex Notification of TCP/IP Stack Join or Leave

(Additional Detail)

Sysplex autonomics: ENF signal mapping

- ENF signal mapping:

Mapping macro for z/OS Communications Server ENF event code 80					
Offset Dec	Offset Hex	Type	Len	Name (Dim)	Description
0	0	STRUCTURE	0	ENF80_SYSPLEX	SYSPLEX Event Data - Based on ENF80_END
0	0	BITSTRING	0	ENF80_SYSPLEX_FLAGS	SYSPLEX Flags
		1... ..		ENF80_SYSPLEX_JOIN	The TCP/IP stack is joining the sysplex group
		.1.. ..		ENF80_SYSPLEX_LEAVE	The TCP/IP stack is leaving the sysplex group
		..11 1111		*	Reserved
1	1	BITSTRING	3	ENF80_SYSPLEX_RSVD1	Reserved
4	4	CHARACTER	8	ENF80_TCPIP_JOBNAME	TCPIP job name

Sysplex autonomics: Exploitation

- In order to utilize this new signal, a listener must be coded:
 - Use the ENFREQ macro and specify the following:
 - Action (LISTEN)
 - Code (80)
 - Qualifier ('40000000'X)
 - Exit () – This field points to the intended exit routine

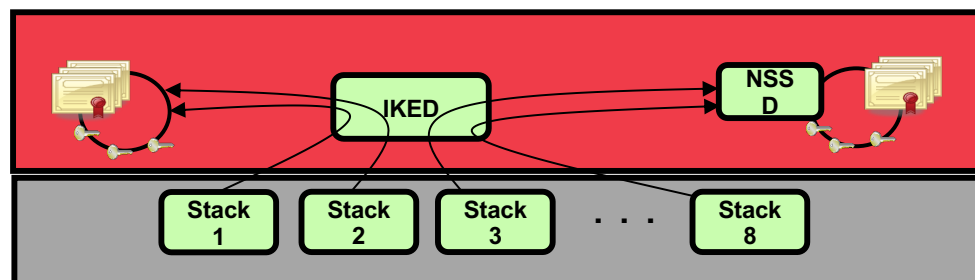
Sysplex Autonomics

for IPSec

(Additional Detail)

IKED autonomics: Background

IKED / NSSD digital certificate processing during IKE negotiations



- IKED manages IPsec negotiations for all stacks on an LPAR
- For IKEv1, IKED can be configured (on a per-stack basis) to do its own certificate-based digital signature operations
- For IKEv2 (and optionally IKEv1), IKED is configured (per stack) to delegate certificate-based signature operations to NSSD for that stack
- IKED maintains a separate connection to NSSD for each stack for which it is configured for NSSD services
- The IKED – NSSD connection must be protected by AT-TLS

IKED autonomics: Problem statement

- An IKED that is incapable of negotiating SWSA Security Associations impacts the sysplex
 - For customers that have significant IPsec-protected sysplex workloads, the IPsec components are an essential requirement (critical resource) in the health of the TCP/IP stack. For example, if for some reason IKED is not available, it can impact the ability to send traffic for the sysplex distributor workload.
- Some conditions that can cause IKED to become unable to negotiate with peers
 - IKED can't get a connection to NSSD when configured to do so
 - IKED cannot build its own certificate cache
 - IKED can't load KeyExchange policy
 - NSSD cannot build its certificate cache
 - IPSec certificate services are not enabled or the IKED client is not permitted to use those certificate services.

IKED autonomics: Monitor key IPsec components

- Sysplex Autonomics function extended to monitor the health of the IPsec components
- The following conditions are monitored:
 - IPsec policy loaded successfully in the stack
 - IKED active
 - IKED successfully built its certificate cache, if IKED providing certificate services for the stack
 - IKED successfully connects to Policy Agent and loads policy
 - IKED connected to NSSD, if NSSD providing certificate services for the stack
 - NSSD successfully built its certificate cache, if NSSD providing certificate services for the stack

z14 Network Interface Updates

New IBM z14 GA1 – Network Interface Updates



■ OSA-Express6S

- Technology Refresh
- Supported on all existing supported releases
 - APAR PI75733 (z/OS V2R1 and z/OS V2R2 - updates the output of D OSA,INFO command when using OSA-Express6S)

■ RoCE Express2 10GbE

- Technology Refresh
- Can be shared across 63 Virtual Functions (VFs) per physical port – earlier version supported 31 VFs
- Requires the following APARs on prior releases:
 - V2R1: OA51949 / PI75199
 - V2R2: OA51950 / PI75200

■ OSA-Express6S features:

- OSA-Express6S 10 Gigabit Ethernet (GbE) Long Reach (LR)
- OSA-Express6S 10 Gigabit Ethernet (GbE) Short Reach (SR)
- OSA-Express6S Gigabit Ethernet Long Wavelength (GbE LX)
- OSA-Express6S Gigabit Ethernet Short Wavelength (GbE SX)
- OSA-Express6S 1000BASE-T Ethernet

New IBM z14 GA2 – Network Interface Updates – Support for 25 GbE

- RoCE Express2 25GbE
 - Support for 25GbE bandwidth
 - No z/OS software changes

- OSA-Express7S 25GbE
 - OSA-Express7S 25GbE Short Reach (SR) - feature #0429
 - General Availability: April 9, 2019
 - APARs AO55256 and PI95703 are required.

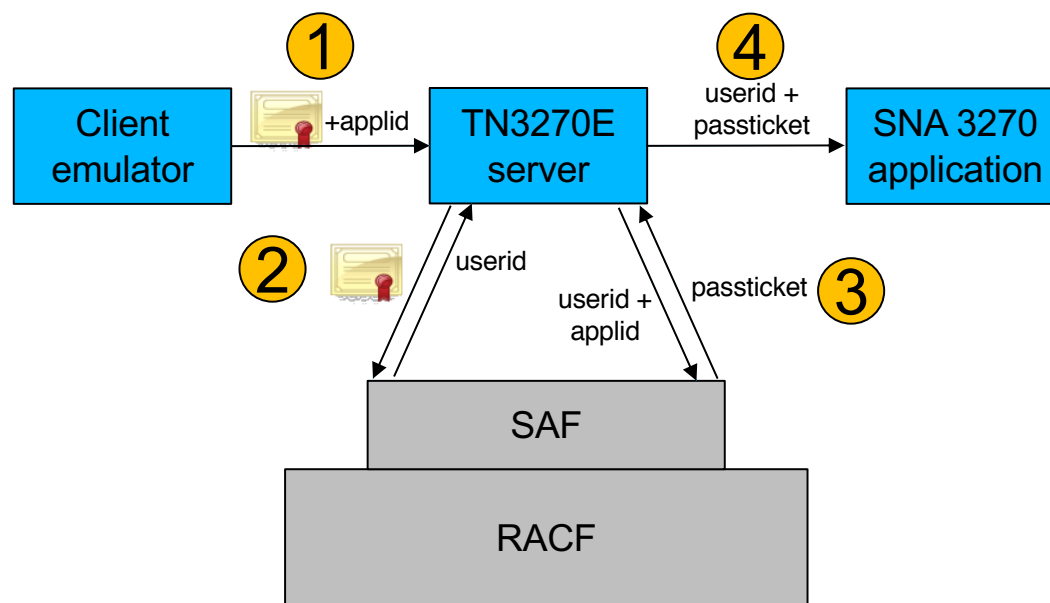


Note. OSA and RoCE 25GbE both require 25GbE Ethernet switch support (bandwidth / speed is **not** auto-negotiated).

**TN3270 Express Logon
Feature (ELF) support for
z/OS Multi-Factor
Authentication (MFA)**

Background: TN3270E Telnet server Express Logon Feature

- The TN3270E Express Logon Feature (ELF) provides a single sign-on capability to z/OS 3270 applications using SAF passtickets
 - A passticket is a one-time use password value that is generated by a SAF compliant security manager like RACF
 - Terminal emulators must be enabled for ELF to use it
- Here's how it works:



Background: z/OS Multi-Factor Authentication

- 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
- Authentication factors:
 - Something you know (password, PIN code, etc.)
 - Something you have (smart card, cryptographic key, etc.)
 - Something you are (fingerprint or other biometric data)
- Prior to MFA, z/OS users could authenticate with:
 - Password
 - Password phrase
 - Passticket
 - Digital certificate
 - Kerberos
- Customers not only needed to use multiple authentication factors, but also needed to use factors that were not supported natively by z/OS
- Multi-factor Authentication (MFA) for z/OS
 - Supports a variety of authentication methods
 - Some through inline flows and others through out-of-band flows
 - List of authentication methods continues to grow

Background: z/OS Multi-Factor Authentication ...

- A specific MFA use case involved the use of smart cards that contain a user's personal certificate and private key
- The user inserts his/her smart card into a reader attached to his/her device
- In order to proceed, the user must enter a PIN code to prove that the card belongs to him/her. This is one authentication factor.
- Next, the client establishes a TLS-protected connection to an MFA authentication server. The X.509 certificate on the smart card is used as the TLS client. In this case, the private key on the card acts as the second authentication factor.
- Once the TLS handshake completes, MFA picks certain components out of the certificate and compares those to what is stored in the user's RACF User profile. A match proves that the certificate is registered to the user and causes MFA to generate a Cache Token Credential which is saved to a sysplex aware cache and is then returned to the client
- The user types that CTC in the password field of a logon dialogue

Background: Customer requirement

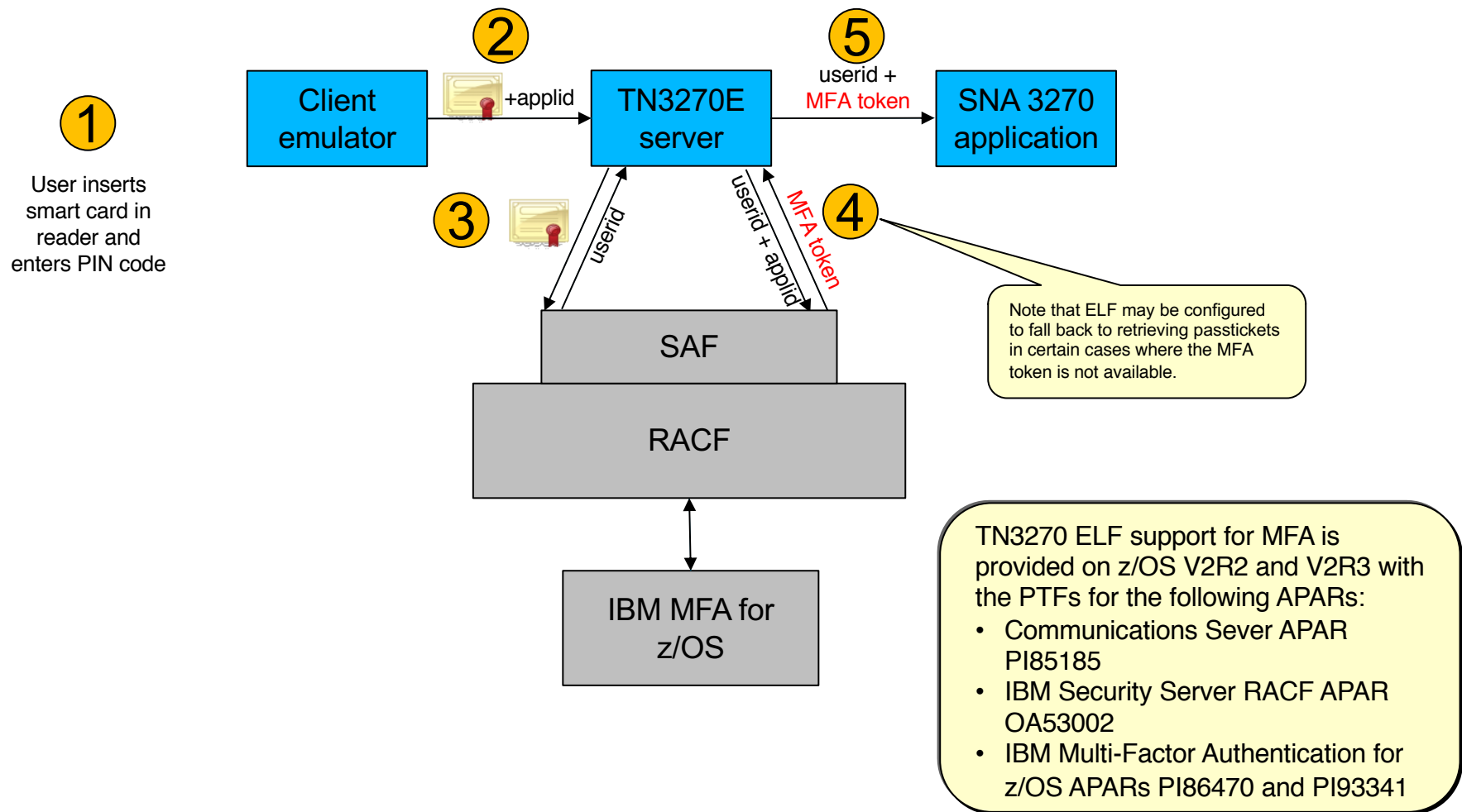
- Customers wanted to use the multiple authentication factors provided by smart cards while retaining the single logon characteristics of the Express Logon Feature.
- IBM Multi-Factor Authentication for z/OS already supported the use of these smart cards using a set of out-of-band flows, but there was no integration with ELF to use the resulting MFA tokens.

TN3270 ELF support for MFA

- When EXPRESSLOGONMFA is enabled in the TN3270 profile, ELF will retrieve an MFA token from SAF using a new R_Factor service (using a new opcode) instead of a passticket as used under EXPRESSLOGON. The new R_Factor function:
 - Takes a userid and APPLID as input
 - Returns an MFA token as long as the userid's SAF profile allows it and the checks based on the user's certificate are successful
- No changes required to ELF-enabled 3270 emulators for solutions that ultimately rely on TLS client authentication (for example, smart cards that contain the user's personal client certificate)
- A TN3270E Telnet server configuration parameter controls whether the existing passticket only function or the new MFA function will be used for ELF. Also provides the option to use MFA and fall back to passtickets where it makes sense.
- RACF updated with the new R_Factor function

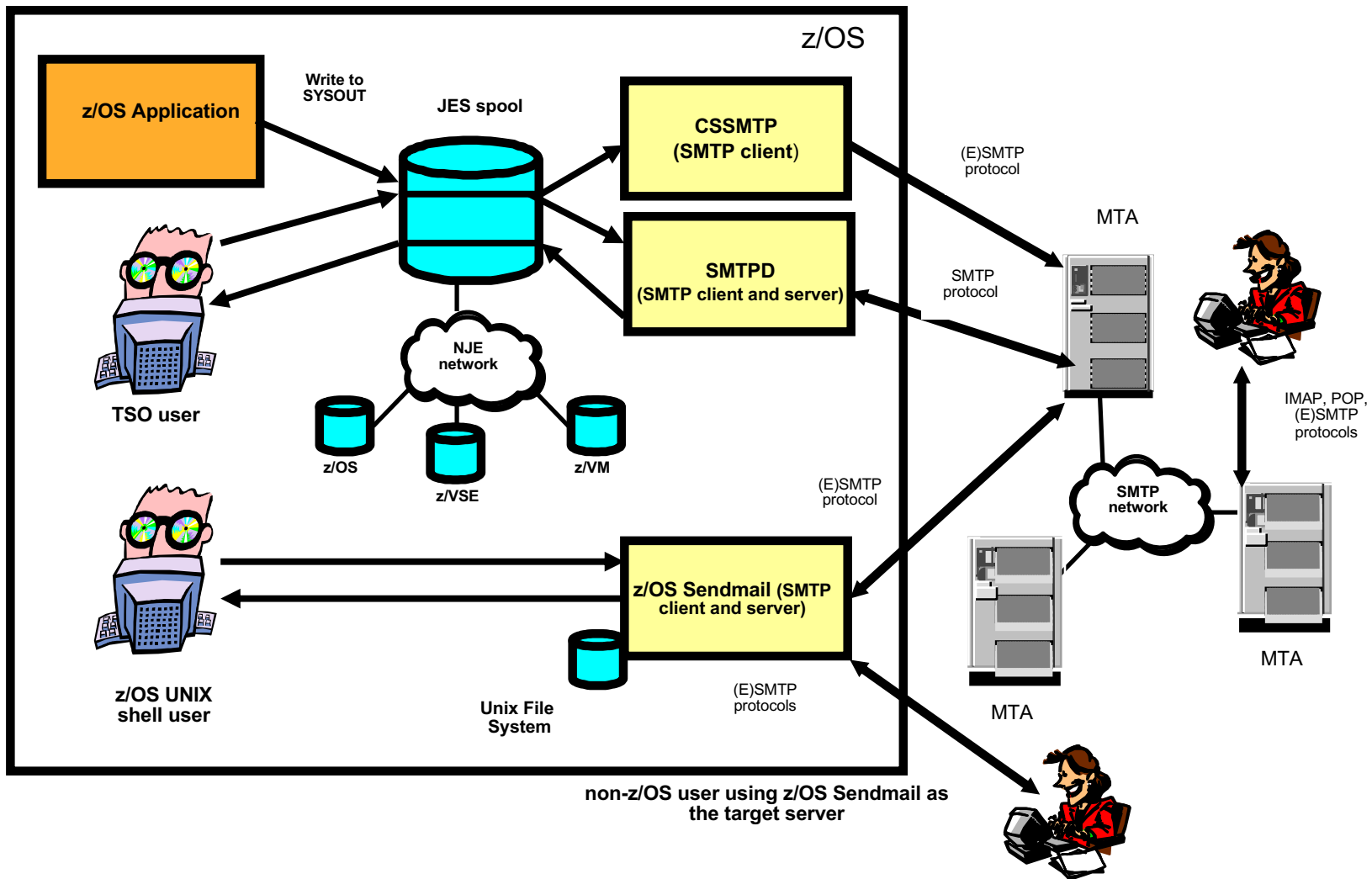
TN3270 ELF support for MFA ...

Here's how it works:

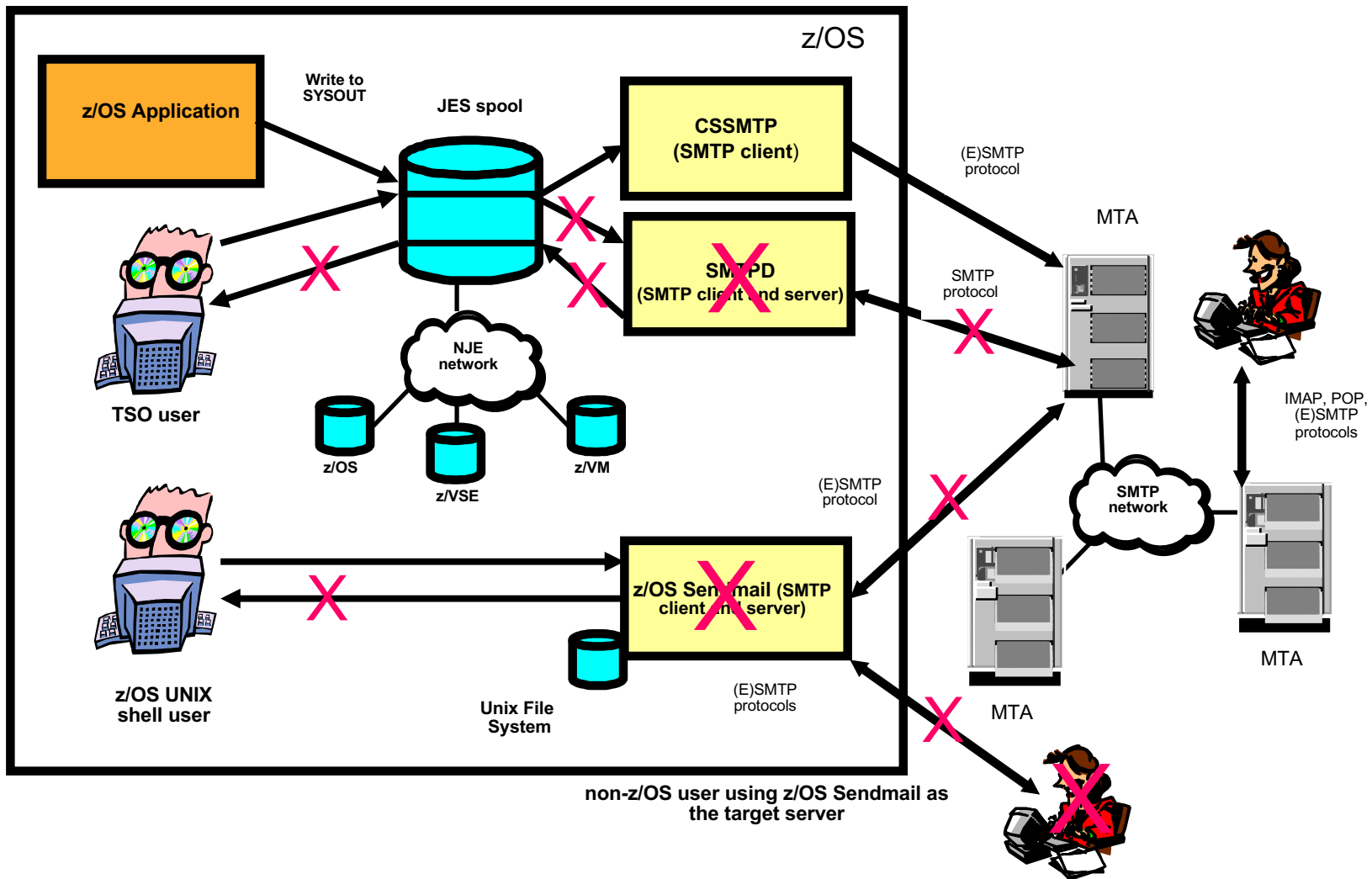


z/OS Mail Updates

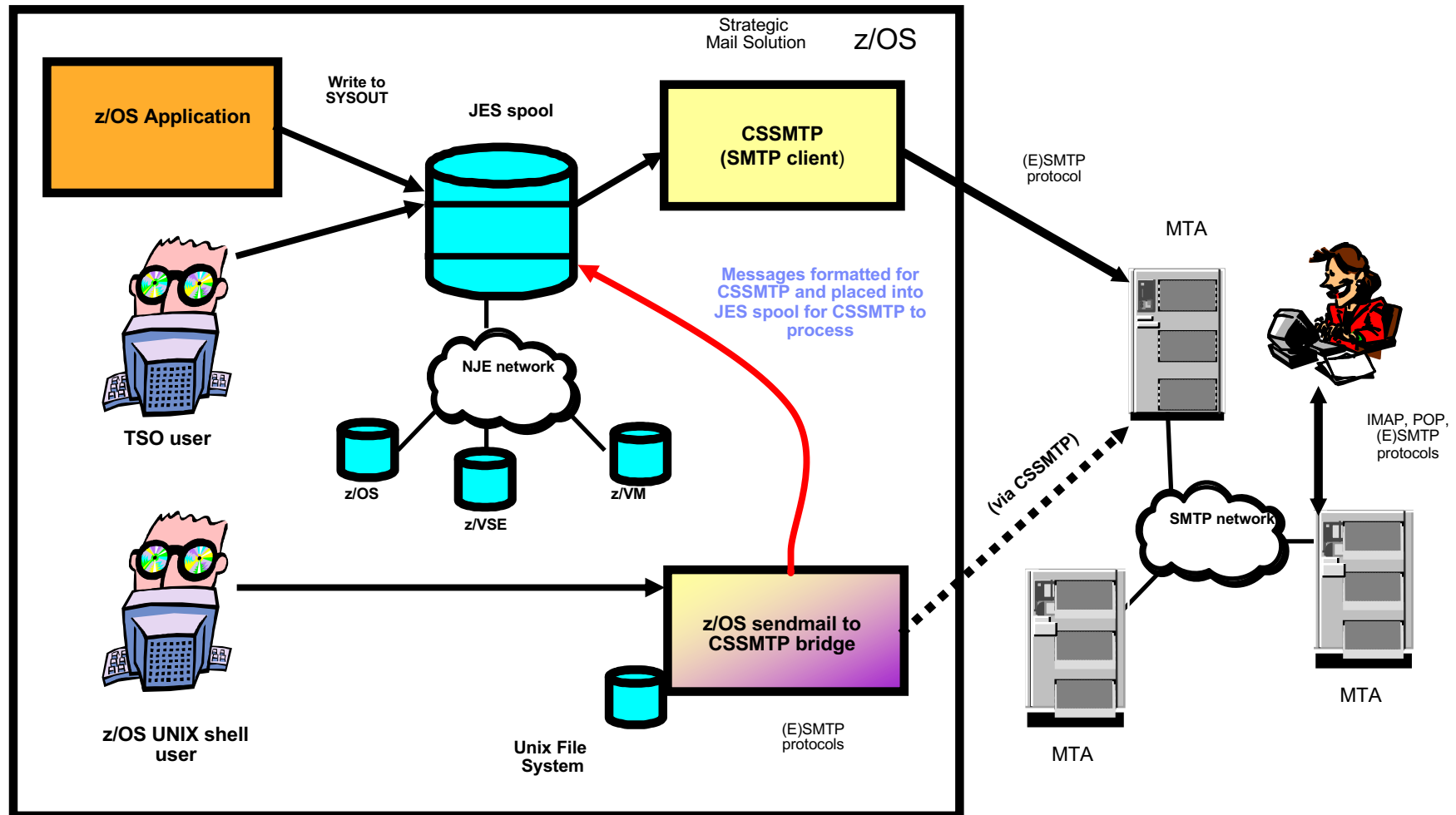
Mail components supported in z/OS V2R2



Mail component changes in z/OS V2R3



Mail components in z/OS V2R3

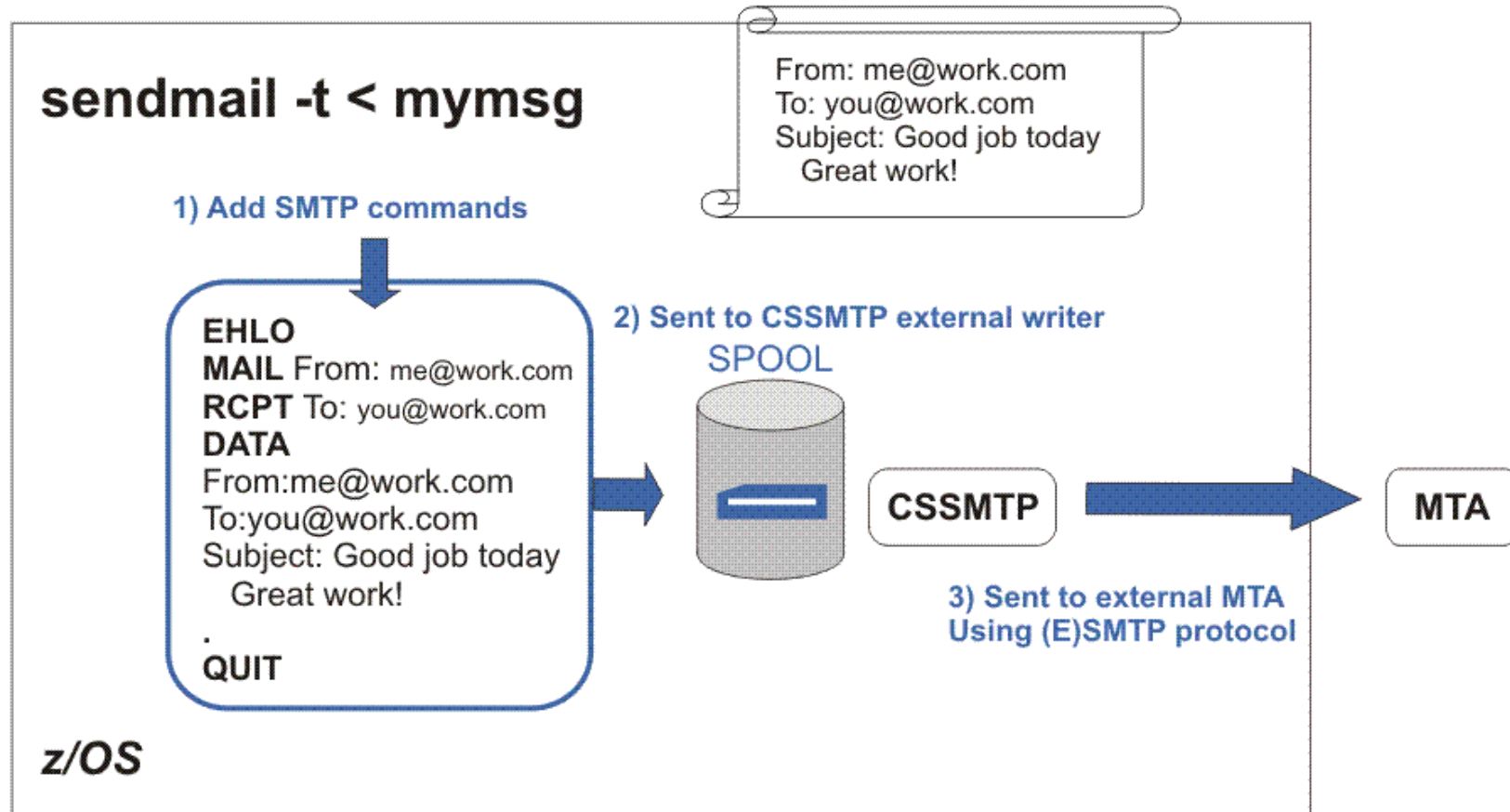


Bottom line: You can still send mail from z/OS using CSSMTPD and the sendmail bridge. But you cannot receive it.

Removal of SMTPD and Sendmail ...

- The SMTPD NJE Gateway and z/OS UNIX sendmail are removed in z/OS V2R3
 - Neither SMTPD nor the sendmail daemon can be configured or started in z/OS V2R3
 - No replacement function provided by z/OS Communications Server for receiving mail for delivery to local TSO/E or z/OS UNIX System Services user mailboxes or for forwarding mail to other destinations
 - While some users may be accustomed to issuing sendmail commands from the UNIX shell, more problematic is the fact that some applications may issue sendmail commands as part of their processing
 - Sendmail commands can still be issued in V2R3 due to the presence of the sendmail to CSSMTP bridge (see next chart)

Sendmail to CSSMTP bridge ...



Sendmail to CSSMTP bridge on V2R1 and V2R2

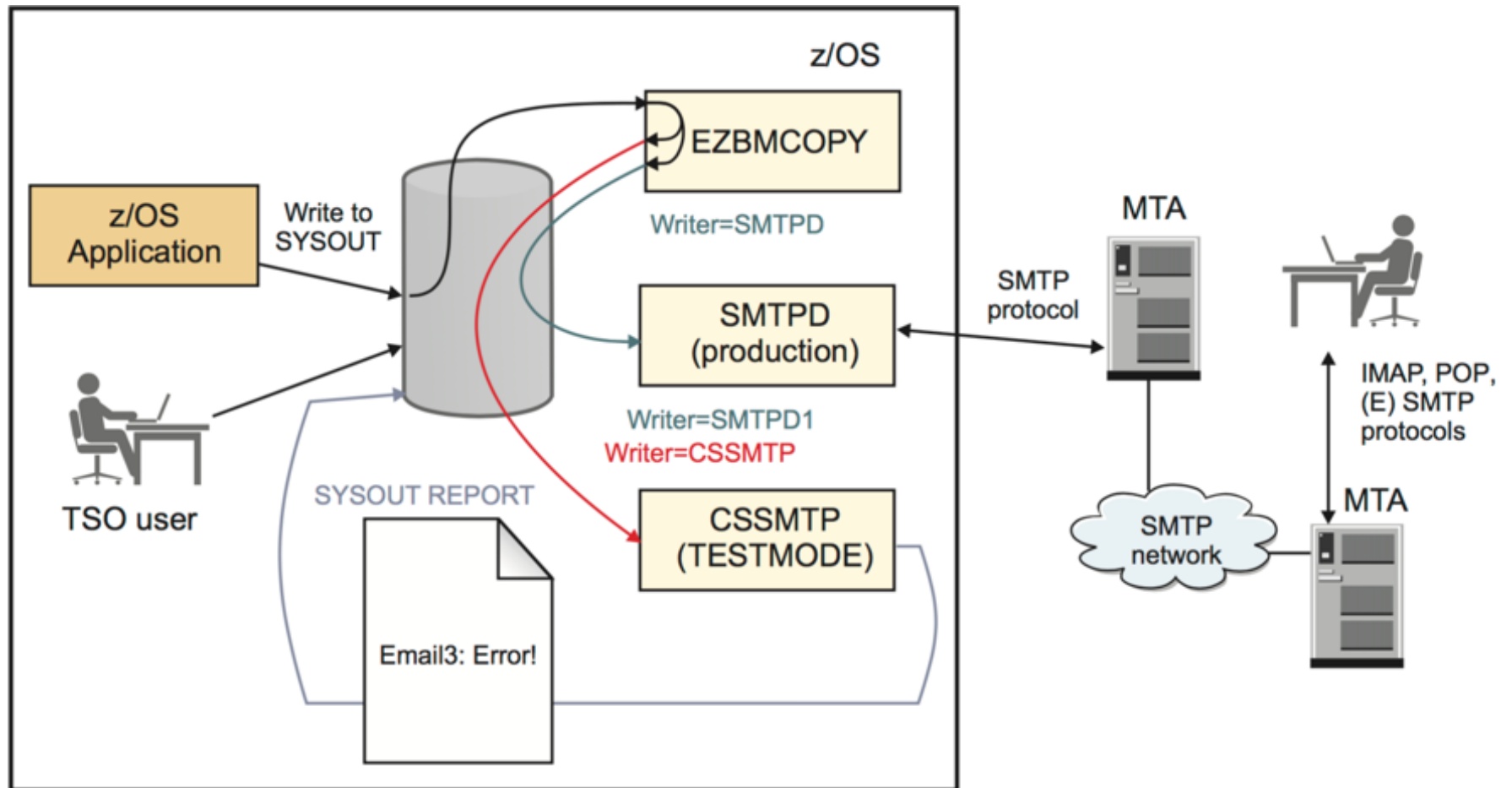
- Support for the sendmail to CSSMTP bridge will also be provided for z/OS V2R1 and V2R2 with APAR PI71175
 - ezatmail (name of the sendmail to CSSMTP bridge executable) command invokes sendmail bridge
 - sendmail unchanged
 - Symbolic link can be added for sendmail to invoke sendmail bridge (ezatmail) for testing

CSSMTP Test Mode Support and EZBMCOPY

Mail migration strategy: SMTPD to CSSMTP

- CSSMTP has stricter standards than SMTP
 - How do you verify that CSSMTP will process your existing production mail workload?
- V2R2 function: CSSMTP test mode
 - A new configuration parameter that causes CSSMTP to run in Test Mode
 - CSSMTP will perform its normal email processing, except it will not actually send emails
 - It will report email failures and discard successful emails
 - You can address incompatible emails before migrating to CSSMTP
 - SMTPD continues to process your mail messages
 - Production emails are unaffected during the test
 - EZBMCOPY
 - Utility program provided by IBM to copy JES email messages to two destinations, SMTPD and CSSMTP
- This is available on V2R1 via APAR PI48700

TEST Mode/EZBMCOPY architecture



CSSMTP Test Mode

- Parameters on the CSSMTP Options statement:

```
>>--Options-----| Put Braces and Parameters on Separate Lines |--><
```

Options Parameters:

```

      +--TestMode NO-----+
|-----+-----+-----+----->
      +--TestMode+-NO--++
                          +-YES--

```

- Notes on TestMode:
 - TestMode cannot be dynamically altered. CSSMTP must be recycled to change its value
 - If no errors are found in a spool file, CSSMTP will release spool files when it has completed processing. If errors are found, CSSMTP will honor the setting of BADSPOOLDISP
 - Make sure the REPORT statement is coded with a valid destination for the error report. Warning message EZD1841I is issued if it is not.

CSSMTP display config

```

F CSSMTP,DISPLAY,CONFIG
EZD1829I CSSMTP CONFIGURATION:
  CONFIGFILENAME      : /U/USER1/CSSMTP/CSSMTP.CONF

  [...]

  BADSPOOLDISP       : HOLD          REPORT          : SYSOUT
  OPTIONS:
  NULLTRUNC          : NO            DATALINETRUNC    : NO
  TESTMODE:          : NO
  [...]

```

The new configuration parameter is also externalized using the CSSMTP SMF configuration record (CONFIG subtype 48)

EZBMCOPY

- Parm value:
 - WRITER=w Select program name (writer name) w
- EZBMCOPY assumes the writer name specified by the WRITER parameter. It selects spool files in two ways:
 - The file's writer name matches the WRITER parameter, or
 - The file's destination matches the WRITER parameter
- Then it makes as many copies as there are OUTPUT cards in the JCL, then deallocates the original data set
 - Restriction: a maximum of two output cards can be coded

EZBMCOPY usage example

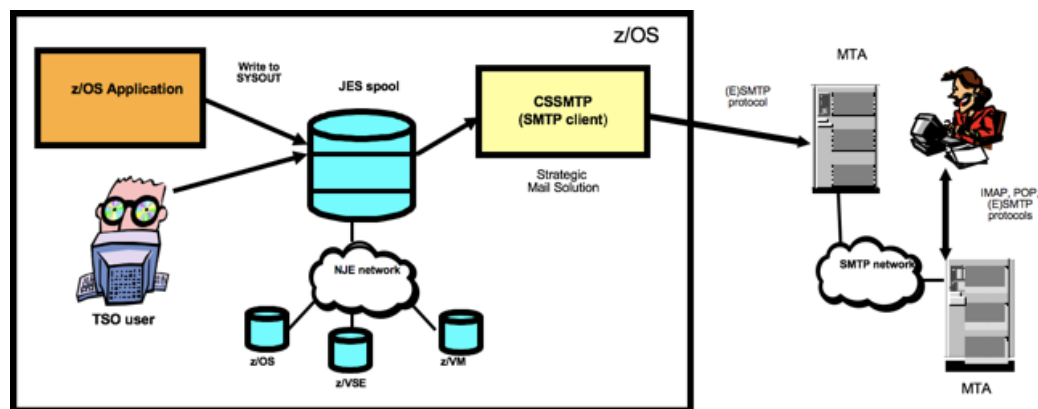
```
//EZBMCOPY PROC
//STEP      EXEC  PGM=EZBMCOPY, PARM='WRITER=SMTPD'
//OUT1      OUTPUT WRITER=SMTPD1
//OUT2      OUTPUT WRITER=CSSMTP
//STEPLIB   DD    DSN=JES2.TESTING.LOAD, DISP=SHR
//SYSUT2    DD    SYSOUT=*, SPIN=UNALLOC, OUTPUT=(*.OUT1, *.OUT2)
//SYSPRINT  DD    SYSOUT=*
//SYSIN     DD    DUMMY
```

- Assume the JCL shown here and SMTPD running with writer name SMTPD.
(note: SMTPD's writer name is its jobname)
 - Change the writer name of SMTPD to SMTPD1 for this test by changing its jobname to SMTPD1
 - Start CSSMTP in TESTMODE with writer name CSSMTP
 - Start EZBMCOPY using the example JCL above

CSSMTP Code Page Enhancements

CSSMTP code page enhancements

- CSSMTP code page enhancements was delivered in July, 2018 via APAR PI93278, and provides two significant enhancements:



- Improved handling of single-byte character set (SBCS) special characters in the mail subject line. Previously, some special characters, such as the euro symbol (€), were not translated correctly.
- Support for multi-byte character sets
 - More details on next chart

CSSMTP code page enhancements ...

- SMTPD provided support for double-byte character sets (DBCS), but prior to APAR PI93278, CSSMTP did not.
- MBCS translation, and in particular DBCS support, is a capability that is used by many customers in some geographies.
- New-function APAR PI93278 for z/OS V2R1, V2R2, and V2R3 provides DBCS support for CSSMTP.
 - Unlike SMTPD, which depended on translation tables, CSSMTP's DBCS support is enabled via specification of a multi-byte code page through a new MBCHARSET operand in the CSSMTP configuration file, along with an MBCS switch to control whether MBCS capability is to be enabled at all.
 - A table in the IP Configuration Guide provides suggestions as to which code page to specify on the MBCHARSET parameter.
- For PTF and documentation information, see the New Function APAR summary web pages (links provided in this presentation)