IBM Education Assistance for z/OS V2R3

Element/Component: Communications Server

Material prepared for IEA and was current as of March 2017

Agenda

- Trademarks
- Session Objectives
- Removal of TFTPD
- Removal of support for legacy devices
- Communications Server support for enhanced system symbols
- IPv6 getaddrinfo() API standards compliance
- AT-TLS currency with System SSL
- Enhanced wildcard support for jobnames on PORT and PORTRANGE statements
- Sysplex-wide security associations (SWSA) scalability improvement
- Removal of SMTPD & sendmail
- sendmail to CSSMTP bridge
- CSSMTP mail compatibility enhancements
- z/OS Encryption Readiness Technology (zERT)
- Session Summary
- Appendix

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 V2R3
  - Removal of TFTPD
  - Removal of support for legacy devices
  - Communications Server support for enhanced system symbols
  - IPv6 getaddrinfo() API standards compliance
  - AT-TLS currency with System SSL
  - Enhanced wildcard support for jobnames on PORT and PORTRANGE statements
  - Sysplex-wide security associations (SWSA) scalability improvement
  - Removal of SMTPD & sendmail
  - sendmail to CSSMTP bridge
  - CSSMTP mail compatibility enhancements
  - z/OS Encryption Readiness Technology

Removal of TFTPD

Overview

- Problem Statement / Need Addressed
  - Trivial File Transfer Protocol (TFTP) – UDP protocol used to transfer files
  - No user authorization, any client that can connect to port 69 has access to TFTPD
  - Access to entire file system, if TFTPD started without a directory
- Solution
  - Remove TFTPD from z/OS
- Benefit / Value
  - Better, more secure file transfer programs available

Migration & Coexistence Considerations

- Migration Considerations:
  - If you are using TFTPD
    - migrate to a supported file transfer program, such as FTP
  - ZOSMIGV2R2_NEXT_CS_TFTP migration health check helps determine if TFTPD is being used – available on V2R1 and V2R2
    - z/OS V2R1 with APARs PI61806 and OA50445 applied.
    - z/OS V2R2 with APARs PI61806 and OA50445 applied.

Removal of support for legacy devices

Overview

- Problem Statement / Need Addressed
  - Legacy devices present testing problems
    - Physical devices not present in test environment
    - Some devices not supported without channel emulation
- Solution
  - Remove support for selected legacy devices
- Benefit / Value
  - Simplified configuration
  - Modern devices provide
    - Improved throughput
    - Lower CPU utilization

Usage & Invocation

- Support for the following devices defined with DEVICE and LINK profile statements has been removed
  - FDDI and Token Ring (LCS with LINKs FDDI and IBMTR)
  - Token Ring (MPCIPA with LINK IPAQTR)
  - Ethernet and FDDI (MPCOSA with LINKs OSAENET and OSAFDDI)

Migration & Coexistence Considerations

- Migration Considerations:
  - Remove TCP/IP profile configuration statements supporting removed devices
  - ZOSMIGV2R2_NEXT_CS_LEGACYDEVICE migration health check helps determine if any of the legacy devices are configured – available on V2R1 and V2R2
    - z/OS V2R1 with APARs PI49962 and OA49071 applied.
    - z/OS V2R2 with APARs PI49962 and OA49071 applied.

Communications Server support for enhanced system symbols

Overview

- Problem Statement / Need Addressed
  - z/OS V2R2 added enhanced system symbol support:
    - longer system symbol names (up to 16 characters) and longer symbol substitution values
    - underscore added as a valid character in a system symbol name
  - Communications Server does not support a system symbol with an underscore in a TCP/IP profile configuration file
  - Communications Server does not support longer symbol substitution values in some cases
- Solution
  - Support enhanced system symbols
- Benefit / Value
  - Provides more flexibility for the use of system symbol names

Usage & Invocation

- System symbols can be used in the following places in Communications Server:
  - PROFILE.TCPIP data sets used by TCP/IP and TN3270
  - Data sets referenced by the VARY TCPIP,,SYNTAXCHECK, the VARY TCPIP,,OBEYFILE, and the VARY TCPIP,,EXPORTPROF commands
  - Resolver setup file and TCPIP.DATA files
  - Values of resolver environment variables, like RESOLVER_CONFIG and RESOLVER_TRACE
  - OMPROUTE configuration file
  - CSSMTP configuration file
  - BeginArchiveParms DSNPrefix parameter in syslogd configuration file
  - Symbol translator utility, EZACFSM1
  - VTAMLST definitions
  - TSOKEY00 parmlib member

Usage & Invocation

- For long symbol substitution (length of substitution value greater than the length of the symbol name):
  - If substitution causes the record to overflow, symbol substitution will fail for the record
- For the TCP/IP profile configuration file, substitution is done for each symbol individually. An overflow can not occur.

IPv6 getaddrinfo() API standards compliance

Overview - Problem

- Problem Statement / Need Addressed
  - getaddrinfo() API - allows applications to resolve hostnames to IPv4 addresses, IPv6 addresses, or combination of both
  - API options indicate which type of addresses to return
  - API implemented in z/OS Communications Server V1R4 from RFC 2553 draft
  - Implementation not compliant with final RFC 3493 in one specific case:
    - IPv6 enabled on system
    - Option ai_family = AF_UNSPEC
    - AI_ALL flag not specified
    - Returns:
      - All IPv6 addresses, if IPv6 address defined for hostname
      - All IPv4 addresses, if no IPv6 address defined for hostname
  - Must specify AI_ALL flag to get both IPv6 and IPv4 addresses
  - Compliant implementation returns both IPv6 and IPv4 addresses associated with hostname

Overview – Solution / Benefit

- Solution
  - Getaddrinfo() API updated to query and return both IPv6 and IPv4 addresses associated with hostname
    - when IPv6 is enabled on the system and ai_family = AI_UNSPEC (without regard to the setting of the AI_ALL flag)
- Benefit / Value
  - Allows IPv6 applications to be ported and run on z/OS without updates to set the AI_ALL flag

Usage & Invocation

- GetAddrInfo API can be invoked for a number of different types of applications:
  - GETADDRINFO REXX socket application programming interface
  - GETADDRINFO Macro application programming interface
  - IMS sockets
    - GETADDRINFO CALL instruction application programming interface
  - CICS sockets
    - getaddrinfo() C language application programming interface
    - GETADDRINFO for the Sockets extended API
  - getaddrinfo(BPX1GAI, BPX4GAI) for Assembler Callable services
  - getaddrinfo() for C/C++

Migration & Coexistence Considerations

- Migration Consideration
  - If IPv6 enabled on your system, applications that issue GetAddrInfo API calls with ai_family = AF_UNSPEC and the AI_ALL flag not specified must be able to accept both IPv4 and IPv6 addresses.
    - Order of returned addresses depends on system configuration and other GetAddrInfo flags, such as AI_ADDRCONFIG
    - IPv4 address can be ordered first in the returned list of addresses

AT-TLS currency with System SSL

Overview / Problem Statment

- Problem Statement / Need Addressed
  - Background: AT-TLS provides SSL/TLS protection to TCP traffic
    - Acts as a System SSL wrapper
    - Applied based on policy, no need to change application source code
    - Stays current with new System SSL features
  - AT-TLS does not support key length transition recommendations defined in NIST SP800-131A Revision 1
  - AT-TLS does not support new certificate processing controls defined in NIST SP800-52A Revision 1 (TLS implementation guidelines)
  - AT-TLS does not support latest Online Certificate Status Protocol (OCSP) features (RFCs 6066, 6277, 6960, and 6961)
  - AT-TLS does not support Suite B Profile clarifications in RFCs 6460 and 5759
  - AT-TLS does not support the Signaling Cipher Suite Value (SCSV) which can provide protection against protocol downgrade attacks (RFC 7507)

Overview / Solution

- Solution - AT-TLS enhanced to:
  - Provide FIPS 140-2 security levels to enforce different cryptographic strengths (NIST SP800-131A Revision 1)
  - Support new certificate processing controls defined in NIST SP800-52A Revision 1, including
    - Support to allow multiple certificates to be specified for use by server when negotiating secure connections
  - Support new OCSP features, such as OCSP stapling (RFC 6066, 6277, 6960, 6961)
  - Support new 128Min and 192Min profiles for the Suite B Profile (RFCs 6460 and 5759)
  - Support the Signaling Cipher Suite Value (SCSV) which can provide protection against protocol downgrade attacks (RFC 7507)

Overview / Benefit

- Benefit / Value
  - More secure FIPS140-2 implementation exploited (NIST SP800-131A Revision 1)
  - New certificate processing controls defined in NIST SP800-52A Revision 1 exploited
  - New OCSP features, such as OCSP stapling are exploited (RFC 6066, RFC 6277, RFC 6960, RFC 6961)
  - New 128Min and 192Min profiles for the Suite B Profile are exploited (RFCs 6460 and 5759)
  - Support for the Signaling Cipher Suite Value (SCSV) is exploited (RFC 7507)

Usage & Invocation

- NIST SP800-131A Revision 1
  - TTLSGroupAction
- NIST SP800-52A Revision 1
  - TTLSEnvironmentAdvancedParms
- RFCs 6066, 6277, 6960, 6961
  - TTLSGskOcspParms, TTLSEnvironmentAdvancedParms, TTLSConnectionAdvancedParms
- RFCs 6460 and 5759
  - TTLSEnvironmentAction, TTLSGskAdvancedParms
- RFC 7507
  - TTLSEnvironmentAdvancedParms
- z/OS Configuration Assistant for Communications Server updated to support all new AT-TLS policy options

Enhanced wildcard support for jobname on PORT and PORTRANGE statements

Overview

- Problem Statement / Need Addressed
  - Ports can be reserved for an application by specifying a jobname value on the PORT/PORTRANGE configuration statements
  - Limited wildcard support for jobname can require many PORT/PORTRANGE statements
    - * matches any jobname
    - APPL1* matches any jobname beginning with APPL1
  - For example, consider the following job names:
    - ab1xyz, ab2xyz, ab3xyz, ab4xyz, ab5xyz
      - These job names are authorized
    - ab1efg
      - This job name is not authorized
  - A separate PORT statement would be needed for each job name
    - ab* would not work as it would authorize ab1efg

Overview continued

- Solution
  - Enhanced wildcard support for jobname
    - * used in any position to represent 0 or more unspecified characters
    - ? used in any position to represent a single unspecified character
- Benefit / Value
  - Simplified configuration – multiple PORT / PORTRANGE statements can be reduced to a single statement
  - For example consider the following job names:
    - ab1xyz, ab2xyz, ab3xyz, ab4xyz, ab5xyz
      - These job names are authorized
    - ab1efg
      - This job name is not authorized
  - A single PORT statement with job name ab?xyz can be configured

Usage & Invocation

- Update the jobname value on PORT and PORTRANGE to use wildcard support
- It is possible for a job name to match multiple PORT/PORTRANGE statements. Search criteria is:
  - An exact match on the job name from the primary address space
  - For a partial specification, job name is compared character by character from left to right
    - When a character in the job name does not match the specification, the following hierarchy is used to determine which is the best match:
      - A non-wildcard character takes precedence over a wildcard specification
      - A single wildcard character of question mark takes precedence over the multiple wildcard character of asterisk
  - An exact match on the job name from the secondary address space

Usage & Invocation, example 1

- Assume two PORT statements:
  - PORT 6002 TCP US?R* SHAREPORT
  - PORT 6002 TCP US*R*
- Job with name USER15 binds to port 6002
- Which PORT statement does USER15 match?
  - PORT 6002 TCP **US?R*** SHAREPORT
  - Single wildcard of '?' beats multiple wildcard of '*'

Usage & Invocation, example 2

- Assume two PORT statements:
  - PORT 6002 TCP U?ER* SHAREPORT
  - PORT 6002 TCP US*R*
- Job with name USER15 binds to port 6002
- Which PORT statement does USER15 match?
  - PORT 6002 TCP **US*R***
  - Specific match on 'S' beats '?'

Usage & Invocation, example 3

- Assume two PORT statements:
  - PORT 6002 TCP USER?? SHAREPORT
  - PORT 6002 TCP USER*
- Job with name USER15 binds to port 6002
- Which PORT statement does USER15 match?
  - PORT 6002 TCP **USER??** SHAREPORT
  - Single wildcard of '?' beats multiple wildcard of '*'

Sysplex-wide security associations (SWSA) scalability improvement

Overview

- Problem Statement / Need Addressed
  - EZBDVIPA coupling facility structure required to support sysplex-wide security associations (SWSA) – DVIPA takeover and sysplex distribution
  - EZBDVIPA has fixed number of lists - 2048 lists
  - As IPSec implementations increase in size, number of EZBDVIPA lists could limit number of security associations deployed in a sysplex
- Solution
  - Configuration option that allows the EZBDVIPA structure to have up to 16,384 lists
- Benefit / Value
  - Increased number of IPSec security associations can be deployed in a sysplex

Usage & Invocation

- Use CFSizer tool to determine size and list count recommendations for the EZBDVIPA structure
- Modify and install CFRM policy with any recommended changes for INITSIZE and SIZE
- Issue MODIFY VTAMOPTS command to modify DVLSTCNT START option for all VTAMs in sysplex
- Issue SETXCF START,REBUILD command for the EZBDVIPA structure to rebuild the structure
- Issue D NET,STATS,TYPE=CFS command to verify number of lists

Interactions & Dependencies

- Software Dependencies
  - CFSizer tool is updated to provide suggested number of lists
    - http://www.ibm.com/systems/support/z/cfsizer/

Migration & Coexistence Considerations

- Migration Considerations - None
- Coexistence Considerations
  - All VTAMs in a sysplex must be at z/OS V2R3 before increasing the number of lists for an EZBDVIPA structure above 2048 lists
  - Number of lists configured for an EZBDVIPA structure must be the same for all VTAMs in a sysplex. If the configured number of lists is different:
    - actual number of lists is unpredictable (dependent on first VTAM to connect to EZBDVIPA structure)
    - IPSec distribution and takeover data can be inaccessible to some TCP/IP stacks in the sysplex or VTAM subplex, resulting in errors such as:
      - Tunnels not being re-established when DVIPA ownership changes, causing data failures
      - EZD0834I Encapsulation failed (reason code 9)

Removal of SMTPD and sendmail

sendmail to CSSMTP bridge

Overview - SOD

- The removal of the SMTPD NJE Mail Gateway and sendmail mail transports was first announced on 24 February 2014 in U.S. Announcement Letter 114-009. On 25 July 2015, Software Announcement 215-267 further stipulated that z/OS V2R2 would be the last release to include these functions.

Overview – SOD (2014)

- U.S. Announcement Letter 114-009, 24 February 2104

Removal of SMTPD NJE Mail Gateway and Sendmail mail transports from z/OS Communications Server:
It is the intention of IBM to remove the Simple Mail Transport Protocol Network Job Entry (SMTPD NJE) Mail Gateway and Sendmail mail transports from z/OS Communications Server in the future. If you use the SMTPD NJE Gateway to send mail, IBM recommends you use the existing CSSMTP SMTP NJE Mail Gateway instead. CSSMTP provides significant functional and performance improvements. The Sendmail client program can also be used to send mail messages; a replacement function using CSSMTP as the SMTP transport is planned. This function will be designed so that it does not require application programming changes. No replacement function is planned in z/OS Communications Server to support using SMTPD or Sendmail as a (SMTP) 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.

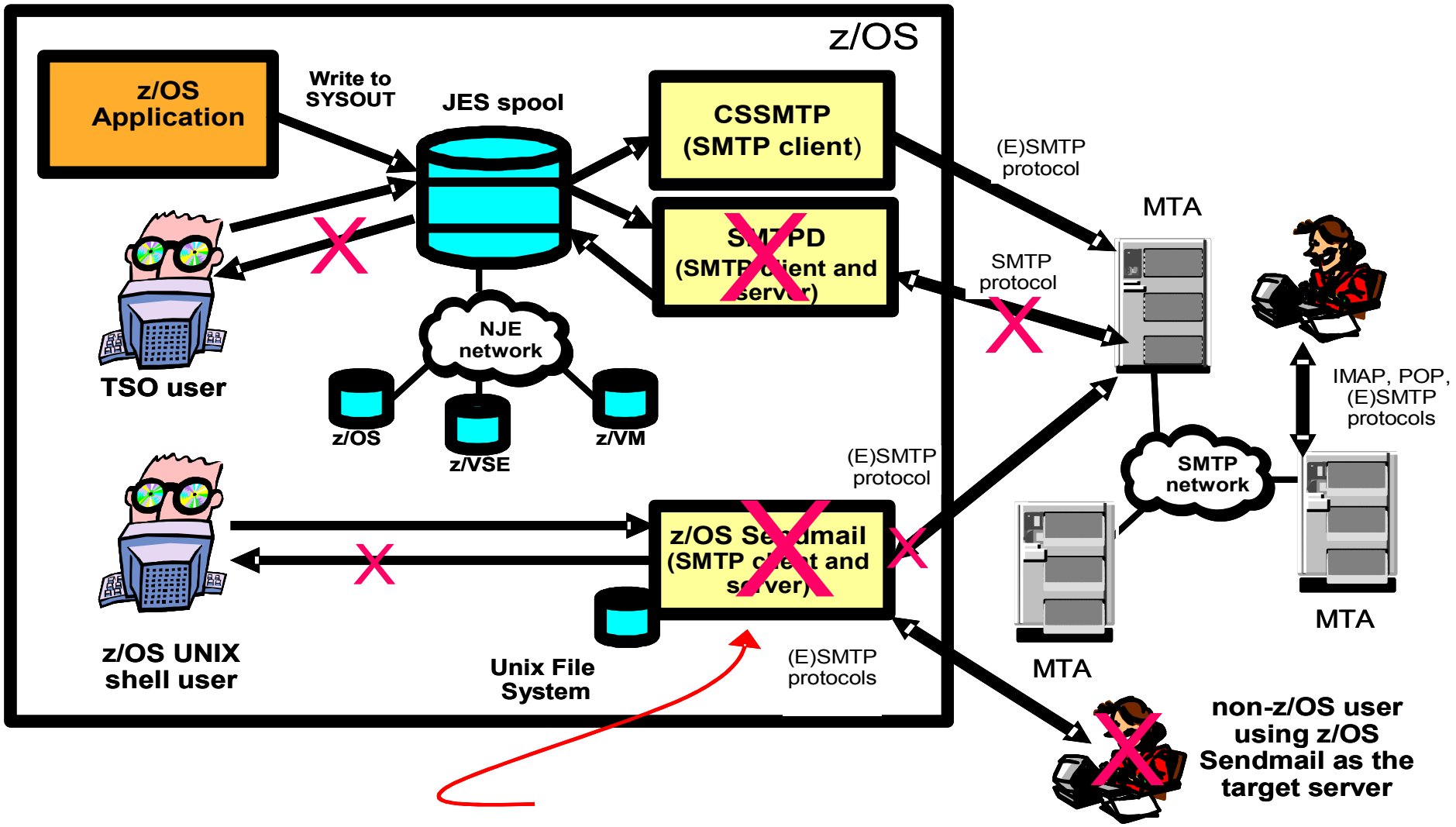
Overview – SOD (2105)

- Software Announcement 215-267, 25 July 2015

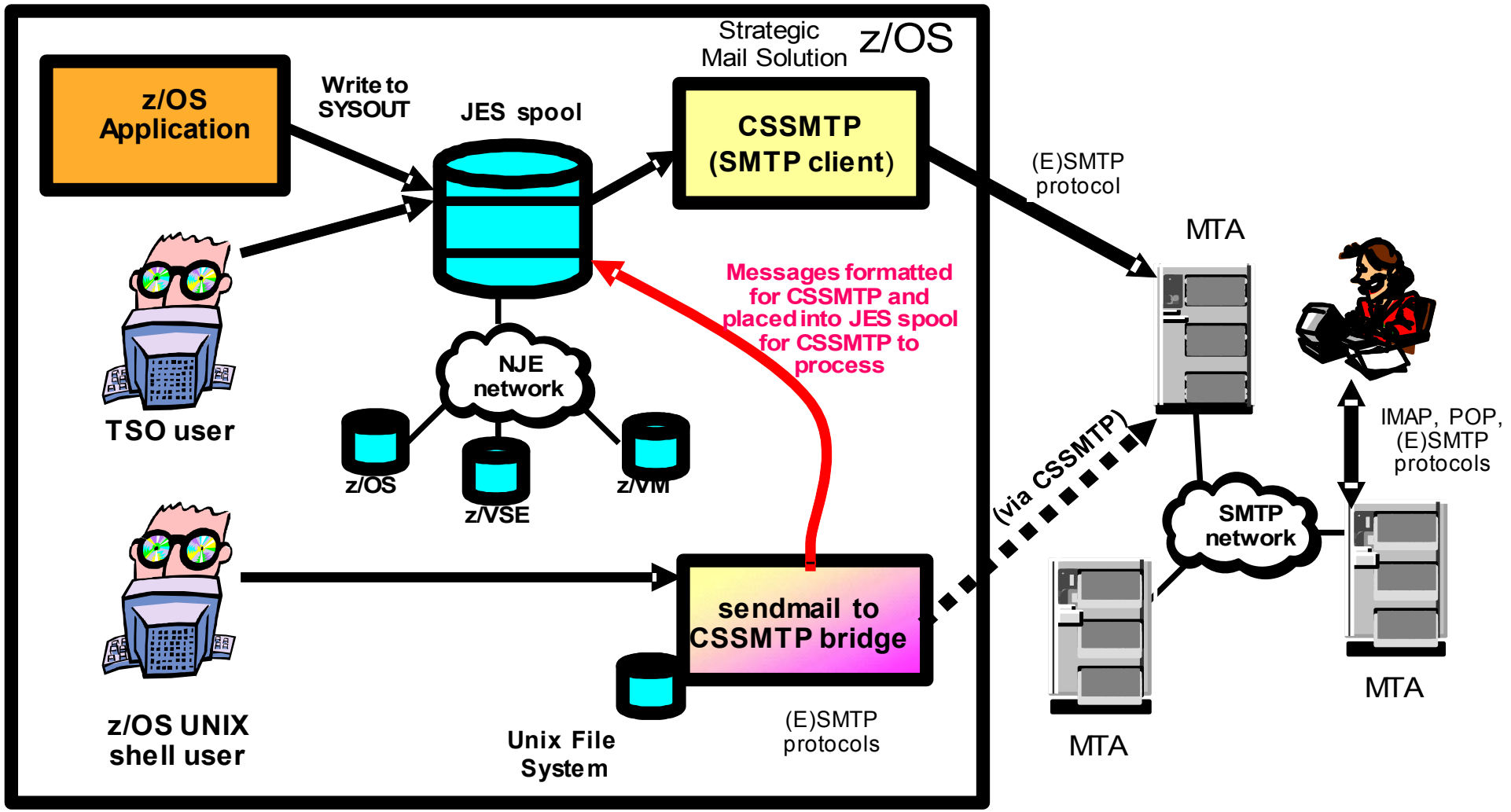
As previously announced in Hardware Announcement 114-009, dated February 24, 2014, the Simple Mail Transport Protocol Network Job Entry (SMTPD NJE) Mail Gateway and Sendmail mail transports are planned to be removed from z/OS. IBM now plans for z/OS V2.2 to be the last release to include these functions. If you use the SMTPD NJE Gateway to send mail, IBM recommends you use the existing CSSMTP SMTP NJE Mail Gateway instead. In that same announcement, IBM announced plans to provide a replacement program for the Sendmail client that would not require programming changes. **Those plans have changed, and IBM now plans to provide a compatible subset of functions for Sendmail in the replacement program and to announce those functions in the future. Programming changes or alternative solutions to currently provided Sendmail functions might be required.** No replacement function is planned in z/OS Communications Server to support using SMTPD or Sendmail as a (SMTP) 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.

Overview – Mail components

- Mail components being removed



Overview – Mail components in V2R3



Bottom line: Still able to send mail from z/OS using CSSMTPD and sendmail to CSSMTP bridge. But not able to receive it.

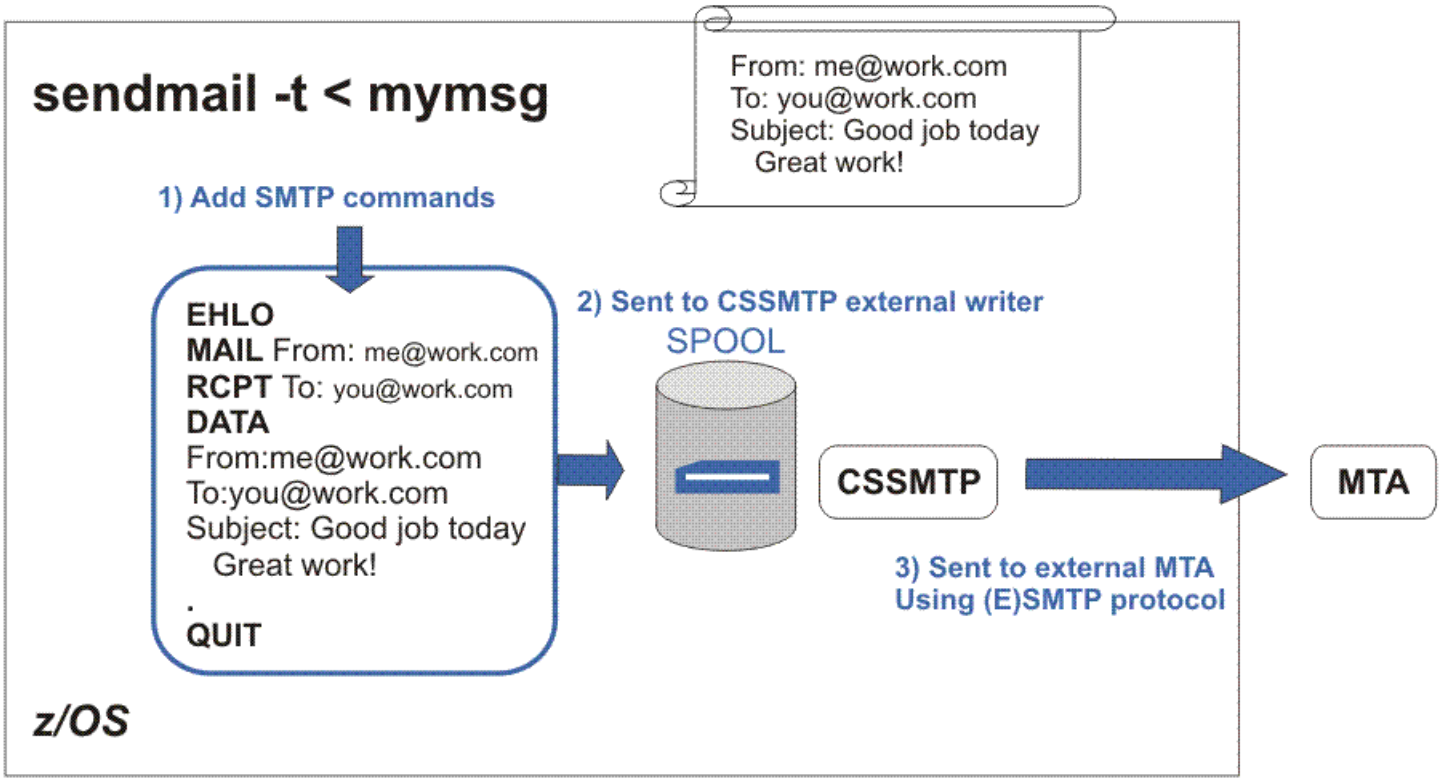
Overview – Problem / Solution

- Problem Statement / Need Addressed
  - SMTPD NJE Gateway:
    - Pascal API application
    - Supports older SMTP RFCs, no support for TLS/SSL or IPv6
    - Performance issues (single-threaded)
  - z/OS UNIX sendmail:
    - Ported code from 2001 – out of date
- Solution
  - SMTPD NJE Gateway removed
  - z/OS UNIX sendmail removed
    - compatible subset of sendmail function provided by sendmail to CSSMTP bridge (sendmail bridge) & CSSMTP to send mail

Overview – sendmail bridge solution

- Solution (continued)
  - sendmail bridge:
    - Parses input options from command line
    - Reads mail message from UNIX System Services file
    - Mail message updated by adding SMTP commands and SMTP headers (if no header specified in input mail message)
    - Mail message transmitted to JES spool data set
  - Communications Server SMTP (CSSMTP) application processes JES spool data set

Overview – sendmail bridge solution (continued)



Overview – Benefit/value

- Benefit / Value
  - CSSMTP provides functional and performance improvements (multi-threaded) for sending mail
  - sendmail to CSSMTP bridge (sendmail bridge) provides mechanism for mail to be sent from z/OS UNIX programs or users
    - Can continue to use sendmail command which is a symbolic link to the sendmail bridge

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

Usage & Invocation – sendmail bridge configuration file

- Create and customize configuration file for sendmail bridge
  - Copy sample file /usr/lpp/tcpip/samples/ezatmail.cf to /etc/mail/ezatmail.cf
    - Can use existing sendmail configuration files /etc/mail/submit.cf or /etc/mail/sendmail.cf (many statements not supported for sendmail bridge, ignored)
  - For information on customizing the configuration file, see “sendmail to CSSMTP bridge” z/OS Communications Server: IP Configuration Guide

Usage & Invocation - sendmail bridge

- CSSMTP application must be active
  - For information on configuring CSSMTP, see “Configuring the CSSMTP application” in the z/OS Communications Server: IP Configuration Guide
- sendmail command is directed to the sendmail bridge (ezatmail)

  sendmail *command_switch(es) recipient name(s) <input mail message*

  Example: sendmail -d0-99.100 you1@work.com </tmp/mymail1

  /tmp/mymail1 contains:
  From: me@work.com
  Subject: Good job today
  Great work!

  Result: Message updated with SMTP commands & headers and transmitted to JES spool data set
- For information on supported *command_switches*, see “Sending emails by using the sendmail to CSSMTP bridge” z/OS Communications Server: IP User's Guide and Commands

Migration & Coexistence Considerations

- Migration Considerations
  - SMTPD NJE Gateway removed
    - migrate to CSSMTP to send mail
  - z/OS UNIX sendmail removed
    - compatible subset of sendmail function provided by sendmail to CSSMTP bridge (sendmail bridge) and CSSMTP to send mail
  - 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
  - z/OS V2R3 Migration and Installation, Communications Server migration action:
    - IP services: Migrate from SMTP and sendmail

Migration & Coexistence Considerations continued

- Migration Considerations
  - SMTPD removal
    - To use SMTPNOTE with CSSMTP, verify that configuration specifies the CSSMTP external writer name
    - LPD server: to send notices of failed jobs, verify that configuration specifies the CSSMTP external writer name
  - sendmail bridge Transport Layer Security (TLS) support
    - Configuration statement D{tls_version} supported but value of tls_version is ignored
      - Secured connection is setup between CSSMTP and target mail server based on configured AT-TLS policy
      - See “Steps for using Transport Layer Security for CSSMTP” in z/OS Communications Server: IP Configuration Guide

CSSMTP mail compatibility enhancements

Overview - Improved TLS compatibility with mail servers

- Problem Statement / Need Addressed
  - CSSMTP reads mail jobs from JES and sends emails to a target server for delivery to destination
  - TLS security setup between a client (CSSMTP) and target server defined in RFC 3207, with an optional second EHLO and capabilities exchange after TLS negotiation
    - CSSMTP does not do 2nd EHLO and capabilities exchange
  - Some target servers will not connect with CSSMTP after TLS negotiation without the second EHLO and capabilities exchange
  - Mail sent by CSSMTP to some target servers can not be secured with TLS
- Solution
  - Configuration option provided to enable EHLO and capabilities exchange following TLS negotiation
- Benefit / Value
  - CSSMTP compatible with target servers that require a second EHLO and capabilities exchange

Usage & Invocation - Improved TLS compatibility with mail servers

- CSSMTP configuration file
  - New parameter on the Options statement : TLSEhlo No | Yes
  - Example:

```
Options
{
   TLSEhlo Yes
}
```

  - Default value: No
  - Support also provided for z/OS V2R2 and V2R1 with APAR PI56614

Overview – CSSMTP customizable ATSIGN character for mail addresses

- Problem Statement / Need Addressed
  - SMTPD has limited code page support, IBM-1047 used for EBCDIC to ASCII conversion
  - Code point for ATSIGN (@) symbol varies in code pages, for example

Code Page	Symbol at '7C'	Symbol at 'B5'
IBM-1047	@	§
IBM-273	§	@

  - Many customers that use IBM-273 modified mail generating programs to force x'7C' character to represent ATSIGN to overcome SMTPD's limited code page support
  - CSSMTP does necessary translation of input mail messages through iconv
    - Example: x'7C' in mail header translated from IBM-273 to IBM-1047 resulting in incorrect ATSIGN character in mail header
  - To migrate from SMTPD to CSSMTP, customer must update mail generating programs

Overview – CSSMTP customizable ATSIGN character for mail addresses (continued)

- Solution
  - Configuration option provided to define the ATSIGN character used by mail generating programs
  - CSSMTP processing:
    - Read mail data set from JES and translate it to IBM-1047
    - Search SMTP commands and headers for the configured ATSIGN symbol
    - Update character to x'7C' (@ in IBM-1047)
    - Body of mail remains unchanged
- Benefit / Value
  - Simplifies migration path from SMTPD to CSSMTP
    - no change required to mail generating programs

Usage & Invocation - CSSMTP customizable ATSIGN character for mail addresses

- CSSMTP configuration file
  - New parameter on the Options statement : AtSign *character*
  - Example:

```
Options
{
   AtSign §
}
```

  - Default *character*: '@' (hex '7C')
  - Support also provided for z/OS V2R2 and V2R1 with APAR PI52704

Overview – Improved CSSMTP code page compatibility with target servers

- Problem Statement / Need Addressed
  - CSSMTP TRANSLATE configuration statement specifies code page of the JES spool files
  - Mail message commands and headers translated from configured TRANSLATE code page to IBM-1047 EBCDIC for processing, then translated to ISO8859-1 ASCII before sending to target server
  - Body of mail message directly translated to ISO8859-1 ASCII before sending to target server
  - No option to configure the ASCII code page for the target server
  - ISO8859-1 does not contain the euro sign (€)
  - ISO8859-1 not always compatible with target server code page

Overview – Improved CSSMTP code page compatibility with target servers (continued)

- Solution
  - Configuration parameter, Charset, provided to specify code page to be used when translating mail message to be sent to target server
  - Mail message body translated from the TRANSLATE code page directly to configured Charset code page
  - Mail message headers translated from IBM-1047 code page to Charset code page
  - Charset code page must be defined to Unicode System Services
- Benefit / Value
  - Improves CSSMTP code page compatibility with target servers
  - CSSMTP can be configured to use same code page as target server
    - Characters, such as the euro sign (€), are supported in body of mail message

Usage & Invocation – Improved CSSMTP code page compatibility with target servers

- CSSMTP configuration file
  - New CSSMTP configuration parameter on the TargetServer statement : Charset *codepage*
  - Example:

```
TargetServer
{
   . . .
   Charset 1252
}
```

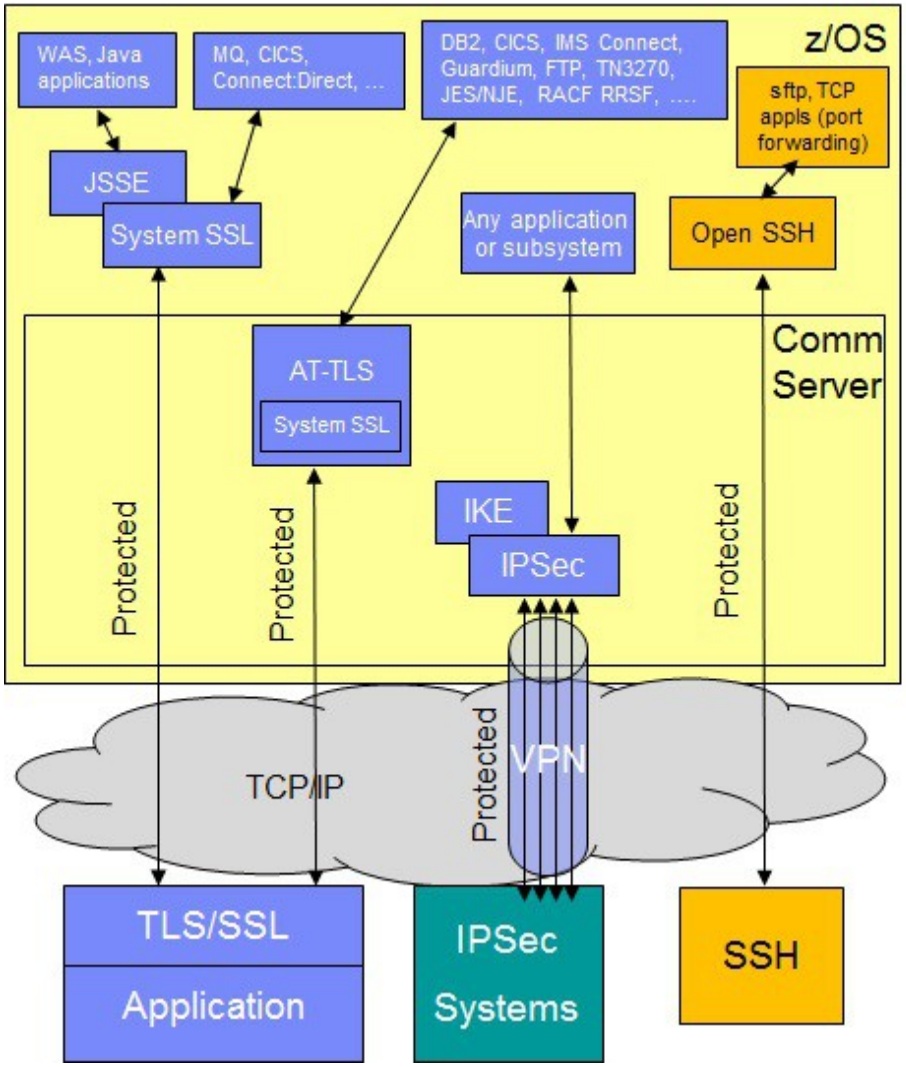
  - Default *codepage*: ISO8859-1
  - Support also provided for z/OS V2R2 and V2R1 with APAR PI73909

z/OS Encryption Readiness Technology

Overview – problem

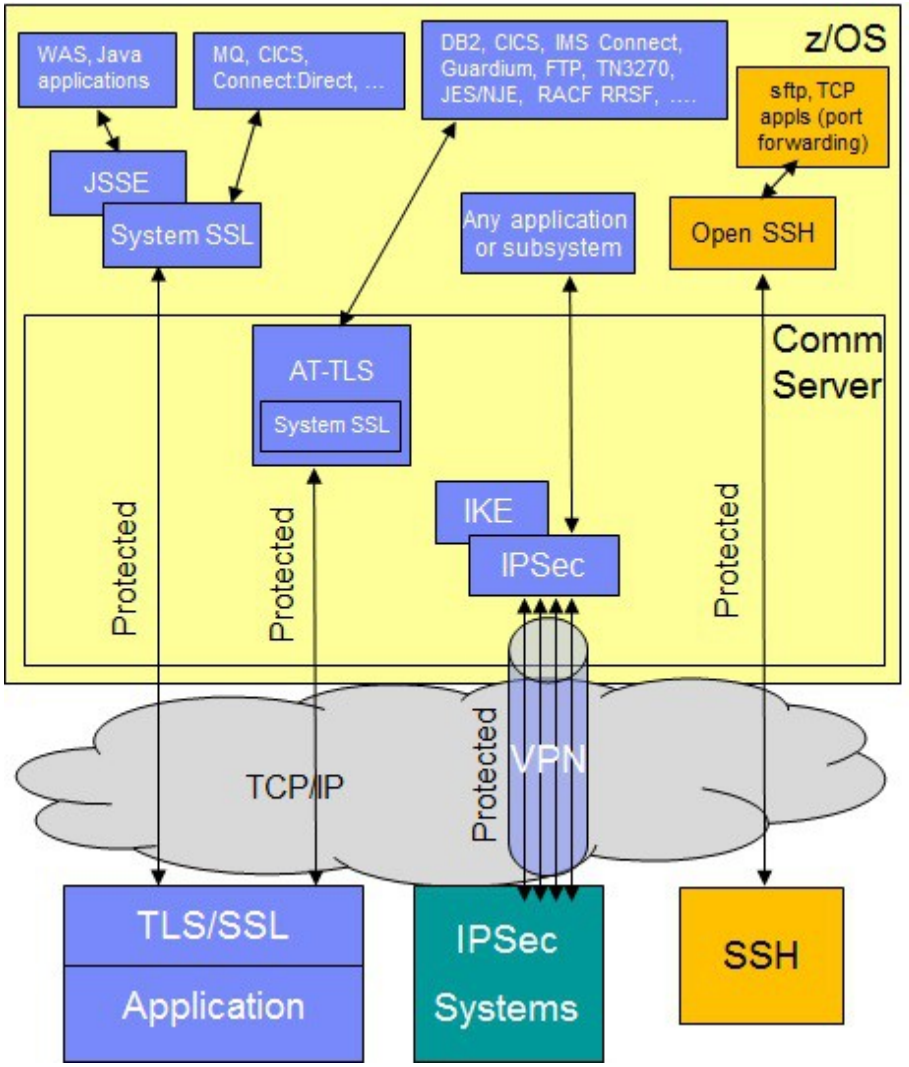
Different ways to cryptographically protect z/OS TCP/IP traffic

- Secure Shell (SSH)
  - sftp and scp secure file transfer
  - ssh proxied sessions
  - TCP only
- TLS/SSL through System SSL or JSSE
  - Applications coded to use TLS/SSL
  - Per-session protection
  - TCP only
- Application Transparent TLS (AT-TLS)
  - TLS/SSL applied in transport layer of TCP/IP stack as defined by policy
  - TCP/IP calls System SSL on appl's behalf
  - Basic, Aware, and Controlling modes
  - TCP only
- IP Security (IPSec)
  - Implemented at IP layer as defined by RFCs, configured through policy
  - Wide variety of traffic can be protected:
    - ANY IP-based traffic (TCP, UDP, raw)
    - Scope: Very wide (IP addr to IP addr), very narrow (specific appl) or anything in between



Overview – problem (continued)

- Given all these different mechanisms, how can I tell:
  - **Which traffic** is being protected?
  - **How** is that traffic being protected?
    - Security protocol?
    - Protocol version?
    - Cryptographic algorithms?
    - Key lengths?
    - …and so on
  - **Who** does the traffic belong to in case I need to follow up with them?
- Once I know the answers to the above questions, how can I easily provide that information to my auditors or compliance officers?
- And how can I easily ensure that new configurations adhere to my company's security policy?



Overview

- Problem Statement / Need Addressed
  - No common technique to monitor network security policy adherence
    - Multiple methods for configuring security protocols for data in flight across a wide variety of z/OS workloads and tiers which can lead to inconsistent implementation of network security and compliance failures
- Solution
  - z/OS Encryption Readiness Technology provides new SMF records and Network Management Interface (NMI) enhancements to enable discovery and auditing of the network encryption attributes associated with TCP and Enterprise Extender (EE) traffic
- Benefit / Value
  - A single interface for monitoring compliance with cryptographic policies for data in flight across the network

Overview - SMF record

- z/OS encryption readiness technology connection detail SMF record (type 119, subtype 11)
  - Event type: connection initiation, connection termination, security attributes change
  - Connection attributes
  - IP filter information (if IP filtering enabled)
  - TLS protection details (if TLS/SSL protection for connection, TCP only)
  - SSH protection details (if SSH protection for connection, TCP only)
  - IPSec protection details (if IPSec protection for connection)

- See the z/OS Communications Server: IP Programmer's Guide and Reference for a complete layout of the SMF type 119, subtype 11 record.

Overview - Discovery of security attributes

- Reported security attributes are learned from:
  - Notifications from cryptographic protocol providers (CPPs) with detailed security attribute data
    - System SSL
    - OpenSSH
    - IPSec
  - Stream observation of TLS/SSL and SSH handshakes for TCP connections
    - If no CPP notification, stream observation provides basic data (such as, encryption and authentication algorithms)
    - Limited amount of observational security data can be obtained, varies by protocol due to factors like predictability of packet contents and handshake information hidden by encryption
- Notifications and observation occur both for client and server connection endpoints on z/OS

Overview – System SSL notifications

- Notifications provided by System SSL rely on previous TLS/SSL stream observation
  - For applications that use AT-TLS (TCP/IP stack uses System SSL) , stream observation is reliable
  - For applications that use System SSL directly, there are cases where stream observation does not recognize the TLS/SSL handshake
    - Result: TLS/SSL attributes not captured
    - SIOCSHSNOTIFY ioctl provided to improve ability of TCP/IP stack to recognize a TLS/SSL handshake (see the z/OS Communications Server: IP Programmer's Guide and Reference for information on SIOCSHSNOTIFY)

Usage & Invocation

- To enable z/OS Encryption Readiness Technology (ZERT)
  - Configure new ZERT parameter on the GLOBALCONFIG statement in the TCP/IP profile
  - GLOBALCONFIG ZERT enables monitoring of TCP and EE connections, internally recording security information for each connection
  - Example: GLOBALCONFIG ZERT
- To generate connection level SMF records with detailed security information from ZERT monitoring
  - Configure new ZERTDETAIL parameter on the SMFCONFIG statement under the 119 options, in the TCP/IP profile
  - ZERTDETAIL enables generation of connection level SMF 119, subtype 11 records for connection initialization, termination, and change in security attributes (if ZERT is enabled)
  - Example: SMFCONFIG TYPE119 ZERTDETAIL

Usage & Invocation (continued)

- To enable the real time z/OS Encryption Readiness Technology SMF NMI service (SYSTCPER)
  - Configure new ZERTSERVICE parameter on the NETMONITOR statement
  - SYSTCPER provides interface for network management applications to obtain connection level SMF type 119 subtype 11 records which are generated for connection initialization, termination, and change in security attributes (if ZERT is enabled)
  - Example: NETMONITOR ZERTSERVICE
  - SAF-based access control available
    - EZB.NETMGMT.*sysname.tcpname.*SYSTCPER
- ZERT SMF records and the NMI SYSTCPER service are enabled/disabled independently – one, both, or neither can be enabled
- z/OS Configuration Assistant for Communications Server updated to support zERT TCP/IP profile parameters

Migration & Coexistence Considerations

- Migration considerations - None
- Coexistence considerations
  - In a sysplex with TCP/IP stacks at different release levels
    - Target stack must be at release V2R3 with ZERT enabled to be able to collect any TLS, SSH or IPSec protection details for a connection
    - If distributing stack is V2R2 or V2R1, IPSec protection details available to the target stack are limited (no IKE tunnel details or lifetime values)
  - 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
  - Before enabling SMF records for z/OS Encryption Readiness Technology
    - Plan for increased volume of connection level SMF records
    - Implement appropriate security for SMF datasets

Session Summary

- Enhancing security
  - AT-TLS currency with System SSL
  - z/OS Encryption Readiness Technology
- Application Development
  - Removal of SMTPD and sendmail
  - sendmail to CSSMTP bridge
  - CSSMTP mail compatibility enhancements
    - CSSMTP customizable ATSIGN character for mail addresses
    - Improved CSSMTP TLS compatibility with mail servers
    - Improved CSSMTP code page compatibility with target servers
  - IPv6 getaddrinfo() API standards compliance
  - Removal of TFTPD

Session Summary continued

- Systems management
  - Communications Server support for enhanced system symbols
- Usability and skills
  - Enhanced wildcard support for jobnames on PORT and PORTRANGE statements
- Scalability and performance
  - Sysplex-wide security associations (SWSA) scalability improvement
- Networking
  - Removal of support for legacy devices

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

Appendix continued

- z/OS Communications Server Publications
  - 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

- 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

- CFSizer tool website
  - http://www.ibm.com/systems/support/z/cfsizer/