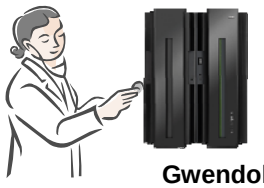
#SHAREorg

SHARE

The Doctor is In: Conducting a z/OS Communications Server TCP/IP Health Check



Gwendolyn Dente (gdente@us.ibm.com)
IBM Advanced Technical Skills (ATS)

****

Tues., Feb. 5, 2013 – (11:00 – 12:15) in Golden Gate 3
(Lobby Level of San Francisco Hilton)
Session 12849

SHARE in San Francisco 2013

Abstract

- With every new release of z/OS you do your best just to upgrade your systems to the latest level of code.
- But perhaps you should also take an overall look at your TCP/IP configuration to determine if you are still following Best Practices for configuration and tuning and whether you should be exploiting new features.
- This can be a massive undertaking, or you can simplify it with a quick start that requires analysis of just a few pages of output from command displays. No tracing or dump analysis is necessary!
- This brief session provides you with basic tips on how to determine if your TCP/IP is well-behaving or not and whether you may have to go in for more "lab tests."
- **NOTE: The short version of this presentation may skip pages; a longer version may allow us to look at the details in the Appendices.**

System z Social Media

#SHAREorg

SHARE

System z official Twitter handle:

- @ibm_system_z

Top Facebook pages related to System z:

- Systemz Mainframe
- IBM System z on Campus
- IBM Mainframe Professionals
- Millennial Mainframer

Top LinkedIn Groups related to System z:

- Mainframe Experts Network
- Mainframe
- IBM Mainframe
- System z Advocates
- Cloud Mainframe Computing

YouTube

- IBM System z

Leading Blogs related to System z:

- Evangelizing Mainframe (Destination z blog)
- Mainframe Performance Topics
- Common Sense
- Enterprise Class Innovation: System z perspectives
- Mainframe
- MainframeZone
- Smarter Computing Blog
- Millennial Mainframer

SHARE in San Francisco 2013

Agenda

1. What do we mean by “Health Check”?
2. What are the steps to take in a Health Check?
3. What types of data do we collect for a networking Health Check?
4. Description of our Example for this Presentation
5. Networking Documentation for an Educational Health Check
    1. Topology Diagrams
    2. Output from Networking Command Execution
    3. Resources to determine which output to request and what to analyze:
        1. *Migration efforts*
        2. *New Features*
        3. *Best Practices*
6. Sample Health Check Analysis
7. Appendix A: Health Check Requested due to a PMR
8. Appendix B: Tools Available for Health Checks

What is a z/OS Networking Health Check?

- It is a *complement* to Monitoring, Migration, and Management Processes that you already have in place.
- It *examines* one or more components and *assesses* them and their interactions for a *stated purpose*
- It defines the *boundaries (scope)* of the Health Check:
  - Which platforms (software or hardware) are subject to the analysis?
  - Which specific nodes or topologies require analysis?
- It depends on input provided by a customer or the installation.

Summary of Steps

1. Define the Purpose or Expected Outcome of the Networking Health Check and its Scope
   - A. Education and Advice?
   - B. Analysis, Audit?
   - C. Insight into a Problem?
2. Define the Format of the Networking Health Check Report
3. ***List the documentation and tools required for the analysis and the personnel who will provide the documentation***
4. ***Gather and analyze the documentation***
5. Write the report

❖ In this brief presentation, we illustrate some of the documentation and tools for an analysis (bullet #3), and then an analysis of the gathered documentation (bullet #4) and place the bullets in appendices. We omit an example of a completed and full report in this presentation.

#SHAREorg

SHARE

3. Basic Requests for z/OS Network Documentation

- UNIX
- SNA (VTAM) and Topology Diagram
- Enterprise Extender (EE) and Topology Diagram
- TCP/IP and Topology Diagram
- Policy Agent Policy Types (Security and Performance)

SHARE in San Francisco 2013

Request Documentation from Following Command Output at Designated Nodes*

- D OMVS,O
- D OMVS,P
- D OMVS,L
- Output from z/OS Health Checker
  - UNIX System Services?
  - z/OS?
  - z/OS Communications Server?
  - Other application-related messages?
- SYSLOGD configuration file (syslog.conf)

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation from Following Command Output at Designated Nodes*

- D NET,VTAMOPTS
- D NET,BFRUSE,BUFFER=SHORT
  - May need F NET,TNSTATS later
- D NET,CSM,OWNERID=ALL
- D NET,EE,LIST=DETAIL
- D NET,GRPREFS
- D NET,STATS,TYPE=VTAM
- D NET,E,ID=<names of Model Major Nodes – EE, RTP, VN, XCF)
- D NET,EEDIAG,TEST=YES [, ,<multiple variations>]
- D NET,E,ID=<XCA Major Node for Enterprise Extender>
- D NET,E,ID=<SWNet Major Nodes for Enterprise Extender>
- D NET,E,ID=<EE PUs inside SWNet Major Nodes>
- D NET,TOPO,<multiple variations>
- D NET,TGPS
- D NET,TRL
- D NET,E,ID=TRLEname

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation from Following Command Output at Designated Nodes*

- F RESOLVER,DISPLAY
- D TCPIP,,N,CONFIG
- D TCPIP,,N,HOME
- D TCPIP,,N,STATS
- D TCPIP,,N,DEV[,INTFNAME=interface name]
- D NET,TRL
- D NET,E,ID=TRLEname
- D TCPIP,,OSAINFO,INTFNAME=<name of QDIO OSA interface>
- OSA/SF “GET CONFIG” and “GET OAT”
- D TCPIP,,N,ROUTE,DETAIL
- D TCPIP,,OMP,OSPF,STATS
- D TCPIP,,OMP,OSPF,NBRS
  - May need additional OSPF command output*
- D TCPIP,,N,VIPADCFG,DETAIL
- D TCPIP,,SYSPLEX,VIPADYN
- D TCPIP,,N,VDPT,DETAIL
- D TCPIP,,N,VCRT,DETAIL
- Copy of pertinent TCP/IP Profiles and their INCLUDE files
- Copy of pertinent OMPROUTE Configuration Files

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation for Designated Nodes*

- Version and Release Level, Currency Level
- Topology Diagram
  - SNA
    - NETIDs
    - SSCPNAMEs
    - APPN[/HPR] Node Roles (NNs, CDSs, ENs, NNSs, LENs)
    - Other Nodes (NCP, Pus, etc.)
    - SNA Links and their Connectivity
    - If using Enterprise Extender (EE), indication of EE Endpoints and Roles

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation for Designated Nodes*

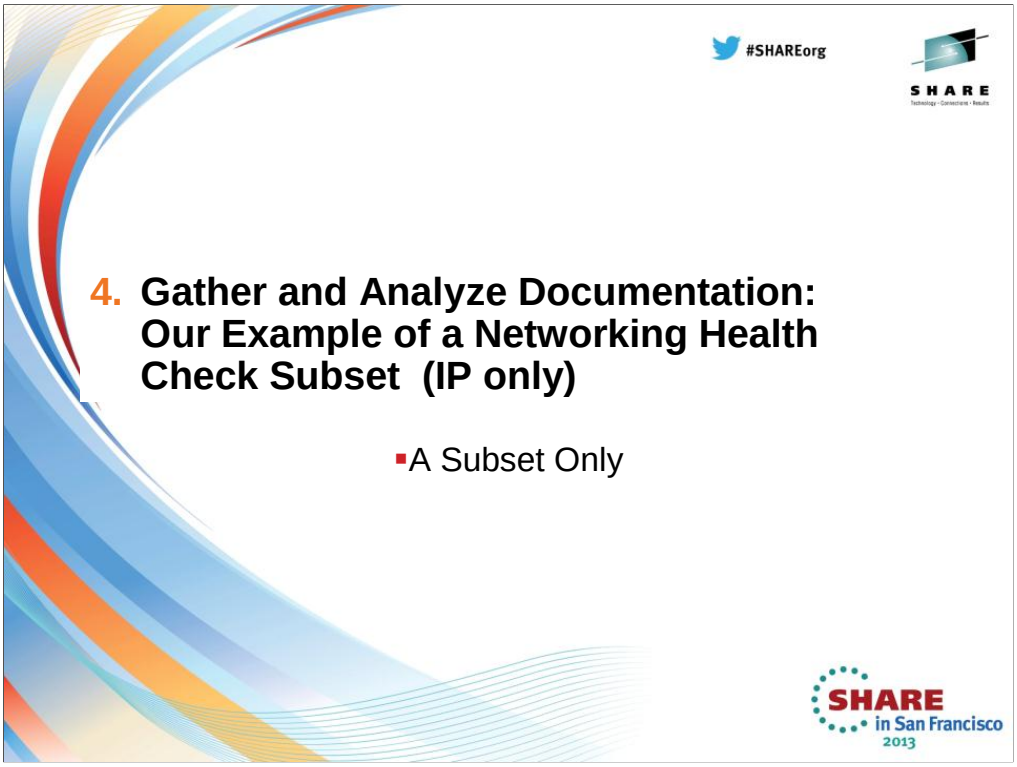
- Version and Release Level, Currency Level
- Topology Diagram
  - IP
    - Host Names
    - IP Networks and Subnets
    - Location of Routers, Switches, Firewalls
    - IP Interfaces and their Connectivity
    - If using Sysplex Distribution, indication of Primary SD(s) and Secondary SD(s) and the target applications for which responsible
    - If OSPF Dynamic Routing
      - *Indication of Area Types and Numbers*
      - *Indication of Area Border Routers, Autonomous System Boundary Routers*
- Definition Files
  - TCP/IP PROFILE and INCLUDE members
  - OMPROUTE Configuration File

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation for Designated Nodes*

- If pertinent to the Scope of the Health Check,
  - Description of Policy Agent Exploitation
    - Security Policies?
    - QoS Policies?
    - Policy Based Routing Policies?
  - Method of Configuring Policies
    - z/OS Communications Server Configuration Assistant on Windows?
    - z/OS Communications Server Configuration Assistant on z/OSMF?

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.



In the remainder of this presentation we show you only a few of the health check items that are evident from various sources that we collected.

Simple z/OS Networking Health Check Example

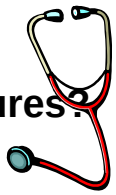
1. Define the Purpose or Expected Outcome of the Networking Health Check and its Scope
   - Our Example:
     - z/OS Image and its TCP Implementation
       - *Exploitation of Release Functions*
       - *Discover Potential Deviations from Best Practices*
       - *Uncover Potential Tuning Problems in Communications Server*
2. Define the Format of the Networking Health Check Report
3. List the documentation and tools required for the analysis and the personnel who will provide the documentation
   - Logical Network Diagram
   - z/OS Health Checker Output
     - Best Practices Checks
     - Migration Checks
   - Subset of Display Commands for TCP/IP and VTAM
4. Gather and analyze the documentation
5. Write the report

This is by no means a comprehensive health check as we must fit this into an hour-long presentation. We merely want to show you the type of information that can be gleaned from some important commands and displays that you may already be using.

#SHAREorg

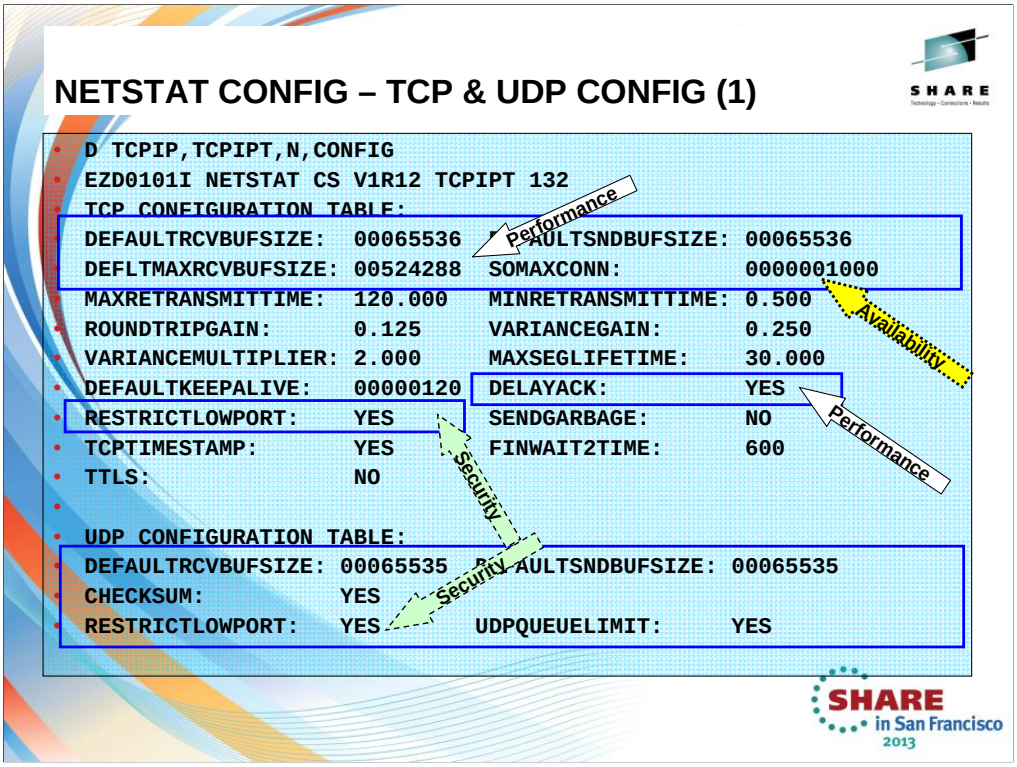
SHARE

Health Check Example:
Do we see any Performance Exposures?



- Evidence of Excessive Fragmentation?
- Evidence of Unstable Network?
- Evidence of Packet Rejects?
- Evidence of Retransmits?
- Evidence of Storage Problems?
- Failure to Exploit New Features?

SHARE in San Francisco 2013



TCPRCVBUFRSIZE *tcp_receive_buffer_size*

TCP receive buffer size between 256 and TCPMAXRCVBUFRSIZE. The default is 16384 (16K). This value is used as the default receive buffer size for those applications which do not explicitly set the buffer size using SETSOCKOPT().

TCPSENDBFRSIZE *tcp_send_buffer_size*

TCP send buffer size between 256 and 256K. The default is 16384 (16 K). This value is used as the default send buffer size for those applications that do not explicitly set the buffer size using SETSOCKOPT().

TCPMAXRCVBUFRSIZE *tcp_max_receive_buffer_size*

The TCP maximum receive buffer size is the maximum value an application can set as its receive buffer size using SETSOCKOPT(). The minimum acceptable value is the value coded on TCPRCVBUFRSIZE, the maximum is 512 K, and the default is 256 K. If you do not have large bandwidth interfaces, you can use this parameter to limit the receive buffer size that an application can set. IBM Health Checker for z/OS can be used to check whether the TCPMAXRCVBUFRSIZE value is sufficient to provide optimal support to the z/OS Communications Server FTP server. By default, it checks that TCPMAXRCVBUFRSIZE is at least 180 K.

SOMAXCONN statement

For applications that host many connections on a single listening socket – example is CICS – set this value to 1024 or higher.

Use the SOMAXCONN statement to specify the maximum number of connection requests queued for any listening socket. The maximum number of pending connection requests queued for any listening socket.The minimum value is 1, the maximum value is 2 147 483 647, and the default is 10.

DELAYACK – can be specified in TCP CONFIG, on PORT, on BEGINROUTES, on Gateway, in OMPROUTE Configuration

Delays transmission of acknowledgments when a packet is received with the PUSH bit on in the TCP header. YES is the default, but the behavior can be overridden by specifying the NODELAYACKS parameter on the TCP/IP stack PORT or PORTRANGE profile

statements for the port used by a TCP connection, or on any of the following statements used to configure the route used by a TCP Connection:

•The TCP/IP stack BEGINROUTES or GATEWAY profile statements

•The Policy Agent RouteTable statement

•The OMPROUTE configuration statements

RESTRICTLOWPORTS | UNRESTRICTLOWPORTS

Use RESTRICTLOWPORTS to increase system security.

When set, ports 1- 1 023 are reserved for users by the PORT and PORTRANGE statements. The RESTRICTLOWPORTS parameter is confirmed by the message:

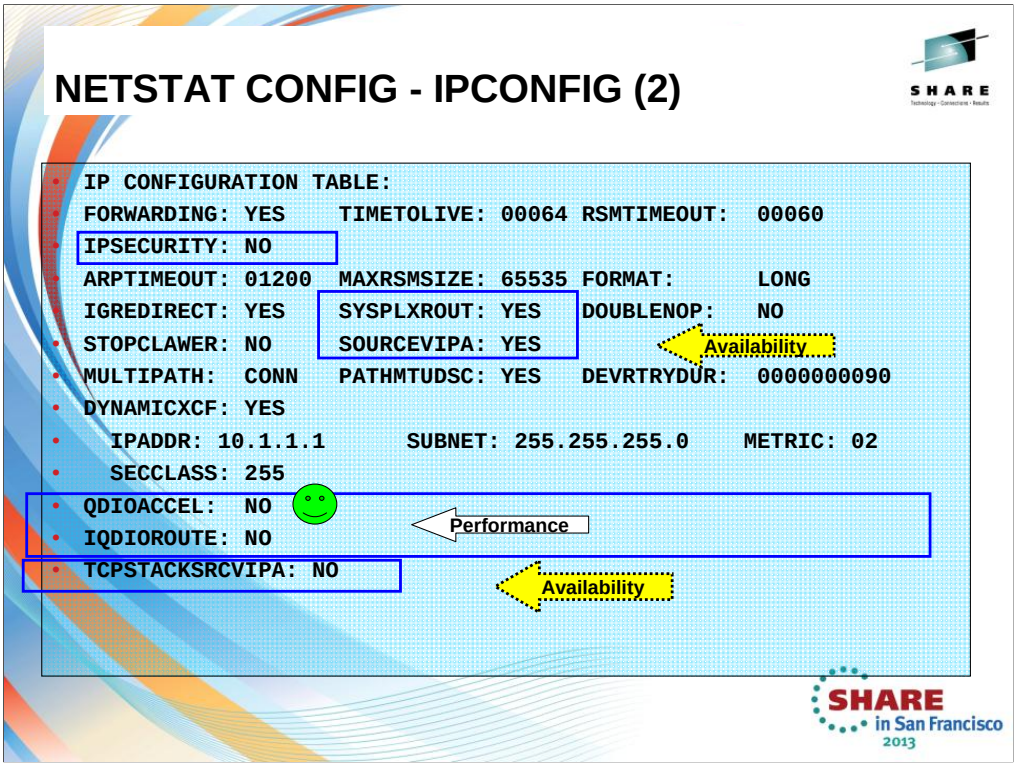
EZZ0338I TCP PORTS 1 THRU 1023 ARE RESERVED

Restriction: When RESTRICTLOWPORTS is specified, an application cannot obtain a port in the 1- 1 023 range unless it is authorized. Applications can be authorized to low ports in the following ways:

•Using PORT or PORTRANGE with the appropriate job name or a wildcard job name such as * or OMVS. If the SAF keyword is used on PORT or PORTRANGE, additional access restrictions can be imposed by a security product, such as RACF.

•APF authorized applications can access unreserved low ports.

•OMVS superuser (UID(0)) applications can access unreserved low ports.



IPSECURITY: NO means that IP Filtering or IPSec VPNs are not being implemented with this stack. If you were to implement QDIOACCEL or IQDIOROUTE, you must specify IPSECURITY of NO.

SYSPLEXROUT: Specifies that this TCP/IP host is part of an MVS sysplex domain.

SOURCEVIPA and TCPSTACKSRCVIPA

Requests that TCP/IP use the TCPSTACKSOURCEVIPA address (if specified) or the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams that do not have an explicit source address.

For outbound-initiated TCP connections or outbound UDP associations, SOURCEVIPA (with or without TCPSTACKSRCVIPA) is only one of the methods available to establish the Source IP field in the IP Header. Other means to establish the source ip field are available which are now usually recommended over the use of SOURCEVIPA. See the Appendix A for more information about source ip selection.

Knowing that SOURCEVIPA is set to YES and TCPSTACKSRCVIPA is set to no would lead you to examine the TCP/IP profile more closely for other options, like SRCIP block or the PORT BIND statement or the INTERFACE Statements. Or it could lead you to examine application configuration and flow patterns to determine why a particular Source IP is being selected for that application.

QDIOACCEL (QDIO Accelerator, HiperSockets Accelerator)

This might provide the opportunity to discuss the benefits of QDIOACCEL in V1R11 with the customer. It is preferred over IQDIOROUTE (introduced in V1R2).

This function allows a user to position a specific or single TCP/IP stack which has direct physical connectivity to the OSAs LANs as the HiperSockets router. Either QDIOACCEL or IQDIOROUTE can be specified, but not both. QDIOACCEL is the more flexible fo the two options since it can be used together with Sysplex Distributor and provides additional connectivity options:

Provides fast path IP forwarding for these DLC combinations:

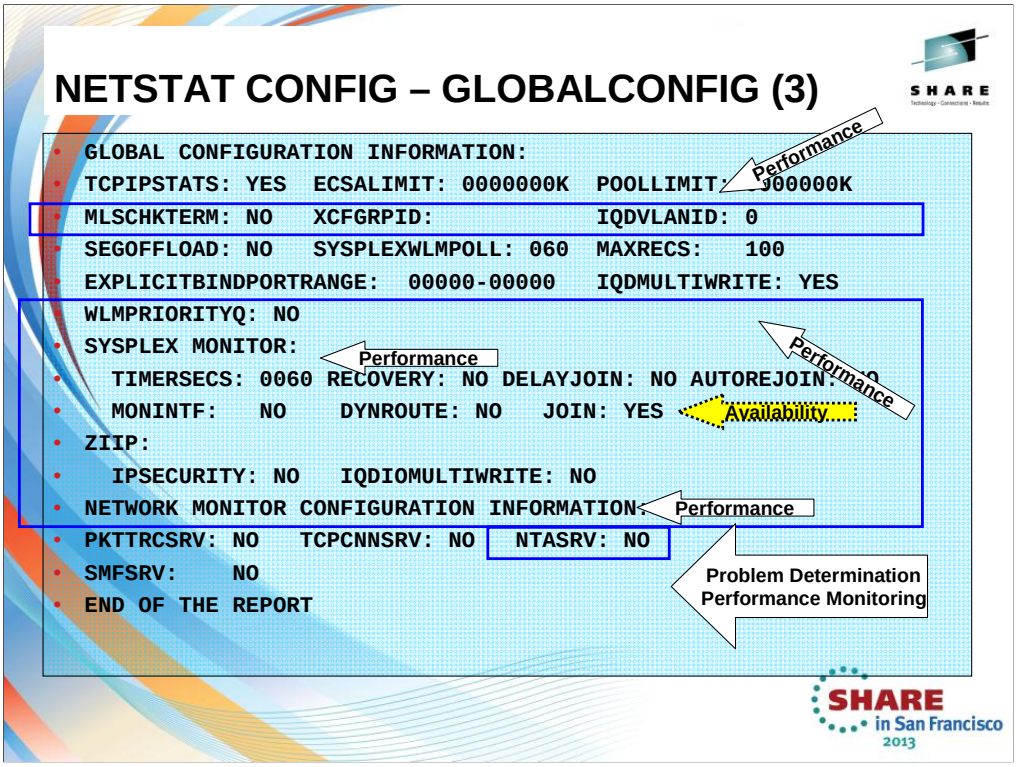
- Inbound OSA-E QDIO → Outbound OSA-E QDIO or HiperSockets
- Inbound HiperSockets → Outbound OSA-E QDIO or HiperSockets

Adds Sysplex Distributor (SD) acceleration

- Inbound packets over HiperSockets or OSA-E QDIO
- When SD gets to the target stack using either:
  - Dynamic XCF connectivity over HiperSockets
  - VIPAROUTE over OSA-E QDIO

Improves performance and reduces processor usage for such workloads..

When configured, the IP forwarding function is pushed down as close to the hardware [or to the lowest software DLC (Data Link Control)] layer as possible so that these packets do not have to be processed by the TCP/IP stack or address space. Therefore, valuable TCP/IP resources (storage and machine cycles) are not expended for purposes of routing and forwarding packets. Requires IP Forwarding; cannot run with IPSecurity or Optimized Latency Mode enabled.



TCPIPSTATS: ***If the customer has been having problems with a particular stack, these statistics can give valuable insight. It is also possible to capture the same statistics in SMF records if the values have been set.*** Yes means that GLOBALCONFIG TCPIPSTATISTICS was configured in the TCP/IP Profile. The TCPIP statistics field under Global Configuration Information indicates whether or not the TCP/IP stack will write statistics messages to the TCP/IP job log or to the output data set designated by the CFGPRINT JCL statement when TCP/IP is terminated. These counters include number of TCP retransmissions and the total number of TCP segments sent from the MVS TCP/IP system.

ECSALIMIT *escalimit* **K | M :** Specifies the maximum amount of extended common service area (ECSA) that TCP/IP can use. The default is no limit, and it can be specified as 0 K or 0 M. The minimum value for ECSALIMIT and POOLLIMIT is not allowed to be set to a value if the current storage in use would be greater than or equal to 80% of that value (for example, not allowed to set it such that there is an immediate storage shortage). ECSALIMIT ensures that TCP/IP does not overuse common storage. It is intended to improve system reliability by limiting TCP/IP's storage usage. The limit must account for peak storage usage during periods of high system activity or TCP/IP storage abends might occur. The limit does not include storage used by communications storage manager (CSM). CSM ECSA storage is managed independently of the TCP/IP ECSALIMIT. Specifying a nonzero ECSALIMIT enables warning messages EZZ4360I, EZZ4361I, and EZZ4362I to appear if a storage shortage occurs.

POOLLIMIT *pool_limit* **K | M:** Specifies the maximum amount of authorized private storage that TCP/IP can use within the TCP/IP address space. The default is no limit, and it can be specified as 0K or 0M. The minimum value for ECSALIMIT and POOLLIMIT is not allowed to be set to a value if the current storage in use would be greater than or equal to 80% of that value (for example, not allowed to set it such that there is an immediate storage shortage). POOLLIMIT ensures that TCP/IP does not overuse its authorized private storage. Most systems can use the default POOLLIMIT (no limit). Systems with limited paging capacity can use POOLLIMIT to help limit TCP/IP storage usage. If the limit is used, it must account for peak storage usage during periods of high system activity or TCP/IP storage abends might occur. POOLLIMIT can be higher than the REGION size on the TCP/IP start procedure because POOLLIMIT applies to authorized storage, whereas REGION applies to unauthorized storage. Specifying a nonzero POOLLIMIT enables warning messages EZZ4364I, EZZ4365I, and EZZ4366I to appear if a storage shortage occurs.

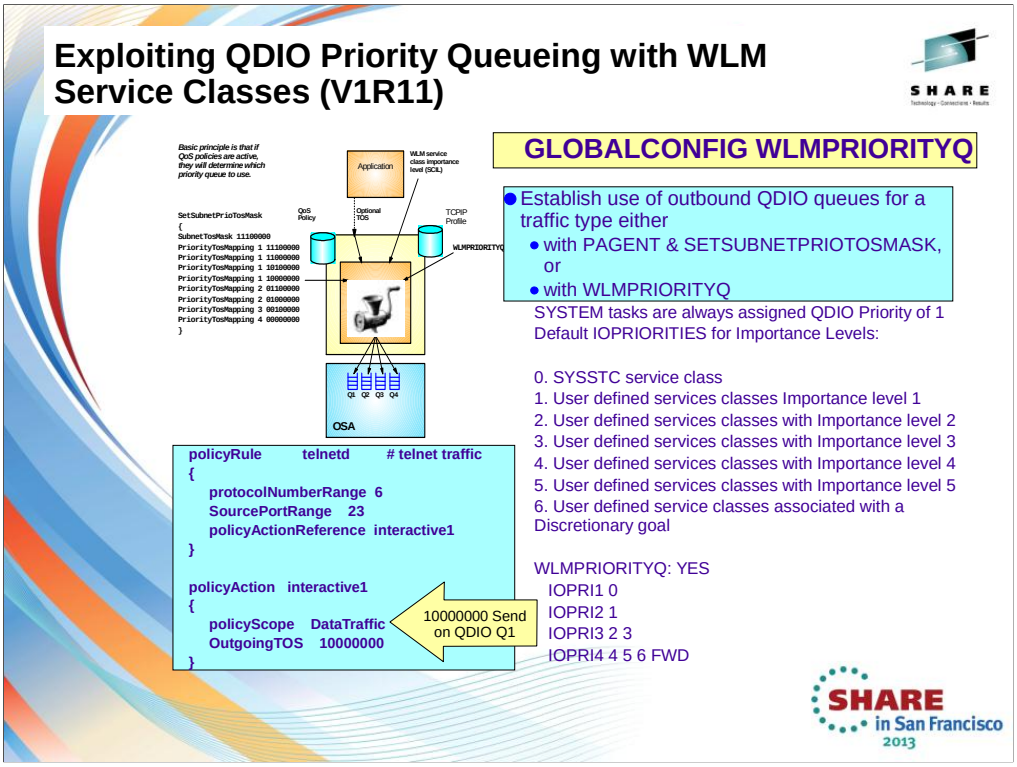
IQDMULTIWRITE | NOIQDMULTIWRITE : Specifies whether HiperSockets interfaces should use multiple write support. HiperSockets multiple write might reduce CPU usage and might provide a performance improvement for large outbound messages that are typically generated by traditional streaming workloads such as file transfer, and interactive web-based services workloads such as XML or SOAP. This parameter applies to all HiperSockets interfaces, including IUTIQDIO and IQDIOINTF6 interfaces created for Dynamic XCF.

WLMPRIORITYQ : Specifies whether OSA-Express QDIO write priority values should be assigned to packets associated with WorkLoad Manager service classes, and to forwarded packets. This enables the prioritization of outbound OSA-Express data using the WorkLoad Manager service class.

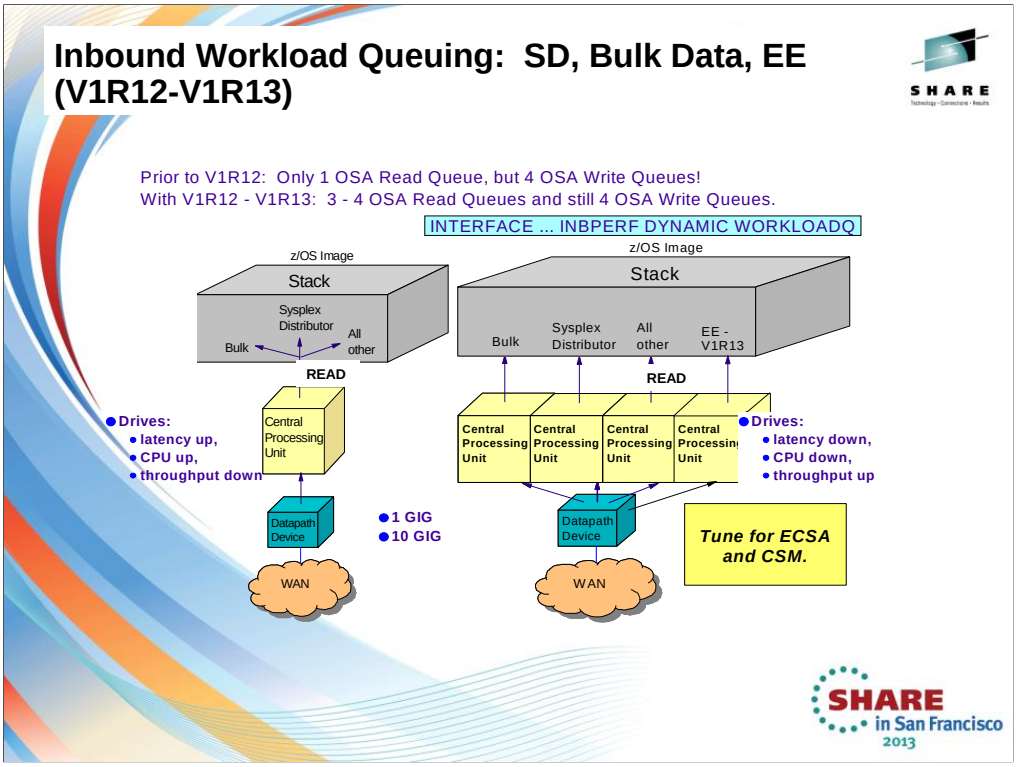
SYSPLEXMONITOR: ***If customer is in a Sysplex and using Sysplex Distribution, these parameters – if enabled -- would betray whether or not he is subject to a loss of high availability.*** Specifies SYSPLEXMONITOR subparameters to configure the operation of the sysplex autonomics function.

ZIIP: Specifies subparameters that control whether TCP/IP displaces CPU cycles onto a System z® Integrated Information Processor (zIIP). **IPSECURITY | NOIPSECURITY** Specifies whether TCP/IP should displace CPU cycles for IPSec workload to a zIIP. **NOIQDIOMULTIWRITE | IQDIOMULTIWRITE** Specifies whether TCP/IP should displace CPU cycles for large outbound TCP messages that are typically created by traditional streaming work loads such as file transfer, and interactive web-based service workloads such as XML or SOAP. The TCP/IP outbound message must be at 32KB in length before the write processing is off-loaded to an available zIIP specialty engine.

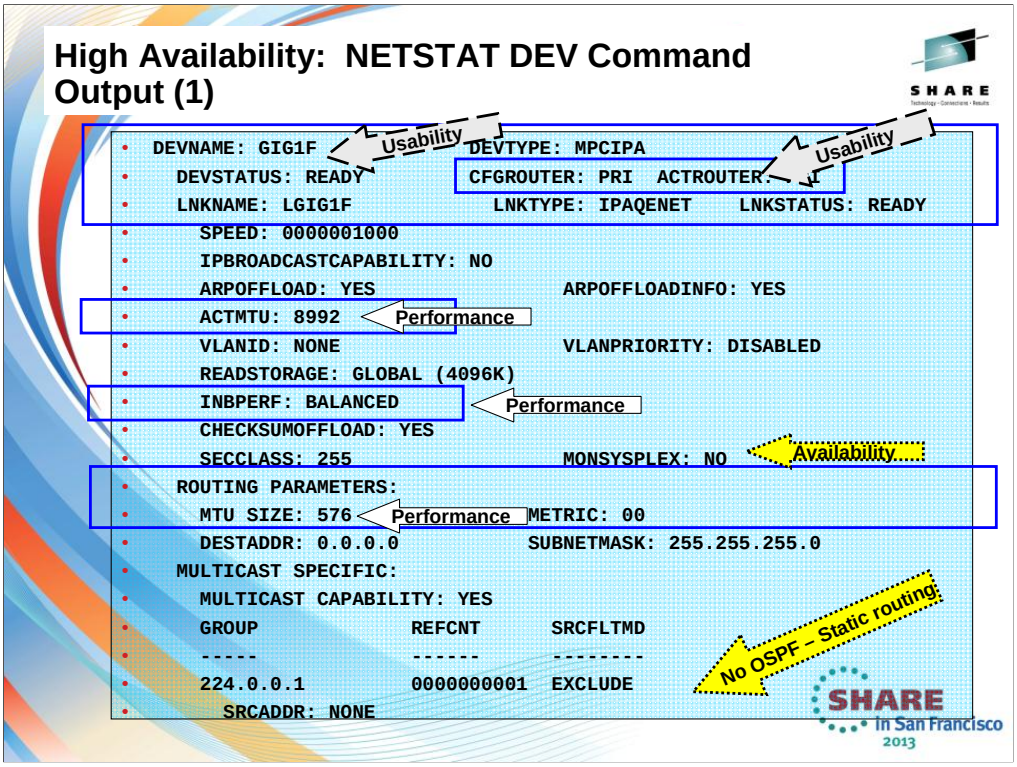
NETMONITOR statement: Use the NETMONITOR PROFILE.TCPIP statement to activate or deactivate selected real-time TCP/IP network management interfaces (NMI). **NTATRCSERVICE | NONTATRCSERVICE:** ***Customer may not be using the Network Monitor Interface, but the examination of these options provides the opportunity to discuss the implementation of OSAENTA, which should be encouraged.*** Specifies the behavior of the real-time TCP/IP OSAENTA trace service (SYSTCPOT). Enables the OSAENTA trace service function to run on this TCP/IP stack. This service enables network management applications to access trace data that is collected for all OSAENTA traces. Access control should be provided for this service. However, note that in the rest of this PROFILE, there is **no OSAENTA** statement at all.



1. The QDIO OSAs are implemented with four internal queues. Outbound Data traffic is distributed over these four queues based upon a Quality of Service (QoS) definition that established Types of Service in the "Precedence Bits" of the IP Header. Most applications fail to establish these precedence bits; Enterprise Extender is an exception to this. Other applications are assigned precedence bits based upon a QoS policy that you may have defined with z/OSMF or with z/OS Configuration Assistant GUI and then installed with Policy Agent into the TCP/IP stack.
2. The first visual in the upper left shows you the four QDIO queues and shows you how different Types of Service are mapped within Policy Agent to distributed traffic outbound over each of the four queues.
3. The visual below the aforementioned visual shows you a sample policy that might be used to assign a high priority (TOS of 10000000) to Telnet traffic and therefore cause it to be dispatched on QDIO OSA Queue #1.
4. In general most shops do little to nothing to prioritize their OSA-Express outbound data, missing any benefits the prioritization provides
5. Beginning with V1R11, it is now possible to allow outbound traffic to be assigned precedence bits based upon WLM priorities and "Service Class Importance Levels."
    1. Since the WLM service classes should already be assigned to the jobs, all that needs to be done is to give the stack 'permission' to use it for prioritization.
    2. Defaults are provided that should give a good distribution of work across the priority queues.
    3. If QoS or the application has assigned an IPv4 ToS/IPv6 Traffic Class then enabling this function will only affect those packets assigned a ToS/Traffic Class value of zeros.
    4. Enterprise Extender always assigns a non-zero ToS/Traffic Class so unless it is changed to zero by QoS, Enterprise Extender traffic is not affected.
6. Therefore, with V1R11, all you need to do is enable the use of WLM Service Class importance Level as a means of assigning traffic to the QDIO queues. You do this by enabling:
    1. GLOBALCONFIG WLMPRIORITYQ (WLMPRIORITYQ: YES on a Netstat Config indicates that WLMPRIORITYQ is enabled) WLMPRIORITYQ specifies that OSA-Express QDIO write priority values should be assigned to packets associated with WorkLoad Manager service class values and to forwarded packets.
        1. If you do not want to accept the default queueing, you may override it with a parameter of IOPRIn. Below you see the default settings for IOPRIn when you sepcify WLM:PRIORITYQ by itself on the IPCONFIG statement.
            1. IOPRI1 0 OSA-Express priority queue 1 is used for packets from jobs with a control value 0 (SYSSTC)
            2. IOPRI2 1 OSA-Express priority queue 2 is used for packets from jobs with a control value 1 (services classes with Importance level 1)
            3. IOPRI3 2 3 OSA-Express priority queue 3 is used for packets from jobs with control values 2 and 3 (services classes with Importance levels 2 and 3)
            4. IOPRI4 4 5 6 FWD OSA-Express priority queue 4 is used for packets from jobs with control values 4, 5, and 6 (services classes with Importance levels 4 and 5 and discretionary) as are all non-accelerated forwarded packets
7. Points to remember:.
    1. WLMPRIORITYQ has little effect unless there is enough traffic to cause contention for the OSA-Express resources
    2. WLMPRIORITYQ has no effect unless packet IPv4 ToS/IPv6 Traffic Class is zeros. This is typically the case if you have not defined a network QoS policy



1. Prior to z/OS V1R12, all inbound QDIO traffic is received on a single read queue regardless of the data type. The maximum amount of storage available for inbound traffic is limited to the read buffer size (64K read SBALs) times the maximum number of read buffers (126). A single process is used to package the data, queue it, and schedule the TCP/IP stack to process it. This same process also performs acceleration functions, such as Sysplex Distributor connection routing accelerator.
2. The TCP/IP stack must separate the traffic types to be forwarded to the appropriate stack component that will process them. For these reasons, z/OS Communications Server is becoming the bottleneck as OSA-Express3 10GbE nears line speed. z/OS Communications Server is injecting latency and increasing processor utilization. This can impede scalability.
3. Under the pre-V1R12 z/OS Communications Server model, another QDIO input process will eventually be driven, and another TCP/IP stack thread, thus allowing multiple threads to process the one inbound read queue. However, this is only done when the OSA detects the host is now "falling behind" using the QDIO interrupt threshold algorithm.
4. z/OS Communications Server is becoming the bottleneck as OSA nears 10GbE line speed, this behavior Injects latency, increases processor utilization, and impedes scalability. For BULK Data, multiple processes are used for inbound traffic when data is accumulating on the read queue. This can cause bulk data packets for a single TCP connection to arrive at the TCP layer out of order. Each time the TCP layer on the receiving side sees out of order data, it transmits a duplicate ACK. Overall, throughput is harmed for bulk data traffic.
5. With z/OS Communications Server V1R12 and V1R13, inbound traffic separation is supported using multiple read queues: Bulk, Sysplex Distributor, Enterprise Extender (V1R13), and All Other. TCP/IP will register with OSA which traffic to be received on each read queue. The OSA-Express Data Router function routes traffic to the correct queue.
6. Each read queue can be serviced by a separate process. The primary input queue is used for general traffic. One or more ancillary input queues (AIQs) are used for specific traffic types. Sysplex distributor, EE (V1R13), and bulk data traffic is presorted by OSA and routed to z/OS Communications Server on unique AIQs. All other traffic is routed to z/OS Communications Server on the primary input queue. z/OS Communications Server can now process sysplex distributor, bulk data, EE (V1R13) and other traffic concurrently and independently.
7. The primary queue is always assigned Queue Identifier 1 (QID 1). Each ancillary queue is assigned a Queue Identifier based on when it gets internally registered.
8. The supported traffic types are streaming bulk data and sysplex distributor. Examples of bulk data traffic are FTP, TSM, NFS, and TDMF.
9. Both IP versions (IPv4, IPv6) are supported for all types of traffic.
    1. With bulk data traffic separated onto its own read queue, TCP/IP will service the bulk data queue from a single processor. This solves the out-of-order delivery issue – there are no more race conditions.
    2. With sysplex distributor traffic separated onto its own read queue, it can be efficiently accelerated or presented to the target application. The same applies to Enterprise Extender traffic.
    3. All other traffic is processed simultaneous with the bulk data and sysplex distributor traffic
    4. The dynamic LAN idle timer is updated independently for each read queue. This ensures the most efficient processing of inbound traffic based on the traffic type.
10. The QDIO inbound workload queuing function is enabled with the INBPERF DYNAMIC WORKLOADQ setting on IPAQENET and IPAQENET6 INTERFACE statements. WORKLOADQ is not supported for INBPERF DYNAMIC on IPAQENET LINK statements. WORKLOADQ does require the VMAC on the INTERFACE definition, but you can allow just a dynamically generated value for VMAC.
11. Each ancillary queue will consume:

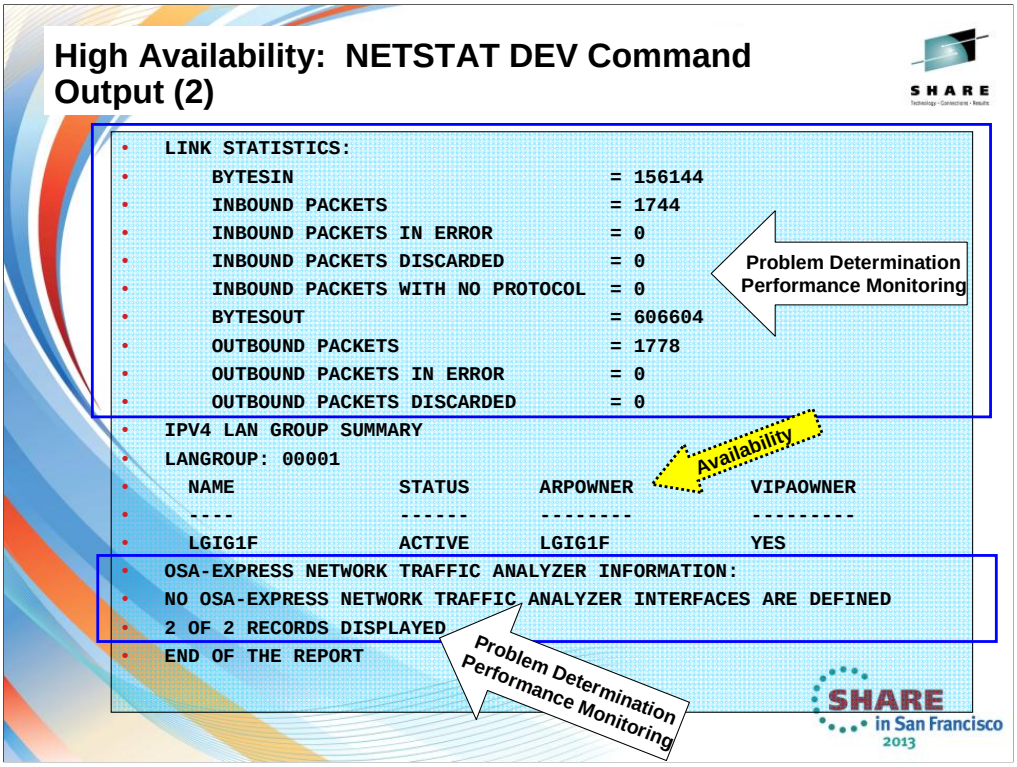


This display shows that the definition for this QDIO IPv4 interface is still using the older definition style: Device and Link. It also shows that, although the OSA port is capable of an MTU size of 8992, what is really being used is only an MTU of 576 bytes … the default. In other words, it reveals that neither the definition nor the routing definition has been optimized. It would be better to convert this definition to the INTERFACE definition. With the INTERFACE definition you can even improve the INBPERF by coding for inbound workload queueing on the INBPERF DYNAMIC statement.

The routing MTU shows that the routing definitions are taking a poor default for MTU: 576. This observation would lead to a re-examination of the routing definitions.

MONSYSPLEX Specifies whether or not sysplex autonomics should monitor the link's or interface's status to determine whether a TCP/IP stack should join the sysplex or even leave it.

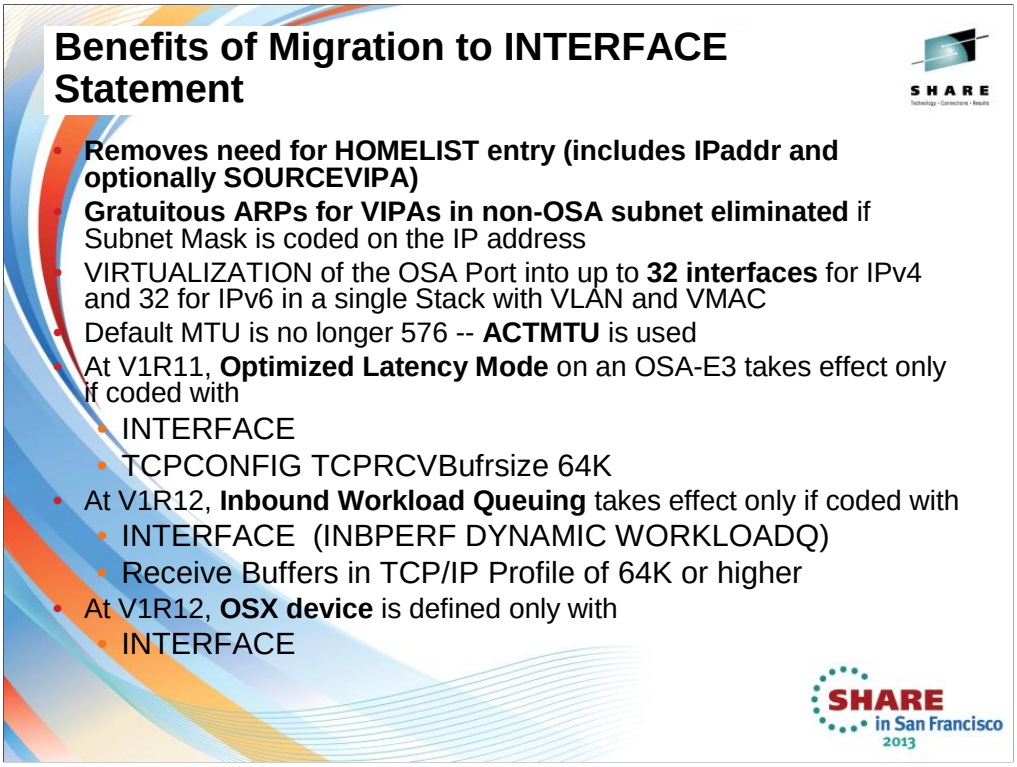
The Multicast address of 224.0.0.1 shows that the link is multicast-capable, but it has not been defined as an OSPF node. Otherwise it would display other multicast addresses to indicate membership in an OSPF area.



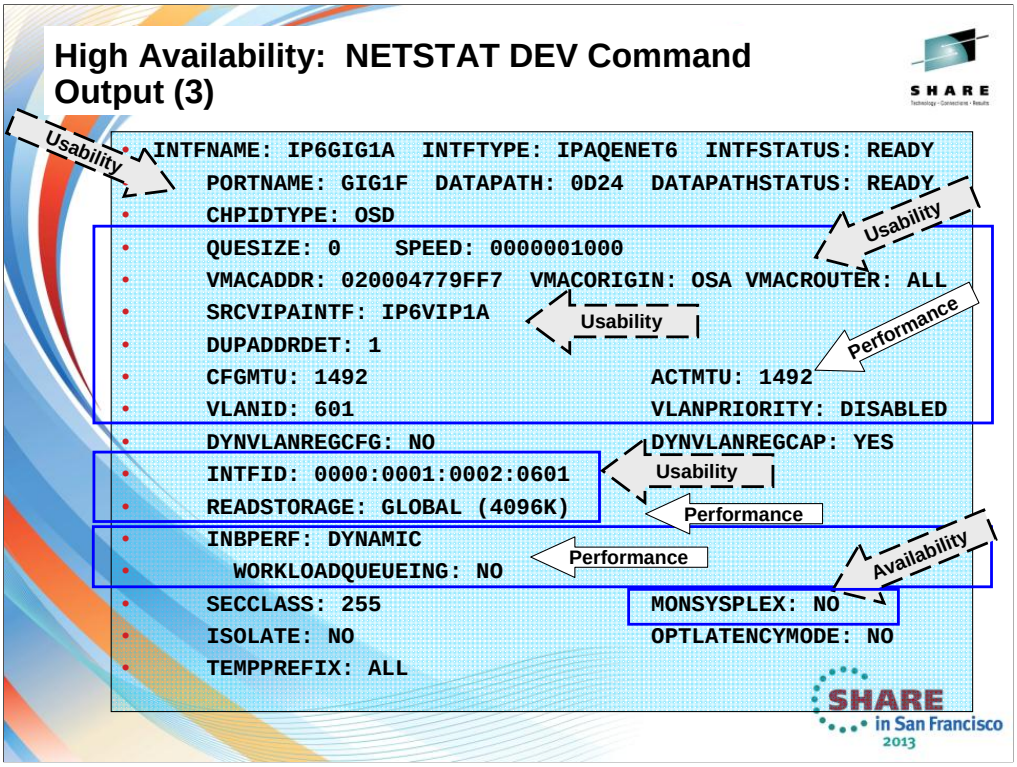
The older style definition of an interface with DEVICE and LINK still reveals the Link Statistics that can be used for PD and for Performance Monitoring and still allows you to implement OSAENTA analysis with OSA-EXPRESS Network Traffic Analyzer. However, note that OSAENTA is not implemented here.

Use the OSAENTA statement to control the OSA-Express Network Traffic Analyzer (OEAENTA) tracing facility in the OSA-Express adapter. You can use this statement to select frames as candidates for tracing and subsequent analysis; OSAENTA traces are recorded externally using the TRACE command.

With this display you can also determine if the installation is exploiting ARP takeover for providing high availability to multiple interfaces attached to the same subnet. (See the LANGROUP and the number of links or interfaces listed below the group.) In this case, high availability is not being provided by ARP takeover but rather by another method such as dynamic routing and a robust topology design. (Or, further investigation might reveal that there has been no consideration of a high availability design, although this is unlikely.)



1. If you define the OSA using DEVICE/LINK statements, then the stack will inform OSA to perform ARP processing for all VIPAs in the home list which can result in numerous unnecessary gratuitous ARPs for VIPAs in an interface takeover scenario.
2. However, if you use the IPv4 INTERFACE statement for IPAQENET, you can control this VIPA ARP processing by configuring a subnet mask for the OSA. If you specify a non-0 num_mask_bits value on the IPADDR parameter of the INTERFACE statement, then the stack will inform OSA to only perform ARP processing for a VIPA if the VIPA is configured in the same subnet as the OSA (as defined by the resulting subnet mask).
3. This is an example of multiple VLAN definitions with two INTERFACE statements for IPAQENET. Each statement defines an IPv4 interface associated with the same OSA-Express port NSQDIO1. Each specifies a subnet mask of 24 bits (‘FFFFFF00”x) and defines a unique subnet.
4. The statements contain different VLAN IDs, and each requests that OSA generate a virtual MAC address (and defaults to ROUTEALL). Each statement specifies the link_name of a static VIPA for the source VIPA function.
5. Because so many definitions that used to reside in the HOME list and in BSDROUTINGPARMS are now included in the INTERFACE definition, it is easier to add and delete interfaces dynamically without having to modify the HOME LIST>
    1. If there is any mismatch between OMPROUTE values (MTU and SUBNET MASK), error messages are generated and the values from OMPROUTE are used.
        1. EZZ8163I stack_name MTU value stack_val for interface differs from omproute_procname MTU value omproute_val
        2. EZZ8164I stack_name subnet mask value stack_val for interface differs from omproute_procname subnet mask value omproute_val



This visual shows you the output from NETSTAT DEV for an IPv6 QDIO interface that was coded with the INTERFACE statement; IPv6 must be coded with INTERFACE, but even IPv4 QDIO is eligible for this type of coding and is preferred over the use of the DEVICE/LINK combination. With the INTERFACE definition you can use the VMAC definitions together with VMAC ROUTALL or ROUTELCL to avoid having to code PRI/SECROUTER.

With the use of VMACs, VLANs, and Inbound Workload Queuing on QDIO and iQDIO (HiperSockets) interfaces you should pay attention to storage consumption.

Each OSA-Express QDIO and HiperSockets interface requires fixed storage for read processing (which is allocated by VTAM through VTAM start options of QDIOSTG and IQDIOSTG). VTAM start options (QDIOSTG, IQDIOSTG), display and modify commands are provided to adjust amount of storage used; Defaults settings should be appropriate in most cases. Storage adjustment may be necessary when many OSA adapters are used, when there are multiple TCP/IP stacks per LPAR or many VM 2nd-level guests. If you define a large number of these interfaces (for example, by configuring multiple VLANs to one or more OSA-Express features), then you need to consider how much fixed storage your configuration requires.

For information about how much fixed storage VTAM allocates by default for each OSA-Express QDIO and HiperSockets interface, how to control the amount of this storage allocation using the VTAM QDIOSTG start option (for OSA-Express QDIO) and the VTAM IQDIOSTG start option (for HiperSockets), and considerations for the IVTPRM00 parmlib member, see z/OS Communications Server: SNA Resource Definition Reference.

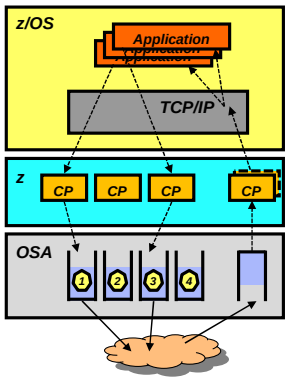
You can also override the global QDIOSTG or IQDIOSTG value and control the amount of fixed storage for a specific OSA-Express QDIO or HiperSockets interface by using the READSTORAGE parameter on the LINK and INTERFACE statements.

INBPERF and WORKLOADQUEUEING: Consult next two pages for information on how changes in V1R12 and V1R13 provide performance enhancements.

MONSYSPLEX Specifies whether or not sysplex autonomics should monitor the link's or interface's status to determine whether a TCP/IP stack should join the sysplex or even leave it.

Pre V1R12 OSA inbound/outbound processing overview

- Queued Direct IO (QDIO) uses multiple write queues for outbound traffic separation
  - Outbound traffic is separated by priority (policy or WLM)
  - Multiple CPs can be used to manage the write queues
- QDIO uses only one read queue
  - All inbound traffic is received on the single read queue
  - Multiple CPs are used only when data is accumulating on the queue
    - During bursts of inbound data
  - A single process for initial interrupt and read buffer packaging
- ***Performance problems observed for bulk inbound traffic:***
  - *Multiple processes run when data is accumulating on the read queue*
  - *Out-of-order packets at TCP for a single inbound TCP connection*
  - *TCP transmits a duplicate ACK every time it sees out-of-order data*
  - *Sending side enters fast retransmit recovery*



TCP/IP stack performs inbound data separation (instead of the OSA as occurs with V1R13 and higher)

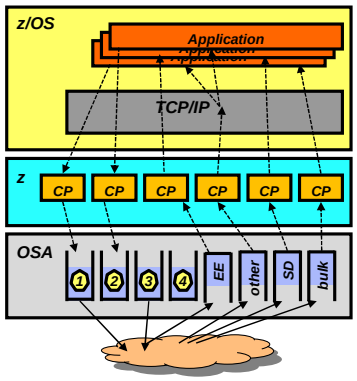
- Sysplex distributor traffic
- Bulk inbound, such as FTP
- IPv4/IPv6
- EE traffic
- Etc.

z/OS Communications Server is becoming the bottleneck as OSA nears 10GbE line speed

- Inject latency
- Increase processor utilization
- Impede scalability

OSA Inbound Workload Queueing (IWQ): Improved performance for mixed traffic patterns

- Allow inbound QDIO traffic separation by supporting multiple read queues
  - "Register" with OSA which traffic goes to which queue
  - OSA-Express Data Router function routes to the correct queue
- Each input queue can be serviced by a separate process
  - Primary input queue for general traffic
  - One or more ancillary input queues (AIQs) for specific traffic types
  - Dynamic LAN idle timer updated per queue



- ***TCP/IP defines, assigns traffic to queues dynamically based on local IP address and port***
- ***Bulk traffic***
  - ***Application sets send or receive buffer to at least 180K, Registered per connection (5-tuple)***
- ***SD traffic***
  - ***Based on active VIPADISTRIBUTE definitions***

Supported traffic types (z/OS V1R12)

Bulk data traffic queue

Serviced from a single process - eliminates the out of order delivery issue

Sysplex distributor traffic queue

SD traffic efficiently accelerated or presented to target application

All other traffic not backed up behind bulk data or SD traffic

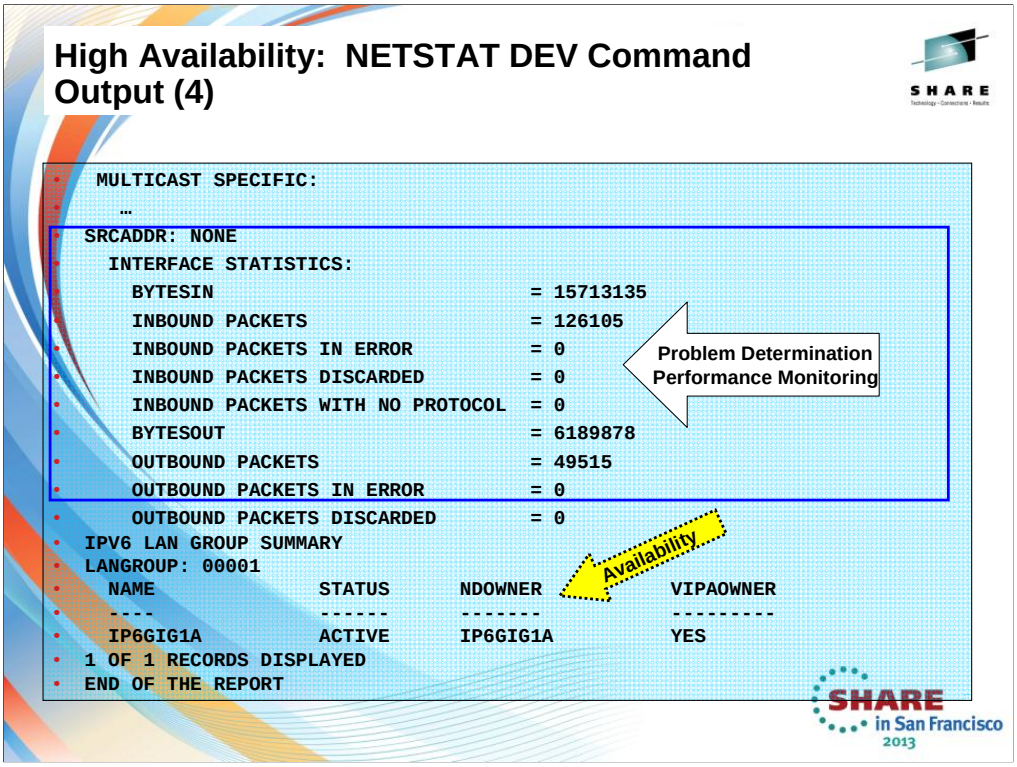
New for z/OS V1R13 – Unique inbound queue for Enterprise Extender traffic

Improved performance for EE traffic

Supported on OSA-Express3 and new OSA-Express4S (CHPID type OSD or OSX)

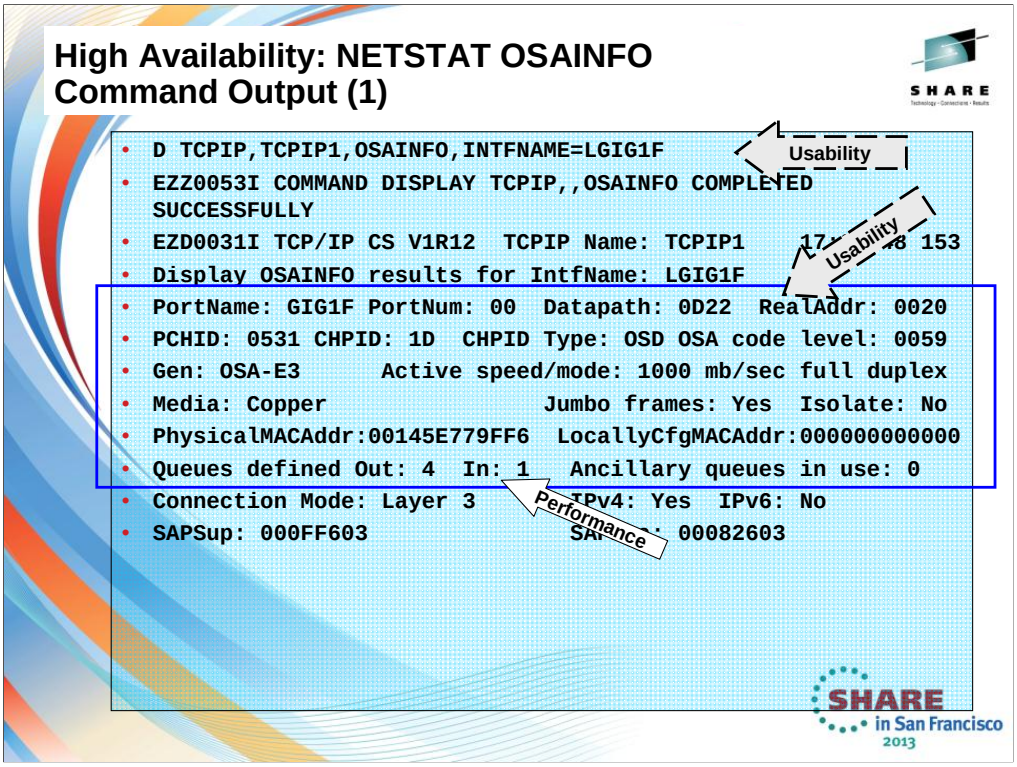
Significant performance improvement for mixed workloads/traffic patterns – for more details see:

http://www-01.ibm.com/common/ssi/rep_ca/6/897/ENUS111-136/ENUS111-136.PDF



The output from an interface coded with the INTERFACE statement reveals the Link Statistics that can be used for PD and for Performance Monitoring.

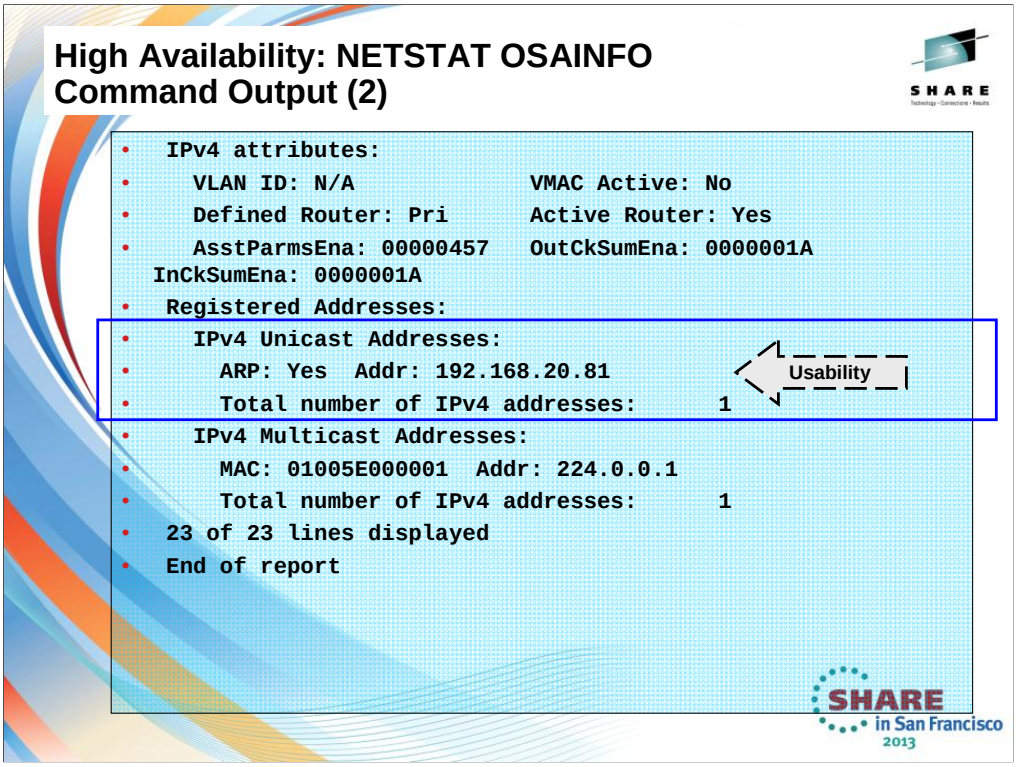
With this display you can also determine if the installation is exploiting ARP takeover for providing high availability to multiple interfaces attached to the same subnet. (See the LANGROUP and the number of links or interfaces listed below the group.) In this case, high availability is not being provided by ARP takeover but rather by another method such as dynamic routing and a robust topology design. (Or, further investigation might reveal that there has been no consideration of a high availability design, although this is unlikely.)



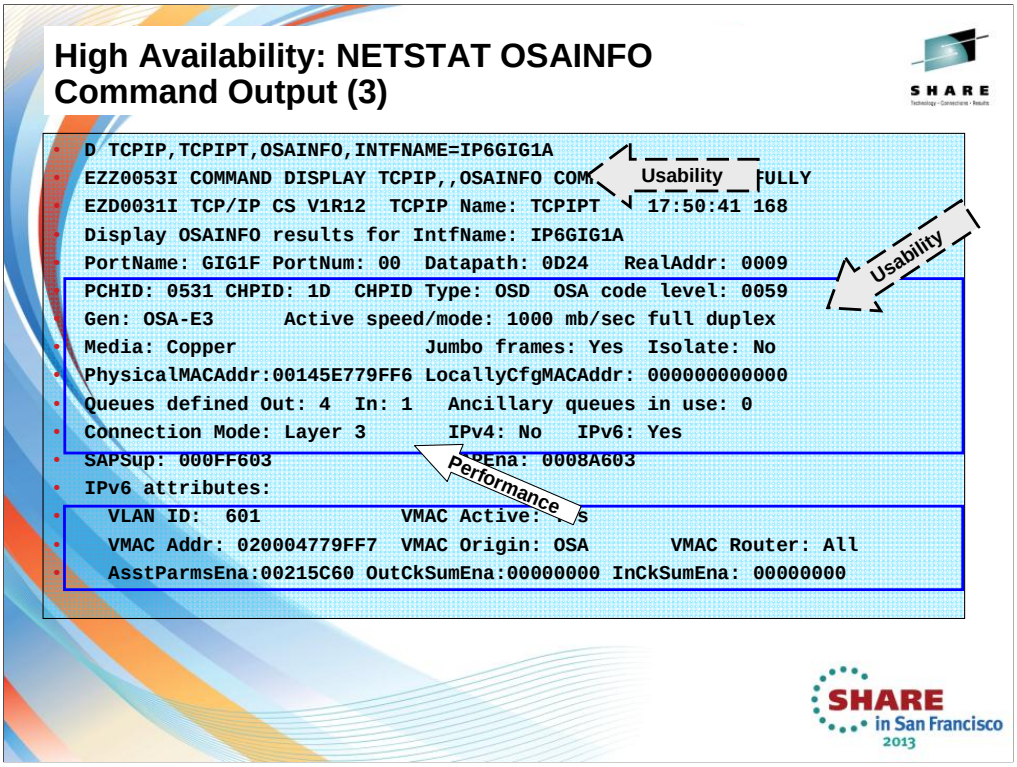
Use the DISPLAY TCPIP,,OSAINFO command to retrieve information for active IPAQENET and IPAQENET6 interfaces. An interface represents a single datapath device of an OSA-Express feature. The information is retrieved directly from the OSA-Express feature. The OSA-Express must be of the appropriate type and at the appropriate MCL level.

This display reveals the relationship between the physical location of the OSA port and the coding in VTAM TRLEs and TCP/IP. For service levels we also see the OSA code level without having to display the VTAM TRLE to obtain the same information about code level.

QDIO inbound workload queueing routing variables – This output is for an interface defined with DEVICE/LINK; as a result, INBOUND Workload Queueing is not available on the INBPERF DYNAMIC statement. This fact explains why there is still only one inbound queue displayed. And so with this you see another reason to convert from DEVICE/LINK definitions to INTERFACE definitions for an IPv4 interface. If QDIO inbound workload queueing is in effect for the interface, this section contains the routing variables for the ancillary input queues. Routing variables identify which inbound packets are to be presented on an ancillary input queue.



The display here does show you the IP address associated with the DEVICE/LINK. However, it does not show you the full list of registered addresses on this OSA port. To display all registered addresses you would still need to implement OSA/SF and issue a “get OAT.”

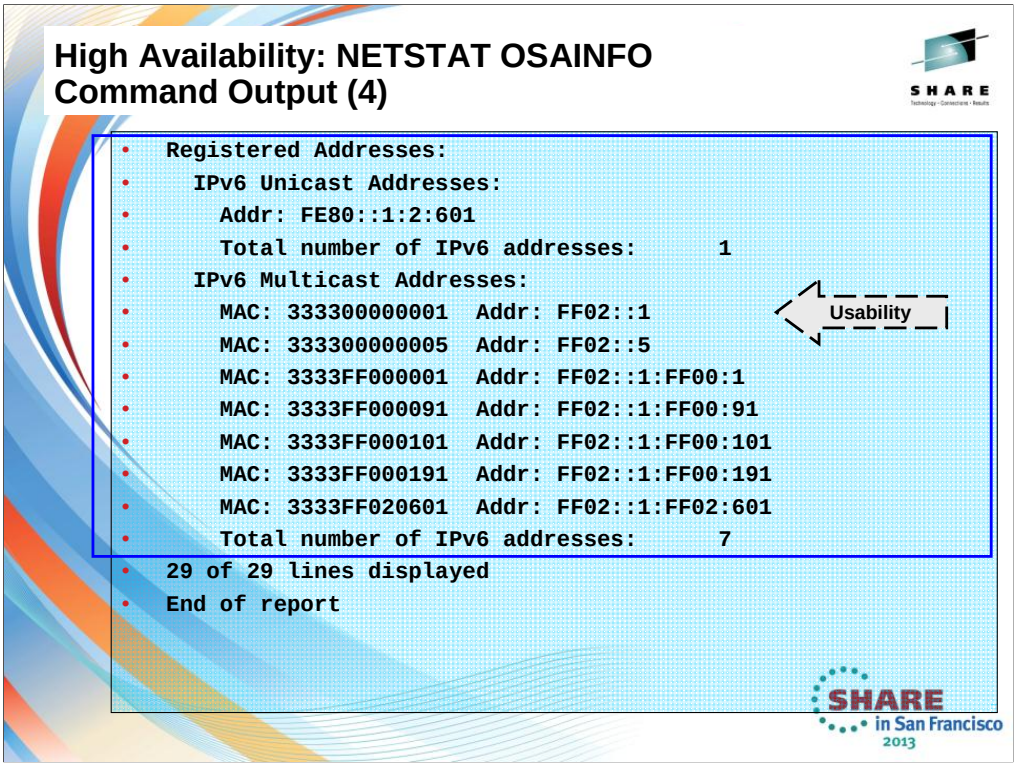


This is the output for an OSA interface coded with the INTERFACE statement.

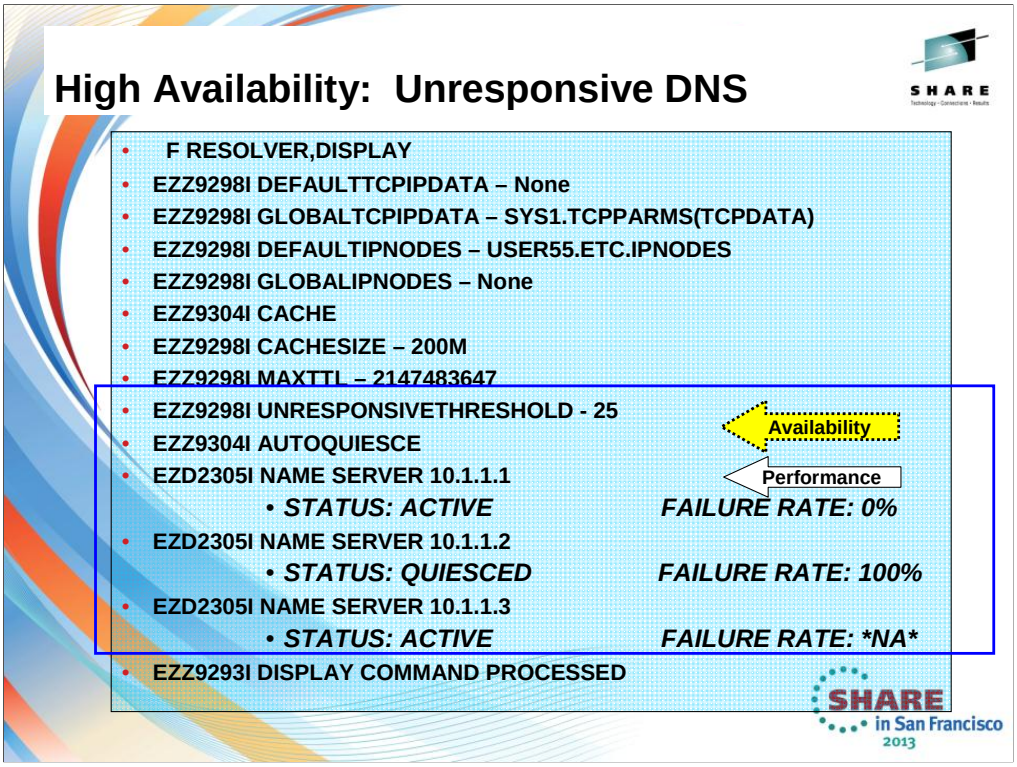
This display reveals the relationship between the physical location of the OSA port and the coding in VTAM TRLEs and TCP/IP. For service levels we also see the OSA code level without having to display the VTAM TRLE to obtain the same information about code level.

If QDIO inbound workload queueing is in effect for the interface, this section contains the routing variables for the ancillary input queues. (Requirement: Receive Buffers in TCP/IP Profile of 64K or higher.) Routing variables identify which inbound packets are to be presented on an ancillary input queue.

QDIO inbound workload queueing routing variables –INBOUND Workload Queueing is available on the INBPERF DYNAMIC statement for an INTERFACE statement. However, notice how this device is not exploiting the performance benefits of INBPERF DYNAMIC WORKLOADQ. A report on this to the customer might encourage the installation to add the inbound queueing enhancement to this definitions.



The display here shows you the Link Local Address associated with the IPv6 INTERFACE. However, it does not show you the full list of registered addresses on this OSA port except for the IPv6 Multicast addresses.



EZZ9298I UNRESPONSIVETHRESHOLD - 25

In z/OS V1R12, the resolver monitors name servers for responsiveness to queries. You specify what "unresponsive" means by coding a threshold failure rate in the resolver setup file A global TCPIP.DATA file is required.

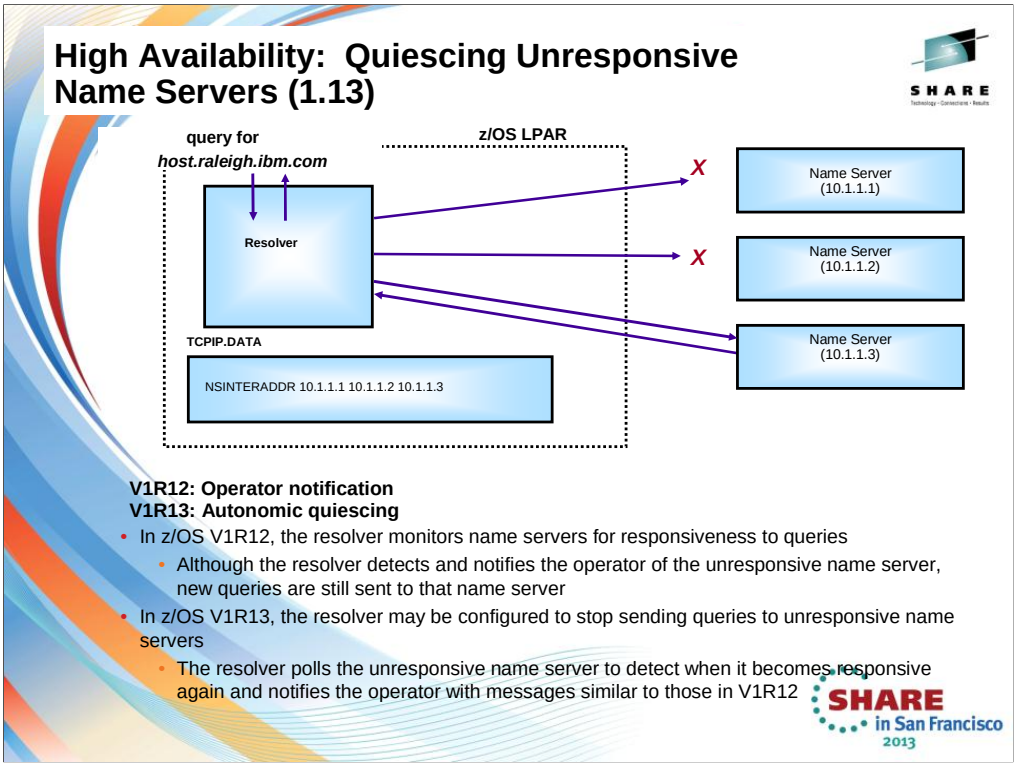
Network operator notification when a name server becomes unresponsive

- Responsiveness is calculated on a sliding 5-minute window of statistics
- Although the resolver detected the unresponsive name server, new queries were still sent to that name server

EZZ9304I AUTOQUIESCE

In z/OS V1R13, the resolver may be configured to stop sending queries to unresponsive name servers

- The resolver polls the unresponsive name server to detect when it becomes responsive again
- Operator notified of condition using messages similar to those used in V1R12



V1R12: Operator notification

V1R13: Autonomic quiescing -- The autonomic quiescing function must be explicitly enabled in the resolver setup file.

In z/OS V1R12, the resolver monitors name servers for responsiveness to queries. You specify what "unresponsive" means by coding a threshold failure rate in the resolver setup file A global TCPIP.DATA file is required.

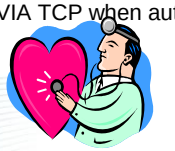
- Network operator notification when a name server becomes unresponsive
- Responsiveness is calculated on a sliding 5-minute window of statistics
- Although the resolver detected the unresponsive name server, new queries were still sent to that name server

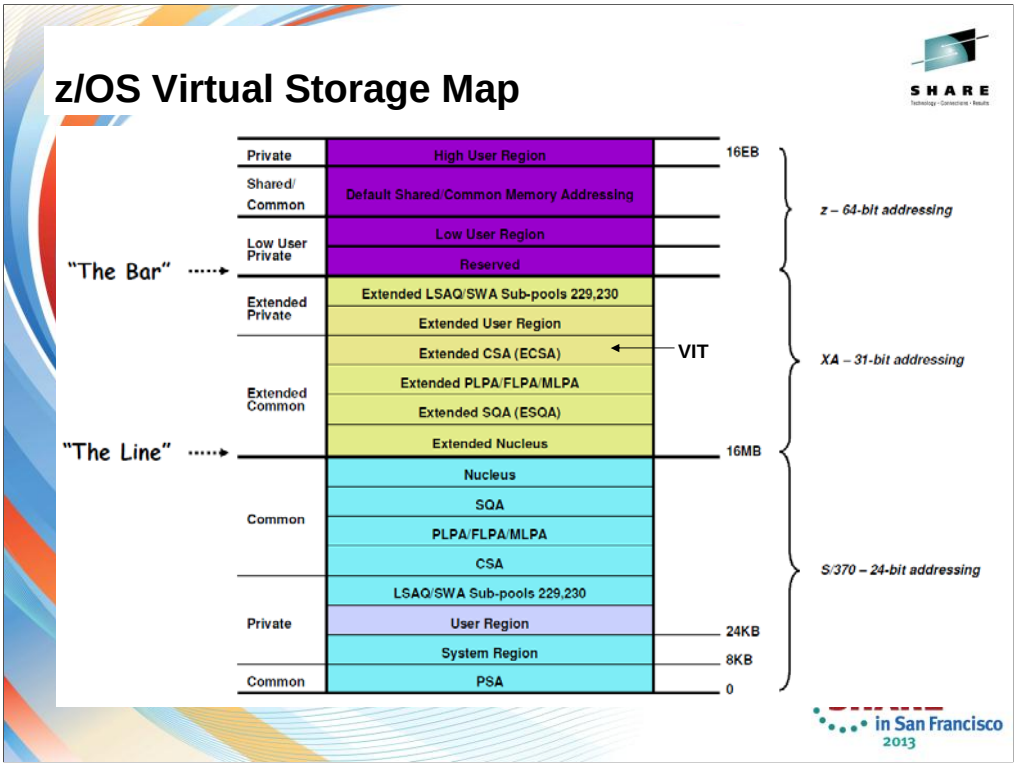
In z/OS V1R13, the resolver may be configured to stop sending queries to unresponsive name servers

- The resolver polls the unresponsive name server to detect when it becomes responsive again
- Operator notified of condition using messages similar to those used in V1R12

Health Checker Detection of Resolver Coding

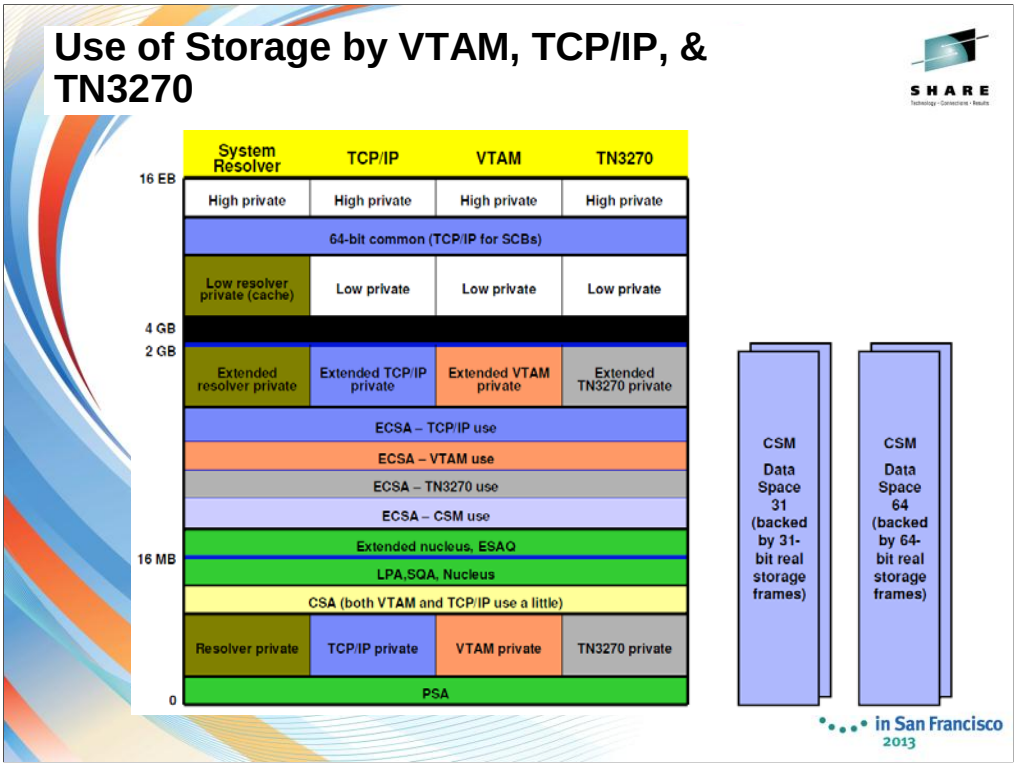
- At V1R13 three checks were added to Health Checker for the autonomic quiescing function:
  - **CSRES_AUTOQ_GLOBALTCPIPDATA**
    - Checks that you have coded the GLOBALTCPIPDATA setup statement if AUTOQUIESCE is coded on the UNRESPONSIVETHRESHOLD setup statement
  - **CSRES_AUTOQ_TIMEOUT**
    - Checks, by default, if you have specified a value greater than five (seconds) for RESOLVERTIMEOUT when autonomic quiescing is enabled
    - You can change the check to have a different value than five seconds if your installation uses a larger timeout value
  - **CSRES_AUTOQ_RESOLVEVIA**
    - Checks if you have specified RESOLVEVIA TCP when autonomic quiescing is enabled
- These checks are performed when the resolver is started and when a MODIFY RESOLVER,REFRESH command is issued





TCP/IP, VTAM, CSM and TN3270 all use pieces of the ECSA storage.

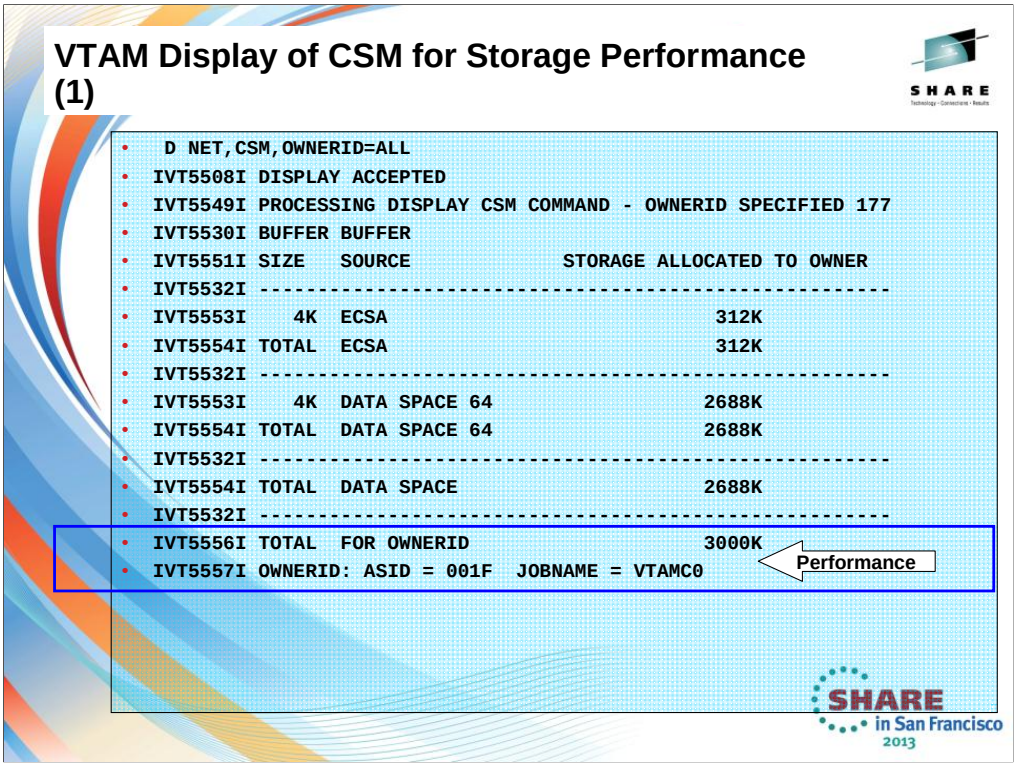
Prior to V1R13, the VIT storage is taken out of ECSA.



This slide provides an overview of the Communication Server's virtual storage model. Of main interest is obviously the use of common storage, since common storage in general is a restricted resource governed by various installation defined limits. VTAM and TCP/IP obtain ECSA storage. Most of this ECSA storage is generally reported as belonging to the MVS Master address space and not TCP/IP or VTAM. The reason for this is the storage is obtained as being persistent. In general, all Communications Server storage is obtained in Key 6 – an RMF monitor II virtual storage report can be examined for how much storage is owned by key 6.

Prior to z/OS V1R13 the VTAM Internal Trace uses ECSA

CSM is a communications server buffer pool manager, that maintains the buffers in a combination of ECSA and data space virtual storage. The best way to monitor CSM storage availability and usage is through the D NET,CSM and D NET,CSMUSE commands.



The DISPLAY CSM command yields the following information:

•Amount of storage allocated to each pool

•Amount of storage allocated to each user of the pool

•If OWNERID=ALL is specified, the cumulative storage allocated to each user across all pools

•If OWNERID is not specified, the highest level of fixed storage obtained since the last DISPLAY CSM command was issued without the OWNERID parameter.

•If OWNERID is not specified, the highest level of fixed storage obtained since the IPL.

•If OWNERID is not specified, the highest level of ECSA obtained since the last DISPLAY CSM command was issued without the OWNERID parameter.

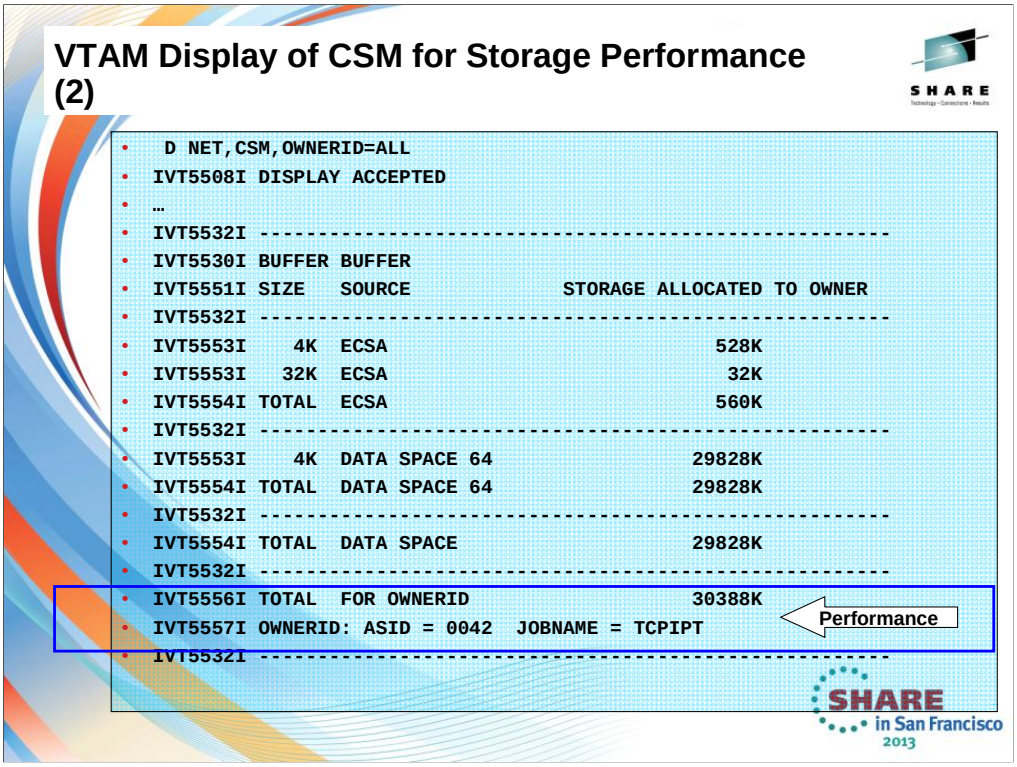
•If OWNERID is not specified, the highest level of ECSA obtained since the IPL.

•If OWNERID is not specified, the names of CSM data spaces.

•The maximum amount of fixed and ECSA storage that can be allocated by CSM and current values of fixed and ECSA storage.

Use the DISPLAY CSM command to identify a user of the pool that is consuming inordinate amounts of storage. This can happen if an application fails to free buffers that it obtained from CSM. The report of storage allocated to a user is based on the value of the user's *owner_ID* parameter. This is the OWNERID

operand on the DISPLAY CSM command. CSM uses the application's address space identifier (ASID) as the OWNERID.



The DISPLAY CSM command yields the following information:

•Amount of storage allocated to each pool

•Amount of storage allocated to each user of the pool

•If OWNERID=ALL is specified, the cumulative storage allocated to each user across all pools

•If OWNERID is not specified, the highest level of fixed storage obtained since the last DISPLAY CSM command was issued without the OWNERID parameter.

•If OWNERID is not specified, the highest level of fixed storage obtained since the IPL.

•If OWNERID is not specified, the highest level of ECSA obtained since the last DISPLAY CSM command was issued without the OWNERID parameter.

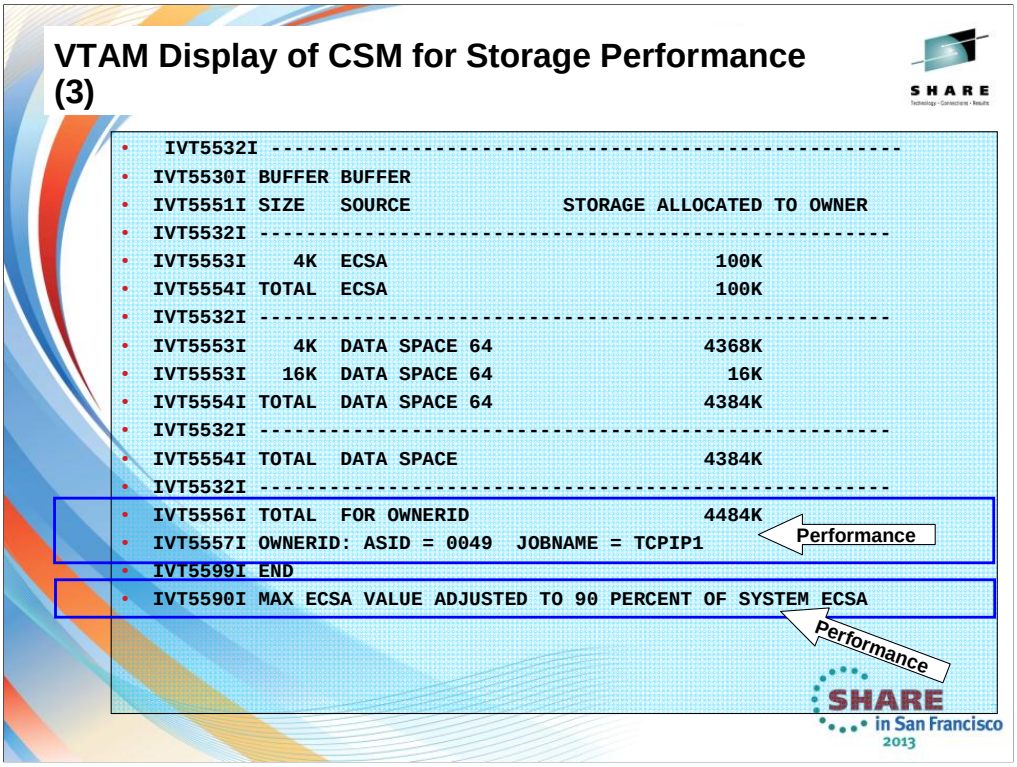
•If OWNERID is not specified, the highest level of ECSA obtained since the IPL.

•If OWNERID is not specified, the names of CSM data spaces.

•The maximum amount of fixed and ECSA storage that can be allocated by CSM and current values of fixed and ECSA storage.

Use the DISPLAY CSM command to identify a user of the pool that is consuming inordinate amounts of storage. This can happen if an application fails to free buffers that it obtained from CSM. The report of storage allocated to a user is based on the value of the user's *owner_ID* parameter. This is the OWNERID

operand on the DISPLAY CSM command. CSM uses the application's address space identifier (ASID) as the OWNERID.



The DISPLAY CSM command yields the following information:

•Amount of storage allocated to each pool

•Amount of storage allocated to each user of the pool

•If OWNERID=ALL is specified, the cumulative storage allocated to each user across all pools

•If OWNERID is not specified, the highest level of fixed storage obtained since the last DISPLAY CSM command was issued without the OWNERID parameter.

•If OWNERID is not specified, the highest level of fixed storage obtained since the IPL.

•If OWNERID is not specified, the highest level of ECSA obtained since the last DISPLAY CSM command was issued without the OWNERID parameter.

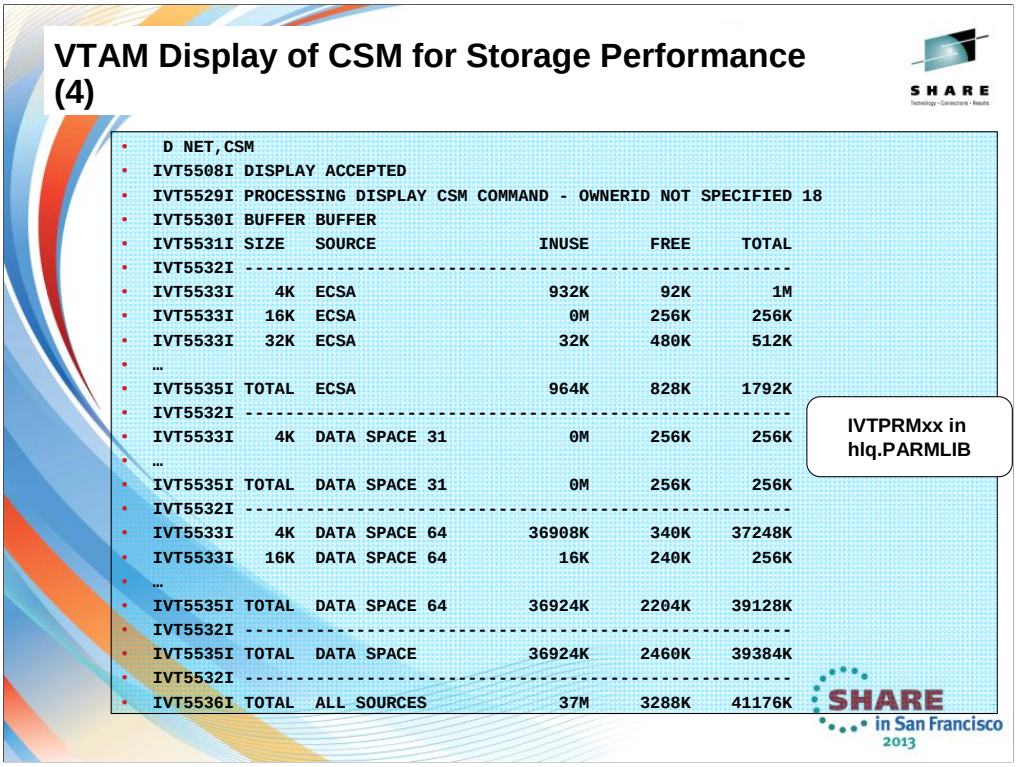
•If OWNERID is not specified, the highest level of ECSA obtained since the IPL.

•If OWNERID is not specified, the names of CSM data spaces.

•The maximum amount of fixed and ECSA storage that can be allocated by CSM and current values of fixed and ECSA storage.

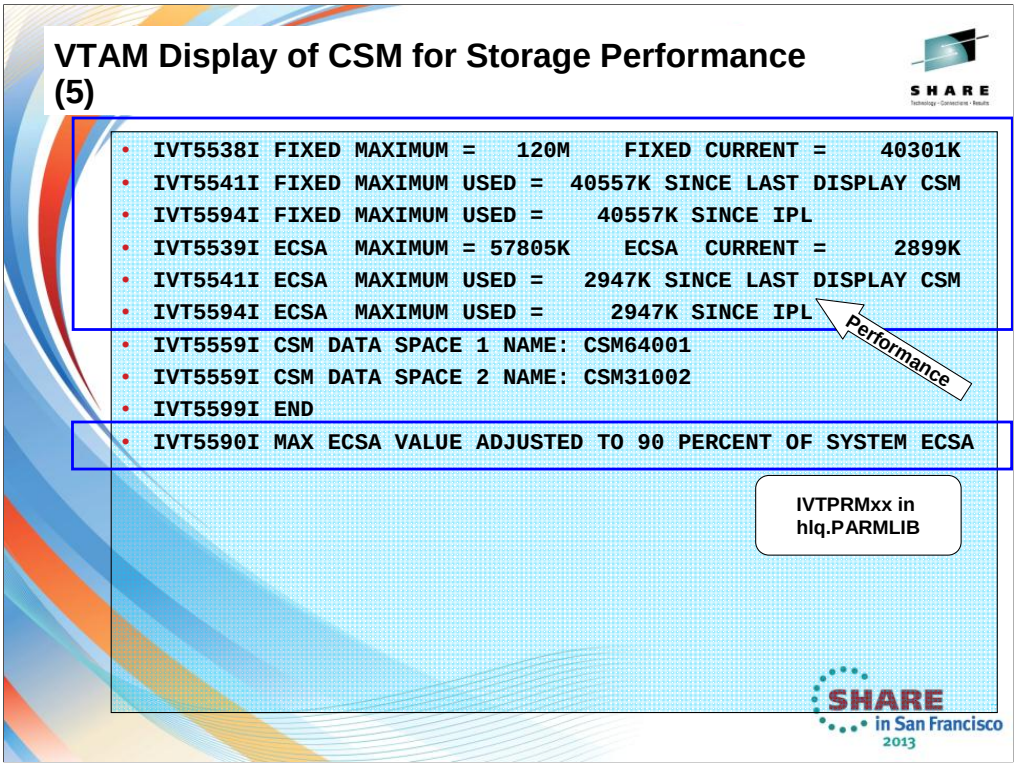
Use the DISPLAY CSM command to identify a user of the pool that is consuming inordinate amounts of storage. This can happen if an application fails to free buffers that it obtained from CSM. The report of storage allocated to a user is based on the value of the user's *owner_ID* parameter. This is the OWNERID

operand on the DISPLAY CSM command. CSM uses the application's address space identifier (ASID) as the OWNERID.



The critical level storage usage is 90% or higher of ECSA MAX or FIXED MAX values specified in CSM parmlib IVTPRM00. The normal level storage usage is 80% or below of ECSA MAX or FIXED MAX values.

CSM issues some messages when CSM storage limits are at a critical level or exceeded. In this case, the system operator can issue the MODIFY CSM command to increase the amount of fixed or ECSA storage available for CSM.



The critical level storage usage is 90% or higher of ECSA MAX or FIXED MAX values specified in CSM parmlib IVTPRM00. The normal level storage usage is 80% or below of ECSA MAX or FIXED MAX values.

CSM issues some messages when CSM storage limits are at a critical level or exceeded. In this case, the system operator can issue the MODIFY CSM command to increase the amount of fixed or ECSA storage available for CSM.

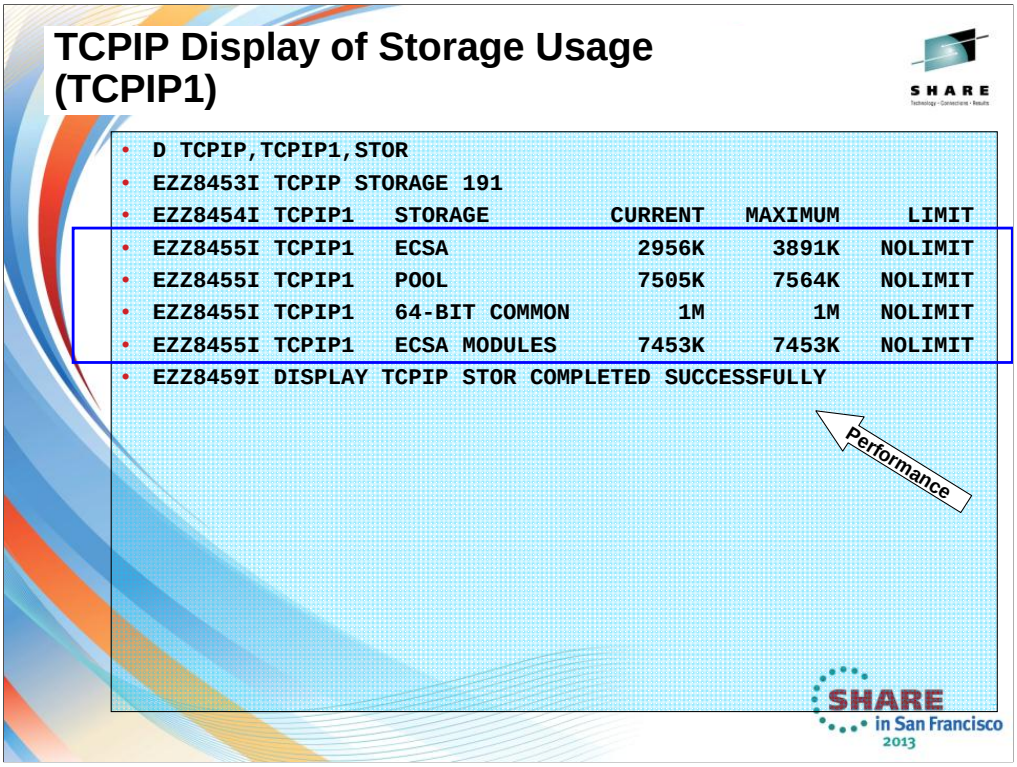
IVT5590I MAX ECSA VALUE ADJUSTED TO 90 PERCENT OF SYSTEM ECSA

Explanation: This message is issued if the MAX ECSA value from the CSM PARMLIB member IVTPRM00 is higher than 90% of the system ECSA value or the MAX ECSA value specified on the MODIFY CSM command is higher than 90% of the SYSTEM ECSA value during the following:

•CSM initialization.

•MODIFY CSM command processing.

•DISPLAY CSM command processing.



The Display TCPIP,,STOR command shows storage usage information for TCP/IP or the TN3270E Telnet server

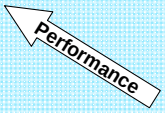
– Mix of 31-bit and 64-bit storage

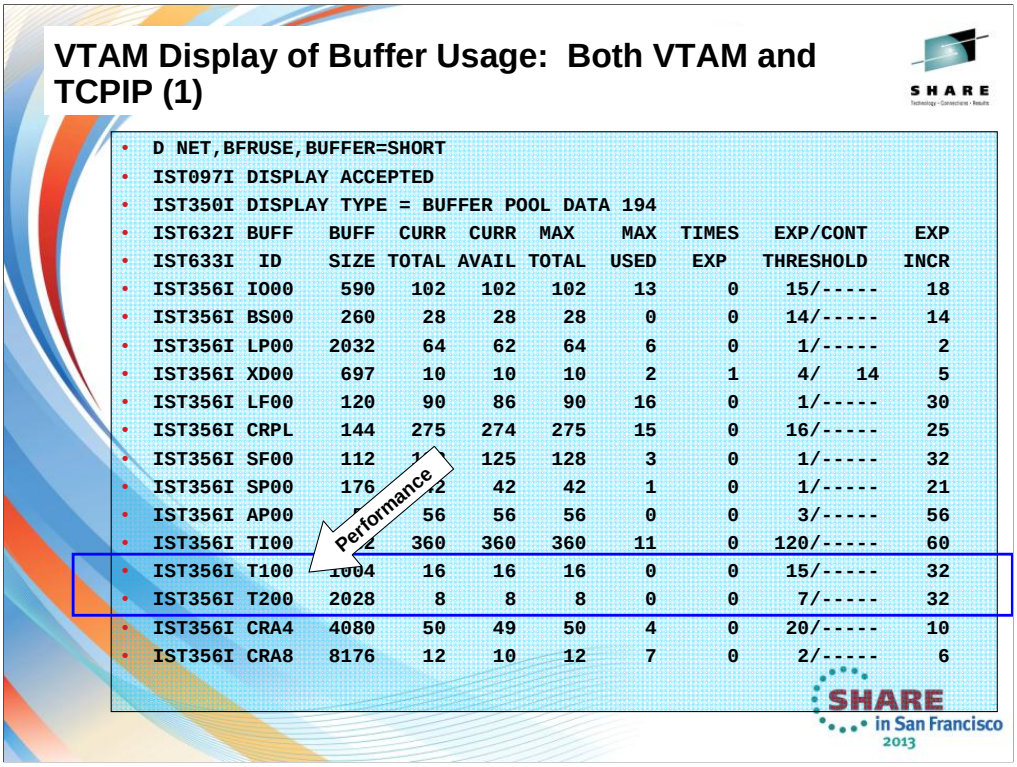
– Prior to V1R13 lacks trace storage information

– TCP/IP example show above – TN3270E output very similar

TCPIP Display of Storage Usage (TCPIPT)

```
D TCPIP,TCPIPT,STOR
EZZ8453I TCPIP STORAGE 189
EZZ8454I TCPIPT   STORAGE          CURRENT    MAXIMUM     LIMIT
EZZ8455I TCPIPT   ECSA               3006K      4054K   NOLIMIT
EZZ8455I TCPIPT   POOL               9076K      9133K   NOLIMIT
EZZ8455I TCPIPT   64-BIT COMMON         1M         1M   NOLIMIT
EZZ8455I TCPIPT   ECSA MODULES       7453K      7453K   NOLIMIT
EZZ8459I DISPLAY TCPIP STOR COMPLETED SUCCESSFULLY
```





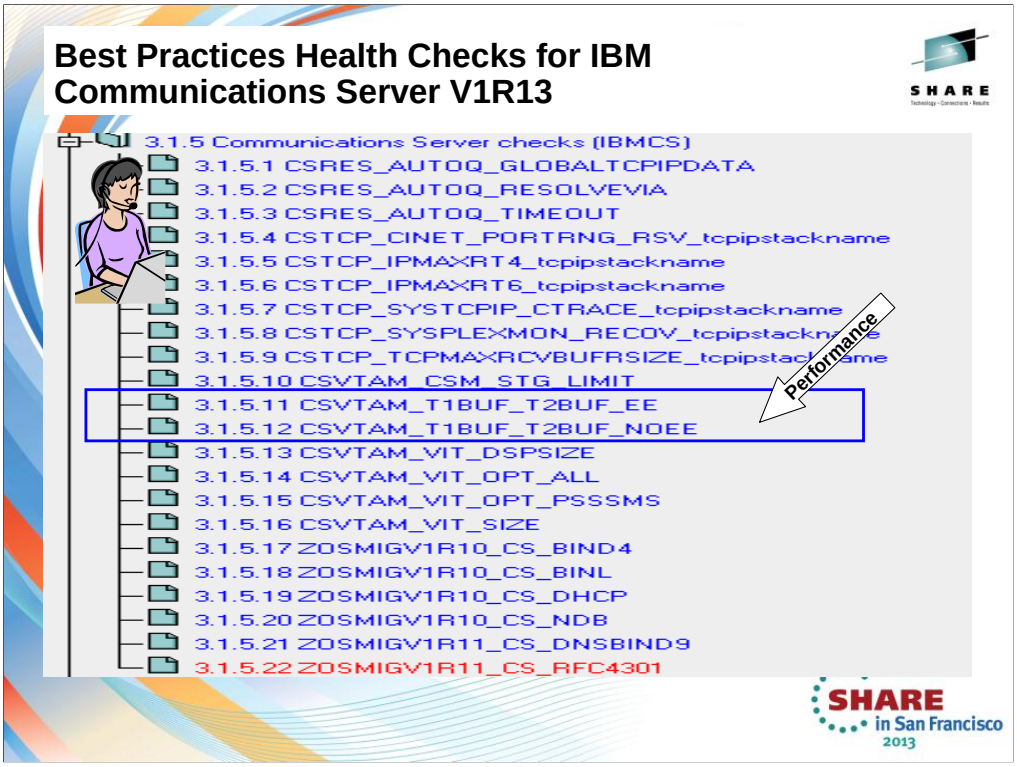
T1BUF The buffer pool that consolidates control information to support HPR data transmissions and acts as a small packing buffer for HiperSockets and QDIO

T2BUF The buffer pool that consolidates control information to support HPR data transmissions and acts as a large packing buffer for HiperSockets and QDIO

This VTAMis running with the default values for T1BUF and T2BUF. This would be a problem if Enterprise Extender were implemented in the system, as the numbers should be greater than the default.

CSVTAM_T1BUF_T2BUF_EE in the z/OS Health Checker

Checks that the number of buffers specified for the T1BUF and T2BUF buffer pools on your system is sufficient. The T1BUF and T2BUF buffers are used exclusively for Enterprise Extender (EE) HiperSockets or OSA QDIO DLCs. If EE is being used with QDIO or HiperSockets on this system, the check is successful if the number of T1BUF and T2BUF buffers specified is **greater than the default** values for the pools. Monitor the T1BUF and T2BUF pool allocations to determine the optimal allocations for these pools when using EE. The allocations should be tuned to minimize the number of expansions. Minimizing buffer pool expansions decreases internal buffer overhead processing, which should increase throughput and reduce CPU consumption. You can monitor these buffer pools using the ***D NET,BFRUSE,BUF=(T1,T2)*** command. The default allocation for the T1BUF pool is 16. The default for the T2BUF pool is 8. By default, this check is performed once at VTAM initialization and then again when the first EE line is activated. You can override this default on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command.



We'll be adding more checks to IBM Health Checker for z/OS periodically, both as APARs and integrated into z/OS. For the most up-to-date information on checks available, see the following Web site:

http://www.ibm.com/servers/eserver/zseries/zos/hchecker/check_table.html

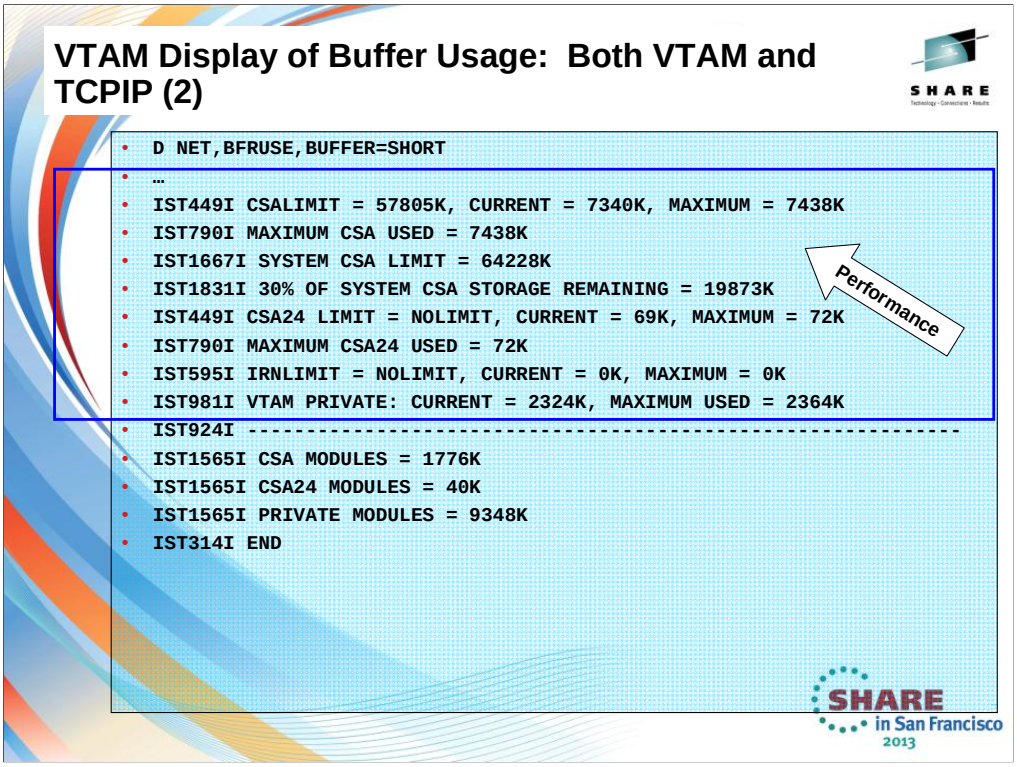
EXCEPT = Status is not acceptable; investigate

SUCCESS = Following Best Practices

ENV N/ == Not Applicable to this environment

CSVTAM_T1BUF_T2BUF_EE in the z/OS Health Checker

Checks that the number of buffers specified for the T1BUF and T2BUF buffer pools on your system is sufficient. The T1BUF and T2BUF buffers are used exclusively for Enterprise Extender (EE) HiperSockets or OSA QDIO DLCs. If EE is being used with QDIO or HiperSockets on this system, the check is successful if the number of T1BUF and T2BUF buffers specified is **greater than the default** values for the pools. Monitor the T1BUF and T2BUF pool allocations to determine the optimal allocations for these pools when using EE. The allocations should be tuned to minimize the number of expansions. Minimizing buffer pool expansions decreases internal buffer overhead processing, which should increase throughput and reduce CPU consumption. You can monitor these buffer pools using the ***D NET,BFRUSE,BUF=(T1,T2)*** command. The default allocation for the T1BUF pool is 16. The default for the T2BUF pool is 8. By default, this check is performed once at VTAM initialization and then again when the first EE line is activated. You can override this default on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command.



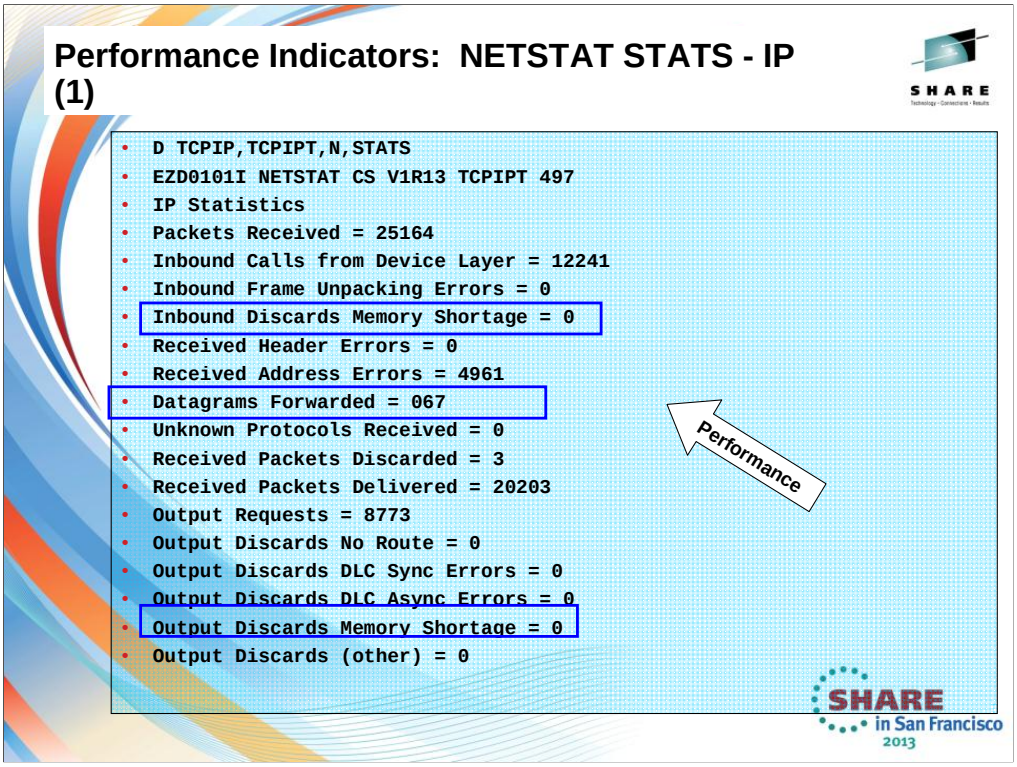
IST449I *limitname* **=** *csa***, CURRENT =** *current***, MAXIMUM =** *maxlevel*

Explanation: This message is the first in a group of messages that VTAM issues in response to a DISPLAY BFRUSE command. This message displays information about VTAM common service area (CSA) usage.

Note: Values are expressed in kilobytes.

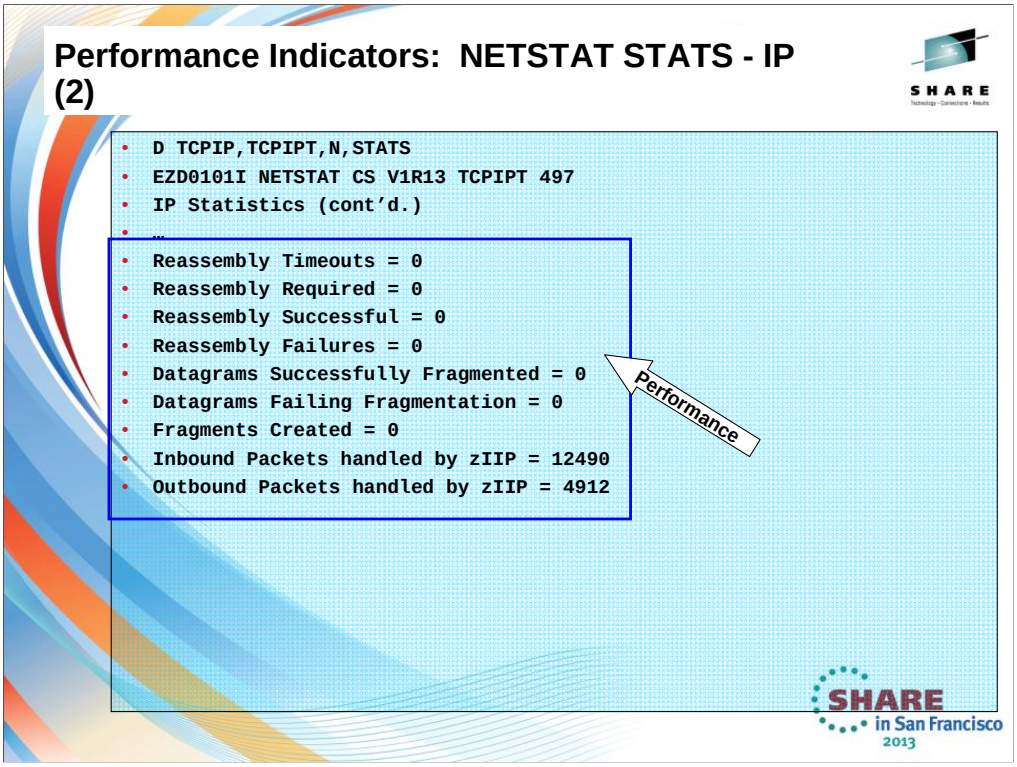
IST1667I

• *sys_csa_limit* is the maximum amount of system CSA and is determined by adding the total amount of CSA and ECSA defined in the system. The maximum amount that VTAM will use is derived by multiplying the *sys_csa_limit* by 0.9 (in other words, VTAM will never use more than 90 percent of the total CSA for the system). See *z/OS Communications Server: SNA Resource Definition Reference* for more information about how the system CSA limit relates to the CSALIMIT Start Option.



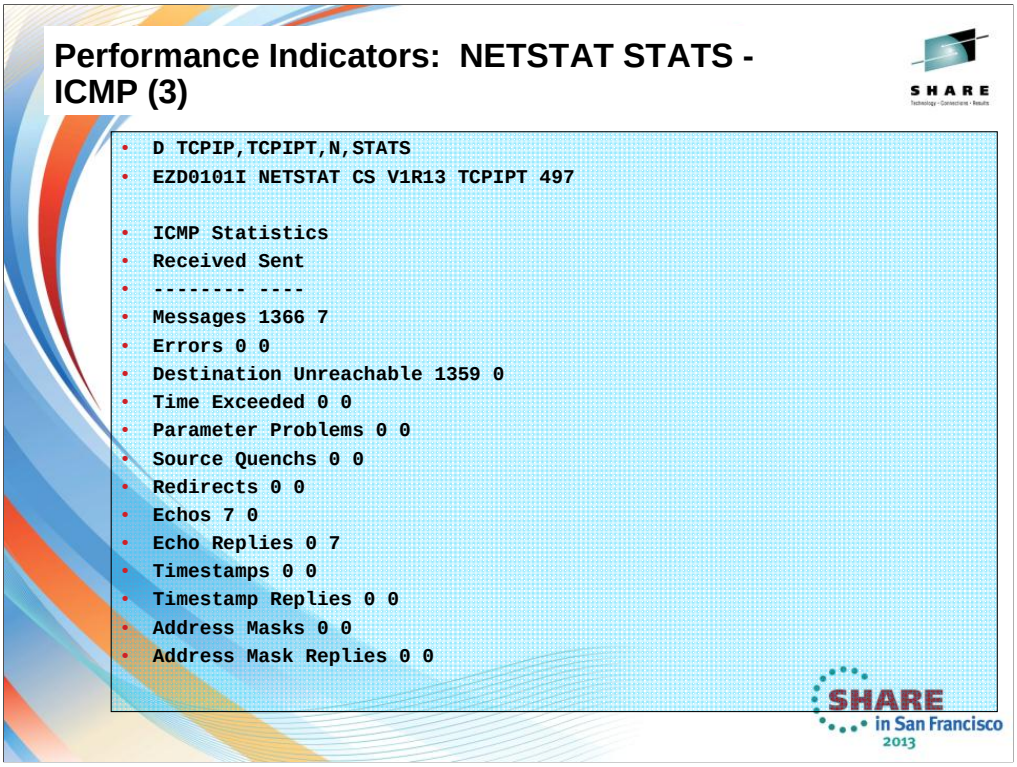
D TCPIP,,N,STATS: Displays TCP/IP statistics for each protocol. This can be used to assess the general health of the TCP/IP stack by pointing out resource shortages or problems handling inbound and outbound packets.

The information derived is for the entire TCP/IP stack and is the same information contained in the TCP/IP address space when it is shut down if you request statistics in the GLOBALCONFIG statement.



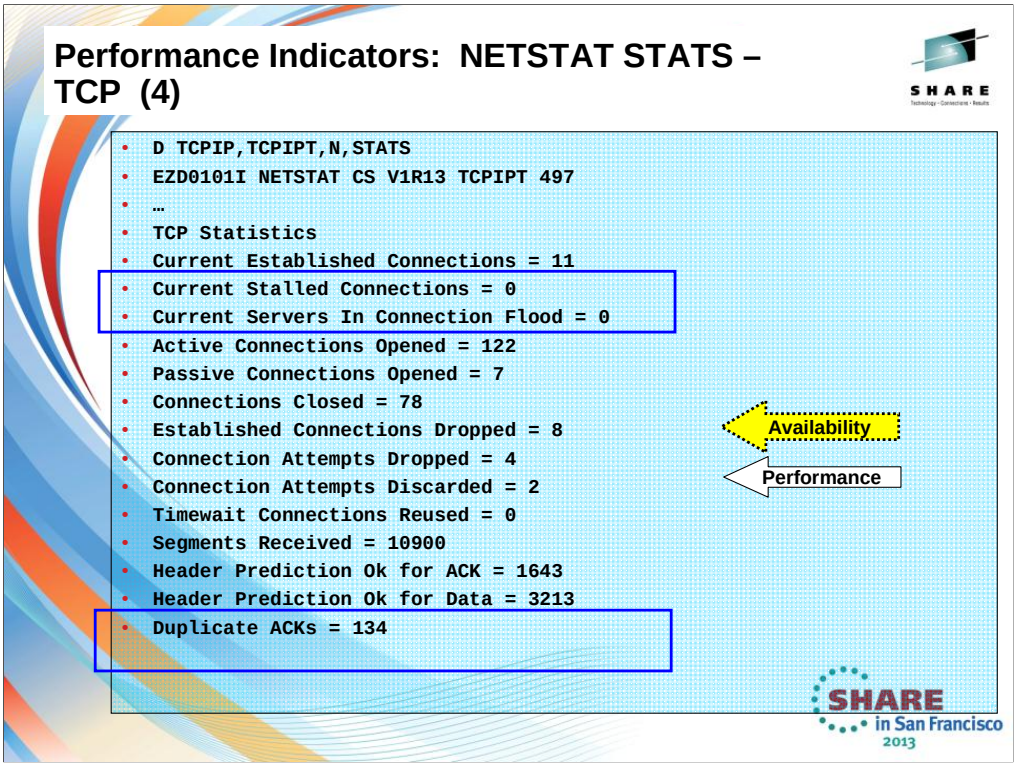
D TCPIP,,N,STATS: Displays TCP/IP statistics for each protocol. This can be used to assess the general health of the TCP/IP stack by pointing out resource shortages or problems handling inbound and outbound packets.

The information derived is for the entire TCP/IP stack and is the same information contained in the TCP/IP address space when it is shut down if you request statistics in the GLOBALCONFIG statement.



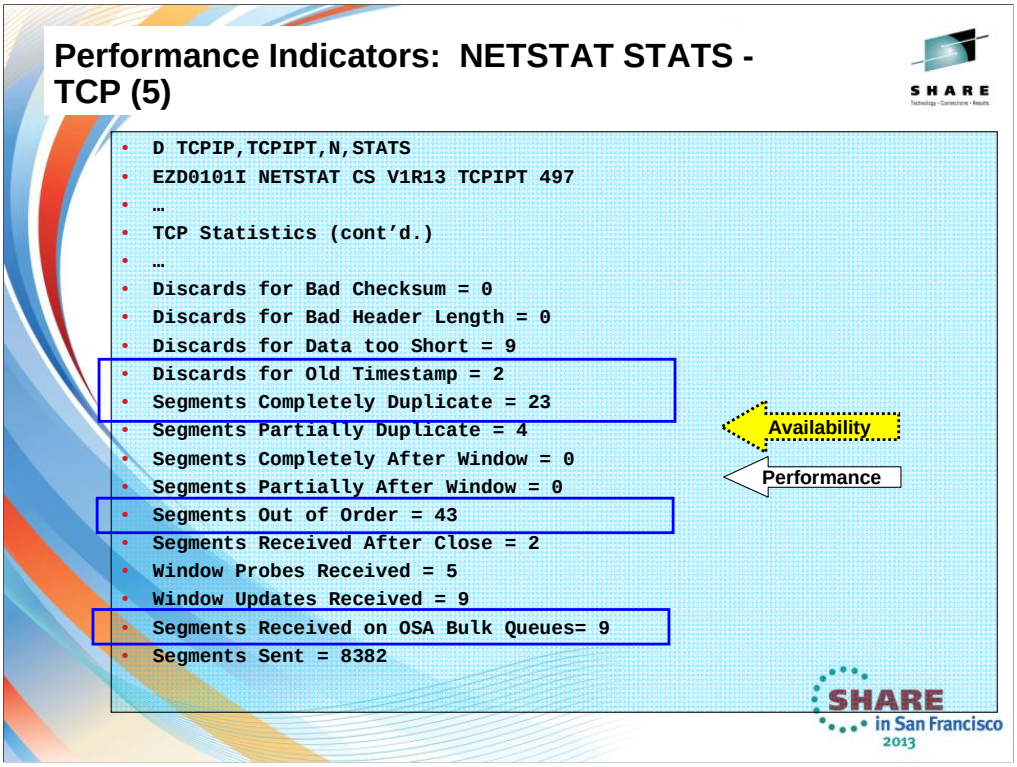
D TCPIP,,N,STATS: Displays TCP/IP statistics for each protocol. This can be used to assess the general health of the TCP/IP stack by pointing out resource shortages or problems handling inbound and outbound packets.

The information derived is for the entire TCP/IP stack and is the same information contained in the TCP/IP address space when it is shut down if you request statistics in the GLOBALCONFIG statement.



D TCPIP,,N,STATS: Displays TCP/IP statistics for each protocol. This can be used to assess the general health of the TCP/IP stack by pointing out resource shortages or problems handling inbound and outbound packets.

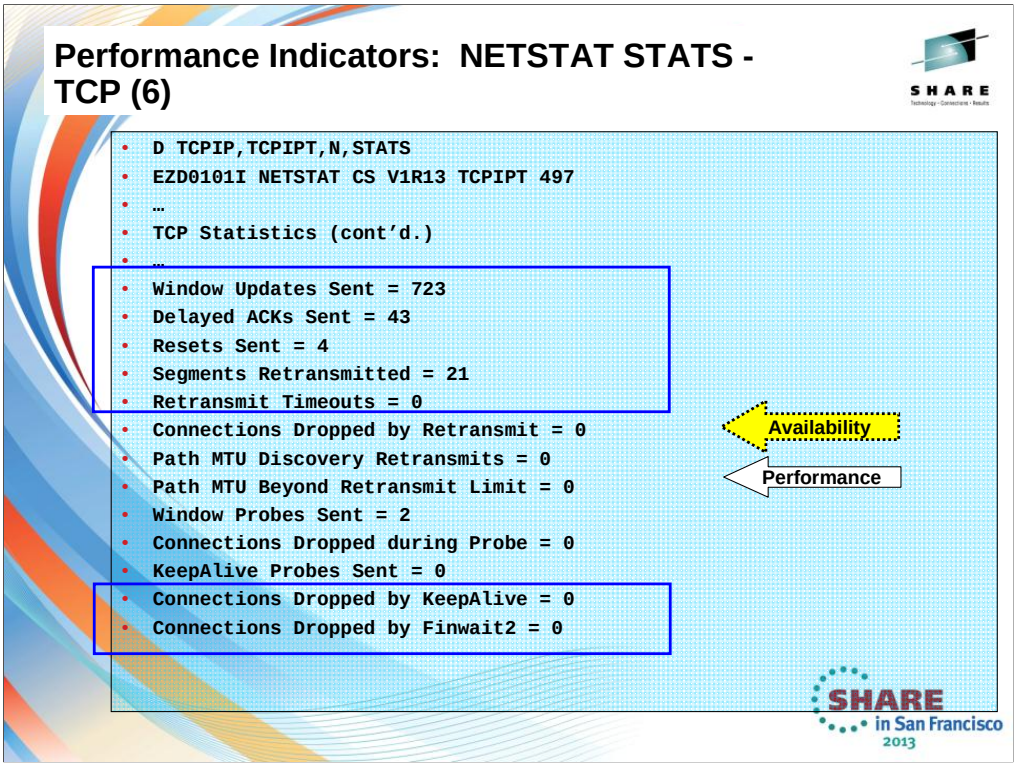
The information derived is for the entire TCP/IP stack and is the same information contained in the TCP/IP address space when it is shut down if you request statistics in the GLOBALCONFIG statement.



D TCPIP,,N,STATS: Displays TCP/IP statistics for each protocol. This can be used to assess the general health of the TCP/IP stack by pointing out resource shortages or problems handling inbound and outbound packets.

In this visual you can also determine if there might be network congestion problems or network resource shortages, since this is showing duplicate segments, discards, etc.

The information derived is for the entire TCP/IP stack and is the same information contained in the TCP/IP address space when it is shut down if you request statistics in the GLOBALCONFIG statement.



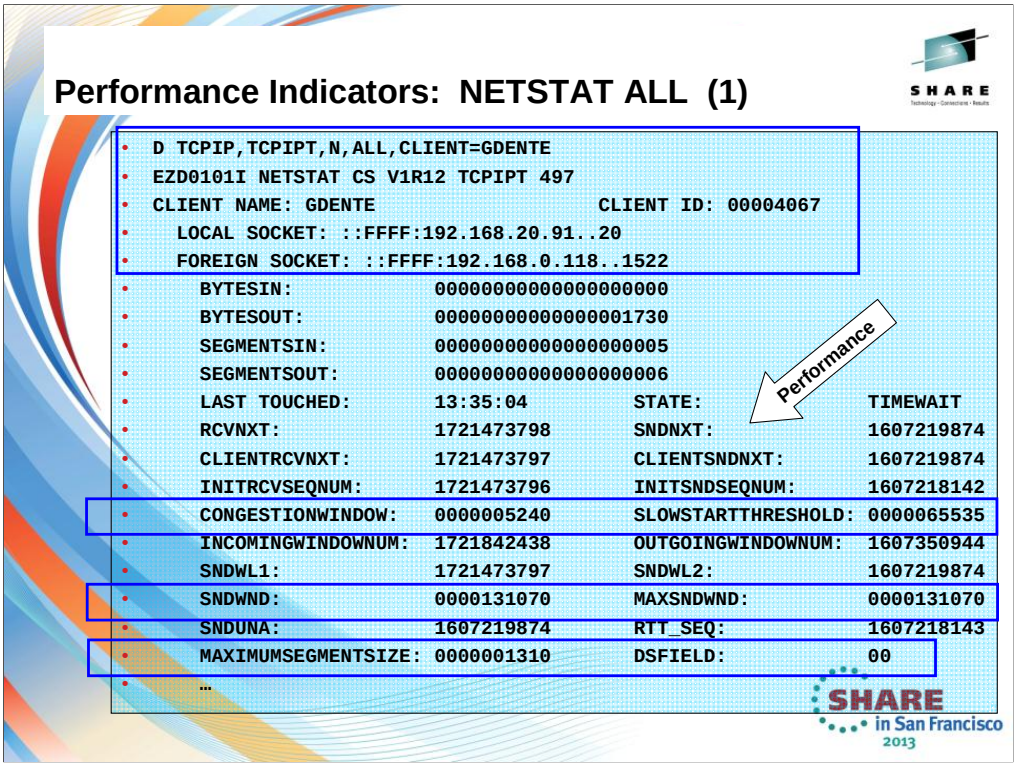
D TCPIP,,N,STATS: Displays TCP/IP statistics for each protocol. This can be used to assess the general health of the TCP/IP stack by pointing out resource shortages or problems handling inbound and outbound packets.

In this visual you can also determine if there might be network congestion problems or network resource shortages, since this is showing duplicate segments, discards, dropped connections, etc.

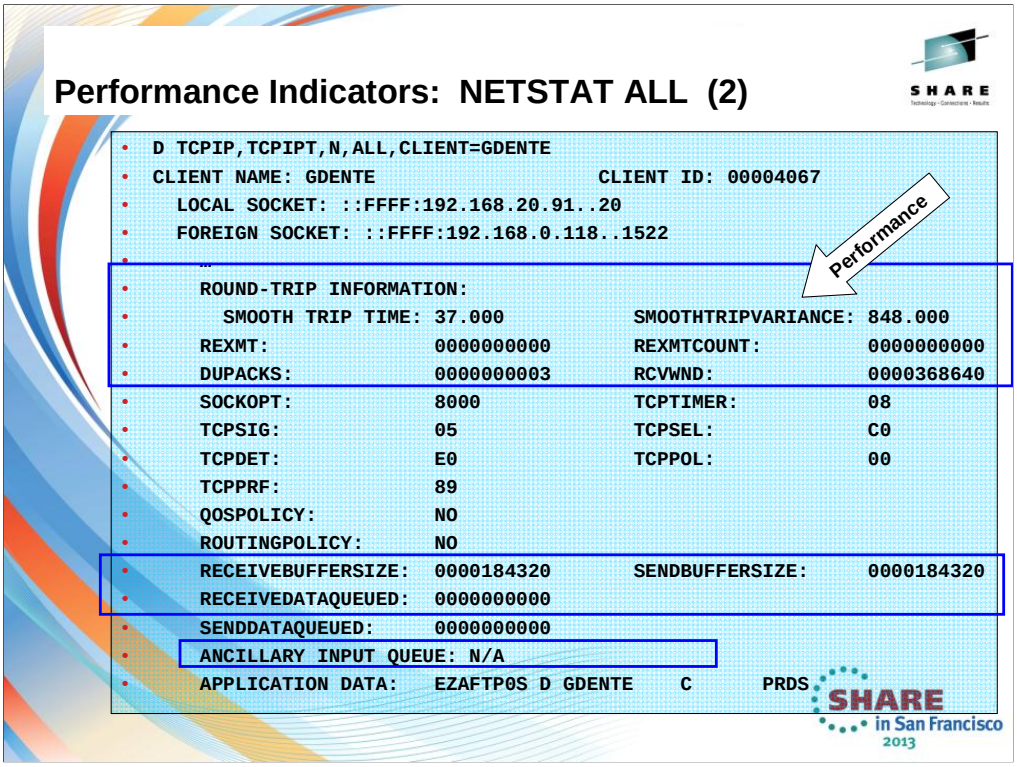
The information derived is for the entire TCP/IP stack and is the same information contained in the TCP/IP address space when it is shut down if you request statistics in the GLOBALCONFIG statement.

Performance Indicators: NETSTAT STATS – UDP (7)

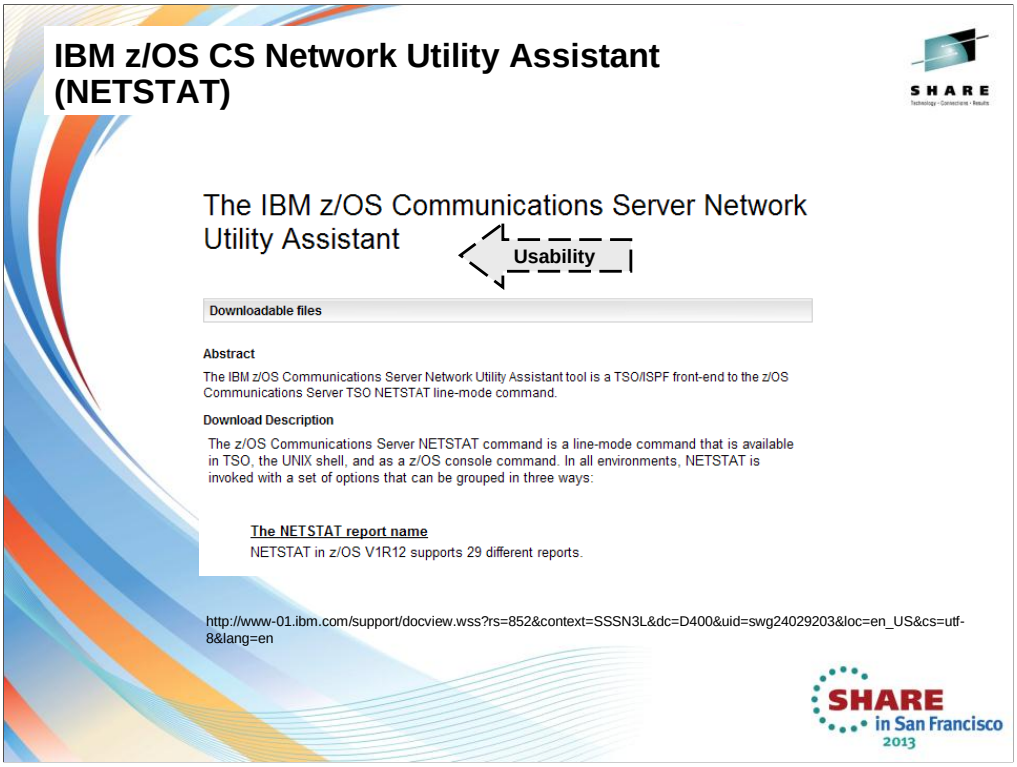
```
D TCPIP,TCPIPT,N,STATS
EZD0101I NETSTAT CS V1R13 TCPIPT 497
…
UDP Statistics
Datagrams Received = 6984
No Port Errors = 2312
Receive Errors = 0
Datagrams Sent = 368
```



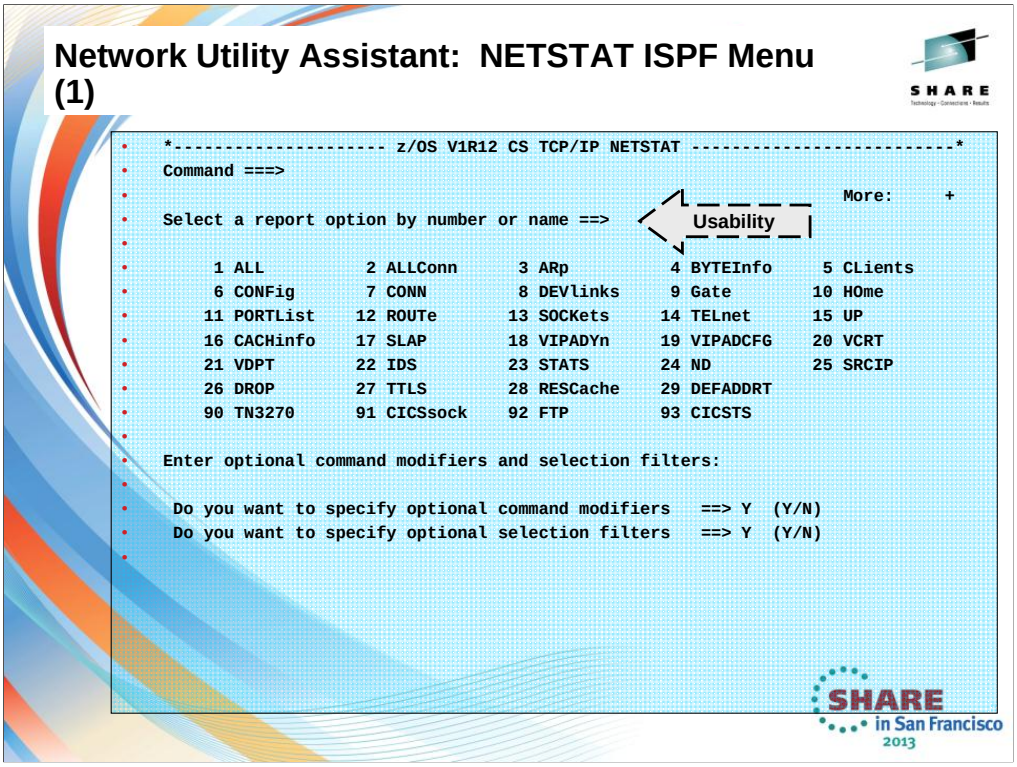
The command to display all connections can exploit various filters, like port number or client name, etc. Here we see an established connection and we are able to determine what the TCP MSS is for this particular connection; we also determine if there are congestion problems in the network (see Congestionwindow and Slowstarthreshold indicators) and what the current window sizes are.



In this visual you see how FTP sets its own receive buffer size; there is no queuing going on in this transmission. There are very few duplicate acks, meaning that we see no evidence of a network problem for this connection. The round trip time in the network can also be an indicator of general network performance in terms of bandwidth.



This shows you that the many parameters of the NETSTAT command can be more easily managed if you exploit the tool known as the z/OS Communications Server Network Utility Assistant.



This shows you that the many parameters of the NETSTAT command can be more easily managed if you exploit the tool known as the z/OS Communications Server Network Utility Assistant. You reach this screen with the following ISPF command:

exec 'netstat.assist.rexx(ezans)' (or whatever REXX library you have installed the code in).


#SHAREorg
SHARE
APPENDICES
SHARE
in San Francisco
2013

Summary of Steps

1. Define the Purpose or Expected Outcome of the Networking Health Check and its Scope
   - A. Education and Advice?
   - B. Analysis, Audit?
   - C. Insight into a Problem?
2. Define the Format of the Networking Health Check Report
3. List the documentation and tools required for the analysis and the personnel who will provide the documentation
4. Gather and analyze the documentation
5. Write the report

- We omit an example of a completed and full report in this presentation.

1. Scope and Purpose: Education, Advice?

- **SCOPE (example):** z/OS TCP/IP and its Interfaces

A. General PURPOSE: For Education, for Advice on …

- New Functions and their Exploitation?
- Obstacles to a future migration?
- Optimizing performance and administration?
- Best Practices for different components?
- Achieving Network Availability?
- Currency of code or platform maintenance?
- Eliminating Networking Security Vulnerabilities?
- Optimization of Network Topology?

1. Scope and Purpose: Analysis, Audit, Insight?

- **SCOPE (example):** z/OS TCP/IP and its Interfaces

B. **Consulting PURPOSE:**
  - Thorough Audit of a component's implementation:
    - *Review of release level currency (Are you missing Hiper PTFs?)*
    - *Discovery of Potential Pitfalls with current definitions or hardware/software implementations*
    - *Discovery of threats to Availability*
    - *Discovery of threats to Security*

C. **Post-Mortem PURPOSE:**
  - To gain insight into cause of a problem and future avoidance
  - Review of IT Problems or Critical Situations recently experienced
    - *Identify the Problem Source and suggest plans to avoid similar situation in future.*
      - *"Lessons Learned"*

2. What is the Format of a z/OS Networking Health Check?

- **Health Check Output from IBM Procedures and Tools**
  - From z/OS Health Checker (HZSPROC)
  - From z/OS Communications Server Configuration Assistant Health Checker
  - Syntax Checks provided by TN3270, by UNIX System Services for BPXPRMxx, etc.
- **Health Check Output and Testing by Application Developers:**
  - Example: Expresso Application Development
    - http://www.jcorporate.com/expresso/doc/edg/edg_index.html
- **Health Check Format – Self-designed**
  - Purpose, Expected Outcome of Health Check
  - Component(s) being analyzed (Scope)
  - Input requested of customer or installation
  - Findings and Observations
  - Recommended Actions and Reasons

z/OS Health Checker Format: IBM Communications Server V1R12

At SDSF enter: "CK"
To MODIFY fields, requires RACF Authorization:

```
ISF015I SDSF COMMAND ATTEMPTED 'F ZSPROC,UPDATE,CHECK=(IBMCS,CSTCP_IPMA
 ...
ICH408I USER(GDENTE  ) GROUP(SYS1    ) NAME(####################) 060
  HZS.MVS1.IBMCS.CSTCP_IPMAXRT6_TCPIP1.UPDATE CL(XFACILIT)
  PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
  ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

NP	NAME	CheckOwner	State	Status
	CSTCP_CINET_PORTRNG_RSV_TCPIP1	IBMCS	ACTIVE(ENABLED)	EXCEPT
	CSTCP_IPMAXRT4_TCPIP1	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSTCP_IPMAXRT6_TCPIP1	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSTCP_SYSPLEXMON_RECOV_TCPIP1	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSTCP_SYSTCPIP_CTRACE_TCPIP1	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSTCP_TCPMAXRCVBUFRSIZE_TCPIP1	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSVTAM_CSM_STG_LIMIT	IBMCS	ACTIVE(ENABLED)	EXCEPT
	CSVTAM_T1BUF_T2BUF_EE	IBMCS	ACTIVE(DISABLED)	ENV N/
	CSVTAM_T1BUF_T2BUF_NOEE	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSVTAM_VIT_DSPSIZE	IBMCS	ACTIVE(ENABLED)	EXCEPT
	CSVTAM_VIT_OPT_ALL	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSVTAM_VIT_OPT_PSSSMS	IBMCS	ACTIVE(ENABLED)	SUCCES
	CSVTAM_VIT_SIZE	IBMCS	ACTIVE(ENABLED)	SUCCES

SHARE in San Francisco 2013

We'll be adding more checks to IBM Health Checker for z/OS periodically, both as APARs and integrated into z/OS. For the most up-to-date information on checks available, see the following Web site:

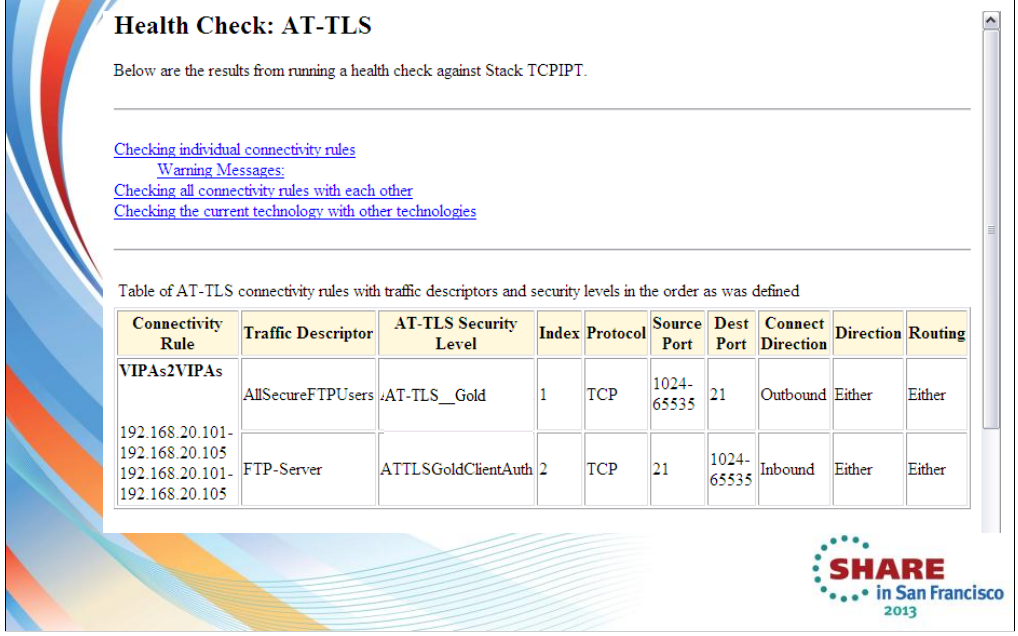
http://www.ibm.com/servers/eserver/zseries/zos/hchecker/check_table.html

EXCEPT = Status is not acceptable; investigate

SUCCESS = Following Best Practices

ENV N/ == Not Applicable to this environment

z/OS Configuration Assistant Health Check Format



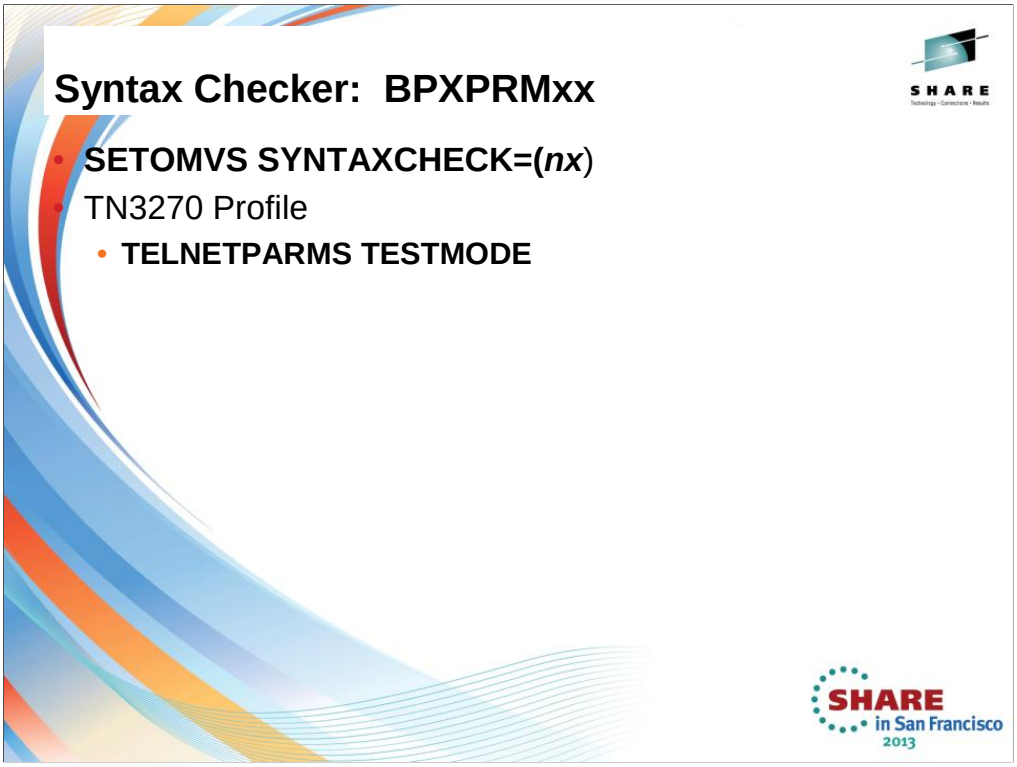
Health Check: AT-TLS

Below are the results from running a health check against Stack TCPIPT.

Checking individual connectivity rules
    Warning Messages:
Checking all connectivity rules with each other
Checking the current technology with other technologies

Table of AT-TLS connectivity rules with traffic descriptors and security levels in the order as was defined

Connectivity Rule	Traffic Descriptor	AT-TLS Security Level	Index	Protocol	Source Port	Dest Port	Connect Direction	Direction	Routing
VIPAs2VIPAs 192.168.20.101-192.168.20.105 192.168.20.101-192.168.20.105	AllSecureFTPUsers	AT-TLS__Gold	1	TCP	1024-65535	21	Outbound	Either	Either
	FTP-Server	ATTLSGoldClientAuth	2	TCP	21	1024-65535	Inbound	Either	Either



SETOMVS SYNTAXCHECK:

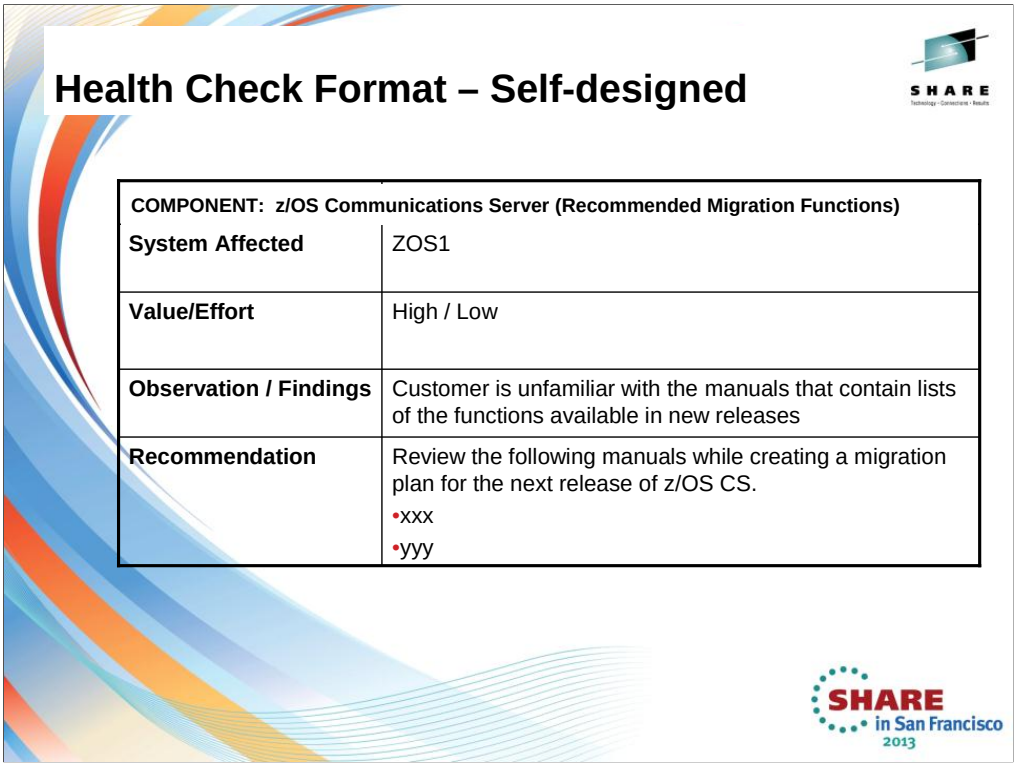
Option on the SETOMVS operator command to syntax check a BPXPRMxx parmlib member **before IPL.** Runs the same logic used at IPL or via SETOMVS. It checks whether HFS / zFSdata sets exist. Any errors cause messages to be written to the system log and these are the same messages as at IPL. You might see messages like the following:

BPXO039I SETOMVS SYNTAXCHECK COMMAND SUCCESSFUL.

BPXO023I THE PARMLIB MEMBER BPXPRMXX CONTAINS SYNTAX ERRORS. REFER TO HARD COPY LOG FOR MESSAGES.

TELNETPARMS TESTMODE:

Use the TESTMODE parameter statement to allow an operator to try a profile without applying it. All the processing and checking are done for an actual update, but at the end of the process, instead of applying the new profile, all data structures are released. If this statement is not coded, the profile becomes the CURRent profile when processed. TESTMODE can be coded only in the TELNETPARMS statement block. With the TESTMODE statement, a Telnet administrator can issue a VARY TCPIP,,OBEYFILE command for a profile data set and determine whether there are any syntax or semantic errors without concern for applying a profile that is not valid. TESTMODE profiles can be processed as often as you want.



This represents a format used by SMEs in the IBM Advanced Technical Skills (ATS) group.

#SHAREorg

SHARE

3a. Basic Requests for z/OS Network Documentation

- UNIX
- SNA (VTAM) and Topology Diagram
- Enterprise Extender (EE) and Topology Diagram
- TCP/IP and Topology Diagram
- Policy Agent Policy Types (Security and Performance)

SHARE in San Francisco 2013

Spreadsheet toTrack Activity

What you request depends on the purpose for conducting the Health Check.

Name of Task	Documentation to Gather	Task Assigned to:
Recent TCP/IP Connection Failures	Network Diagram of Flow, Console Messages, Dumps, Routing Displays	T. C. Pip
Enterprise Extender Performance	Output from EE and VTAM Commands	Victor Tam

Request Documentation from Following Command Output at Designated Nodes*

- D OMVS,O
- D OMVS,P
- D OMVS,L
- Output from z/OS Health Checker
  - UNIX System Services?
  - z/OS?
  - z/OS Communications Server?
  - Other application-related messages?
- SYSLOGD configuration file (syslog.conf)

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation from Following Command Output at Designated Nodes*

- D NET,VTAMOPTS
- D NET,BFRUSE,BUFFER=SHORT
  - May need F NET,TNSTATS later
- D NET,CSM,OWNERID=ALL
- D NET,EE,LIST=DETAIL
- D NET,GRPREFS
- D NET,STATS,TYPE=VTAM
- D NET,E,ID=<names of Model Major Nodes – EE, RTP, VN, XCF)
- D NET,EEDIAG,TEST=YES [, ,<multiple variations>]
- D NET,E,ID=<XCA Major Node for Enterprise Extender>
- D NET,E,ID=<SWNet Major Nodes for Enterprise Extender>
- D NET,E,ID=<EE PUs inside SWNet Major Nodes>
- D NET,TOPO,<multiple variations>
- D NET,TGPS
- D NET,TRL
- D NET,E,ID=TRLEname

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation from Following Command Output at Designated Nodes*

- F RESOLVER,DISPLAY
- D TCPIP,,N,CONFIG
- D TCPIP,,N,HOME
- D TCPIP,,N,STATS
- D TCPIP,,N,DEV[,INTFNAME=interface name]
- D NET,TRL
- D NET,E,ID=TRLEname
- D TCPIP,,OSAINFO,INTFNAME=<name of QDIO OSA interface>
- OSA/SF “GET CONFIG” and “GET OAT”
- D TCPIP,,N,ROUTE,DETAIL
- D TCPIP,,OMP,OSPF,STATS
- D TCPIP,,OMP,OSPF,NBRS
  - May need additional OSPF command output*
- D TCPIP,,N,VIPADCFG,DETAIL
- D TCPIP,,SYSPLEX,VIPADYN
- D TCPIP,,N,VDPT,DETAIL
- D TCPIP,,N,VCRT,DETAIL
- Copy of pertinent TCP/IP Profiles and their INCLUDE files
- Copy of pertinent OMPROUTE Configuration Files

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation for Designated Nodes*

- Version and Release Level, Currency Level
- Topology Diagram
  - SNA
    - NETIDs
    - SSCPNAMEs
    - APPN[/HPR] Node Roles (NNs, CDSs, ENs, NNSs, LENs)
    - Other Nodes (NCP, Pus, etc.)
    - SNA Links and their Connectivity
    - If using Enterprise Extender (EE), indication of EE Endpoints and Roles

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation for Designated Nodes*

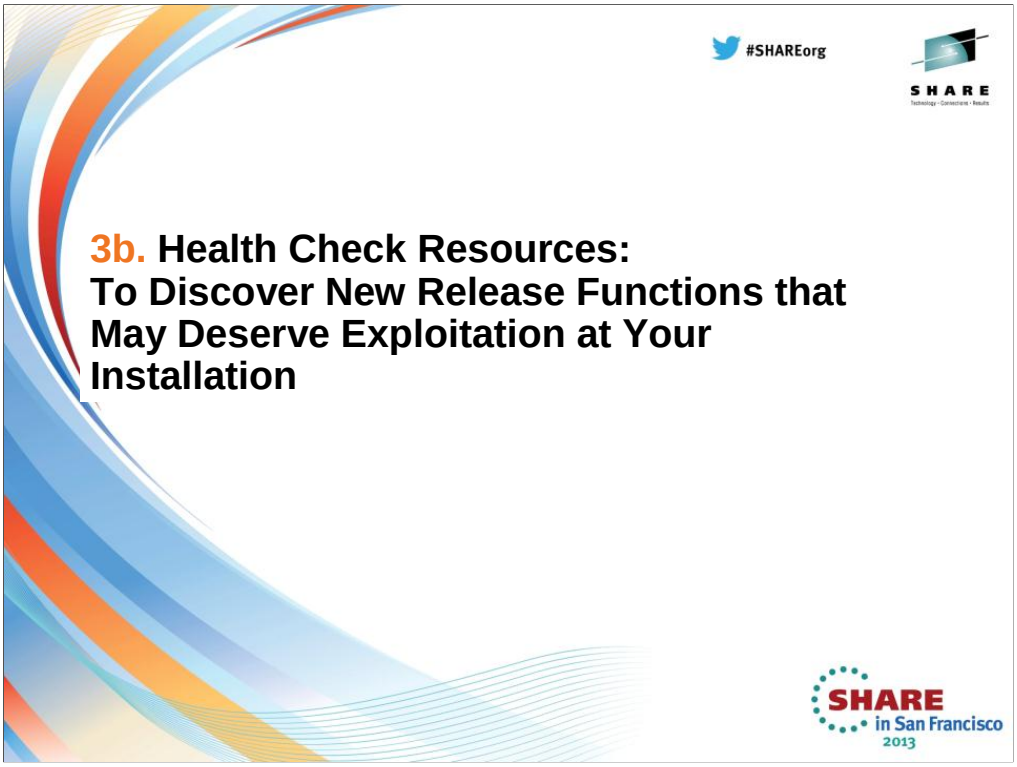
- Version and Release Level, Currency Level
- Topology Diagram
  - IP
    - Host Names
    - IP Networks and Subnets
    - Location of Routers, Switches, Firewalls
    - IP Interfaces and their Connectivity
    - If using Sysplex Distribution, indication of Primary SD(s) and Secondary SD(s) and the target applications for which responsible
    - If OSPF Dynamic Routing
      - *Indication of Area Types and Numbers*
      - *Indication of Area Border Routers, Autonomous System Boundary Routers*
- Definition Files
  - TCP/IP PROFILE and INCLUDE members
  - OMPROUTE Configuration File

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.

Request Documentation for Designated Nodes*

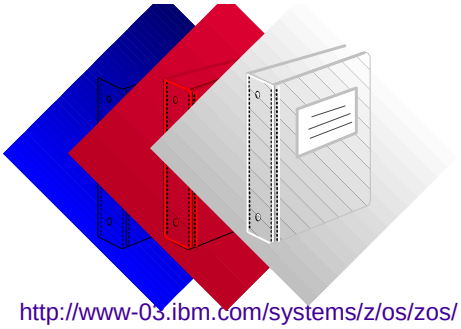
- If pertinent to the Scope of the Health Check,
  - Description of Policy Agent Exploitation
    - Security Policies?
    - QoS Policies?
    - Policy Based Routing Policies?
  - Method of Configuring Policies
    - z/OS Communications Server Configuration Assistant on Windows?
    - z/OS Communications Server Configuration Assistant on z/OSMF?

* The actual list of commands and the designated nodes would be determined by the reason for and scope of the Health Check.



This section of the presentation shows you what should be investigated if the purpose of the Health Check is to consider which new functions in a new or old release should be exploited.

Index of Migration Manuals (V1R10-V1R13)

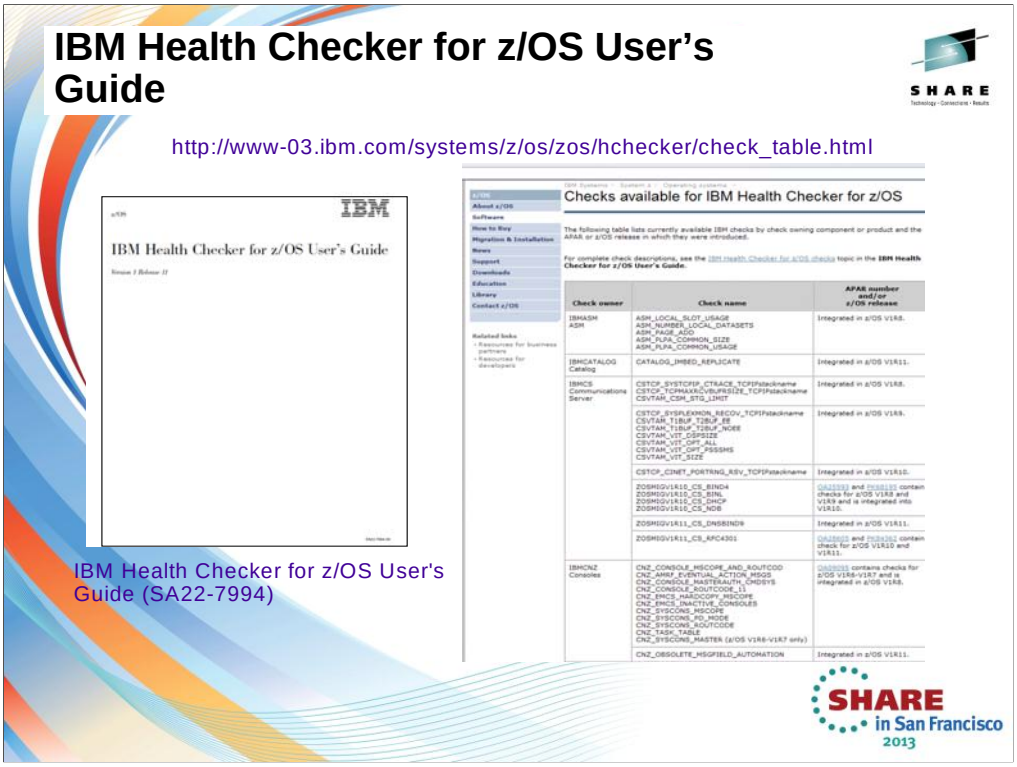


http://www-03.ibm.com/systems/z/os/zos/bkserv/zos_migration_manuals.html

Find this list at: http://www-03.ibm.com/systems/z/os/zos/bkserv/zos_migration_manuals.html

Manuals to Get You Started with CS Migration

- **z/OS Introduction and Release Guide (GA22-7502-nn)**
  - Presents high-level function descriptions with pointers to the detailed descriptions in New Function Summary
- **z/OS Migration (GA22-7499-nn)**
  - Lists Communications Server function that requires you to take action to migrate to V1R12 or V1R13
  - This information is not provided in this format in the Communications Server library
- **z/OS Communications Server New Function Summary (GC31-8771-nn)**
  - Detailed descriptions of new CS functions
- **z/OS Summary of Message and Interface Changes (SA22-7505-nn)**
  - Lists all new and changed Comm Server commands, parameters, socket API changes, FTP and Telnet changes, etc.
  - This information is not provided in this format in the Communications Server library
- **IBM Health Checker for z/OS: User's Guide (SA22-7994-nn)**
  - Install Health Checker on current release to review migration warnings for new release



You will probably want to download the IBM Health Checker for z/OS User's Guide to investigate how to implement Health Checker and to understand the various types of health checks that are available to you, including those in IBM Communications Server.

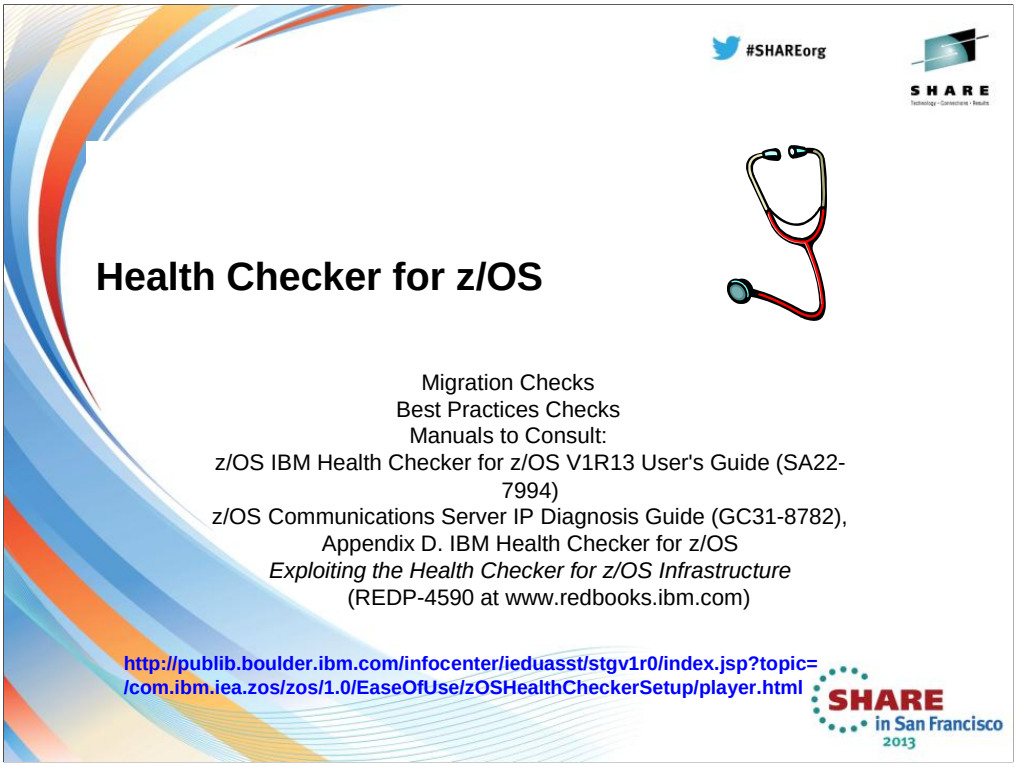
The User's Guide points you to web pages for INFO APARs and Health Check APARs and to the z/OS User's Guide itself.

To set up HealthChecker, perform the following steps as outlined in the Health Checker for z/OS User's Guide (GA22-7994).

1. "Allocate the HZSPDATA data set to save check data between restarts"
2. "Create security definitions"
3. "Start IBM Health Checker for z/OS"
4. "Obtain checks for IBM Health Checker for z/OS"

Once you've gotten IBM Health Checker for z/OS set up, you can use the HZSPRINT utility and SDSF to view and work with check output. See the following for information:

- "Using the HZSPRINT utility"
- To set up and use SDSF, see the following:
  - – Set up security and customization for SDSF support for IBM Health Checker for z/OS using information in IBM Health Checker for z/OS Small Programming Enhancement in *z/OS SDSF Operation and Customization*.
  - – "Using SDSF to manage checks"



To understand the Health Checker for z/OS, see z/OS IBM Health Checker for z/OS V1R13 User's Guide for Version 1 Release 13 (SA22-7994-12).

For a wealth of details and experience-based information about using and writing checks for IBM Health Checker for z/OS, see *Exploiting the Health Checker for z/OS infrastructure* (REDP-4590)

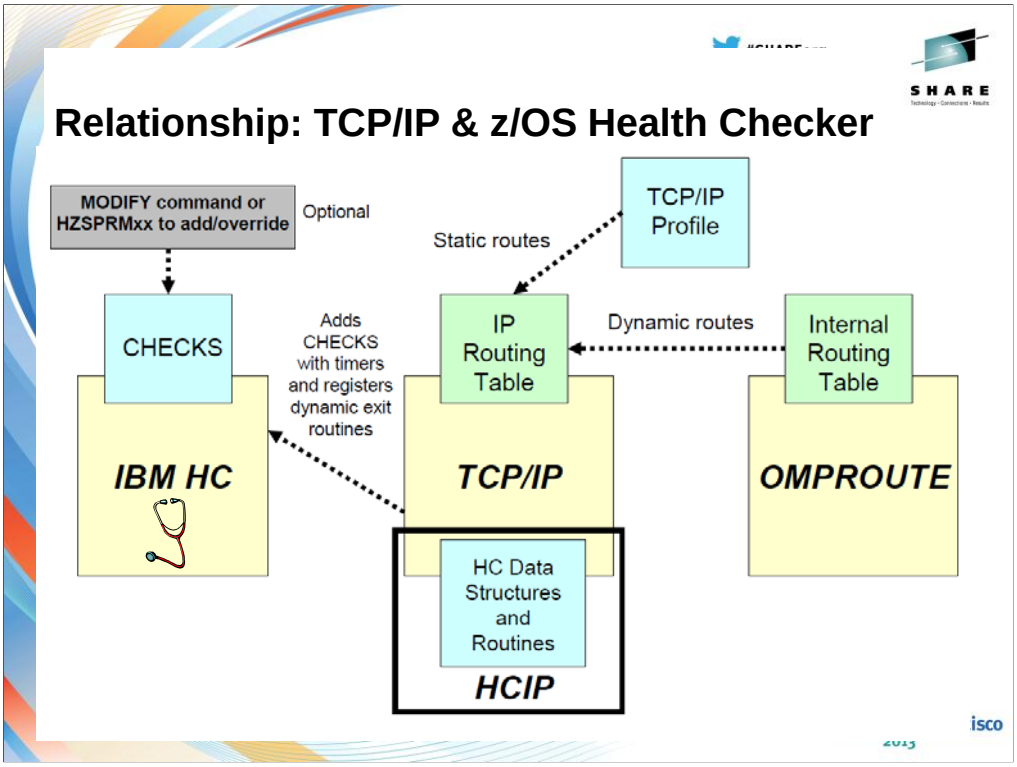
For a list of available z/OS Communications Server Health Checks, see the z/OS Communications Server IP Diagnosis Guide (GC31-8782), Appendix D. IBM Health Checker for z/OS, and the website

The values used by checks come from a variety of sources including product documentation and web sites, such as:

- z/OS system test
- z/OS Service
- Parallel Sysplex Availability Checklist at: http://www.ibm.com/servers/eserver/ zseries/pso/
- ITSO Redbooks at: http://www.redbooks.ibm.com/
- *System z Platform Test Report for z/OS and Linux Virtual Servers* at: http://www.ibm.com/servers/eserver/zseries/zos/integtst/
- Washington System Center Flashes at http://www.ibm.com/support/techdocs/.
- Parallel Sysplex and z/OS publications:
    - *z/OS MVS Initialization and Tuning Reference*, SA22-7592
    - *z/OS MVS Planning: Global Resource Serialization*
    - *z/OS MVS Planning: Operations*, SA22-7601
    - *z/OS MVS Setting Up a Sysplex*, SA22-7625
    - *z/OS Security Server RACF Command Language Reference*
    - *z/OS Security Server RACF Security Administrator's Guide*
    - *z/OS UNIX System Services Planning*, GA22-7800

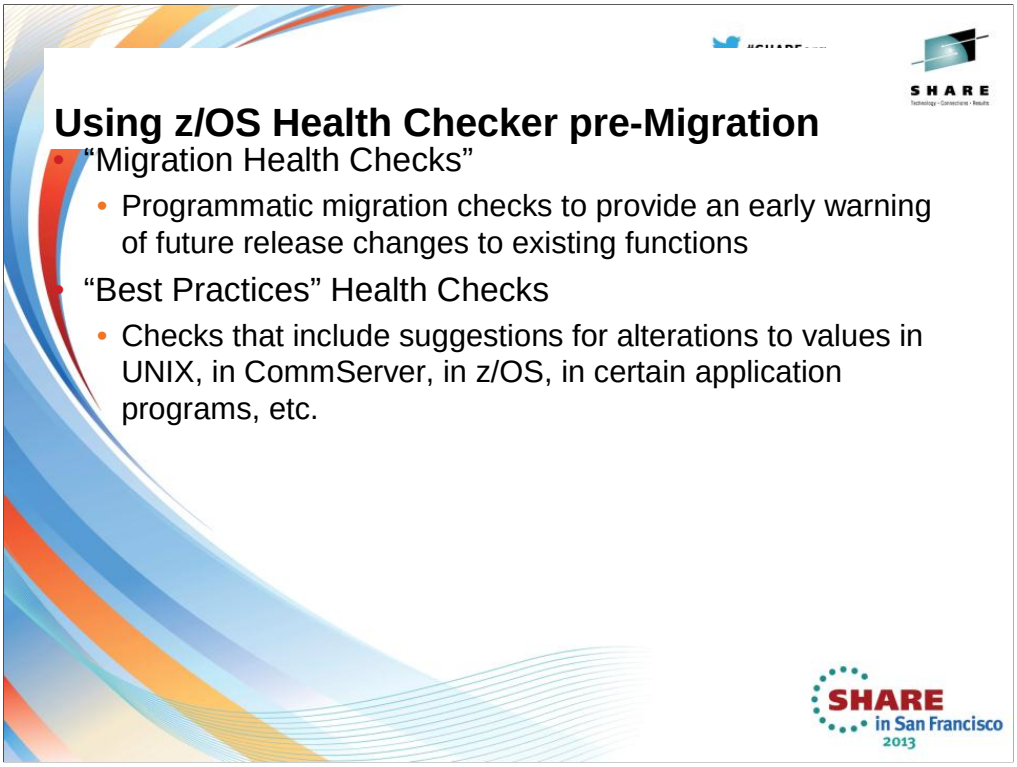
The description of each individual check contains the rationale behind the values used by the check for comparison against your installation settings.

You might find that the values that the check uses for comparison are not appropriate for your installation or for a particular system. If that is the case, you can either specify overrides to default values or suppress individual checks. See Chapter 4, “Managing checks,” of the z/OS IBM Health Checker for z/OS V1R13 User's Guide Version 1 Release 13 (SA22-7994-12).

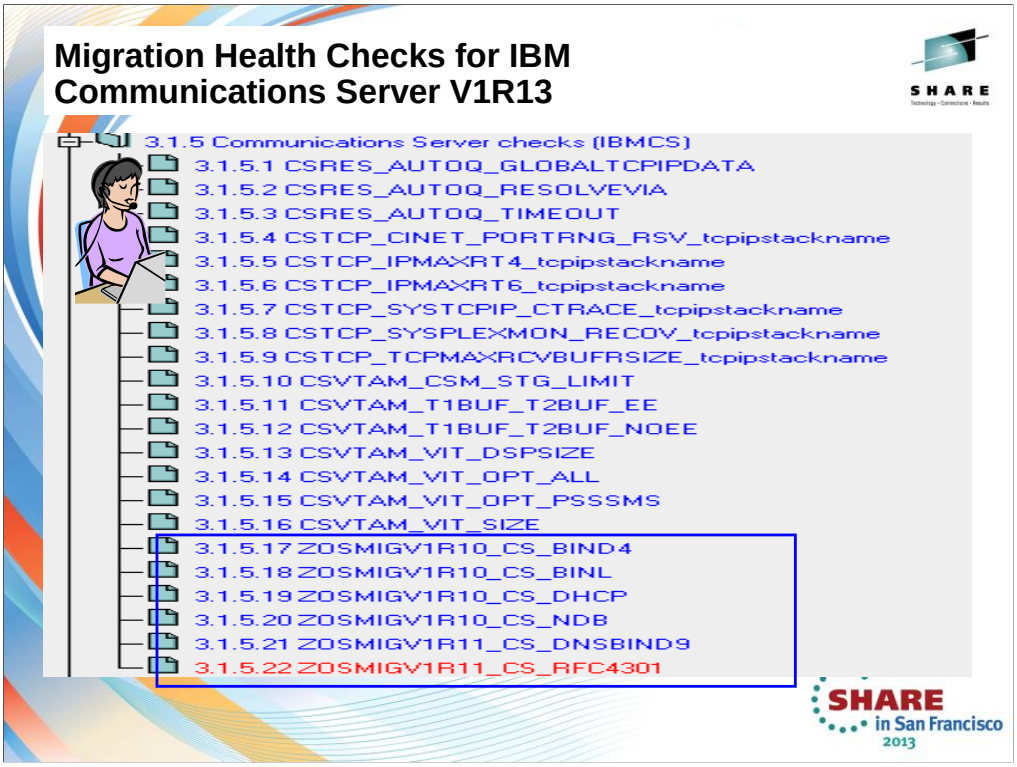


This is a diagram of interacting components: IBM Health Checker for z/OS (IBMHC), TCP/IP stack, TCP/IP Health Checker (HCIP), and OMPROUTE. IBMHC, TCP/IP stack, and OMPROUTE run in their own address spaces. During initialization, the TCP/IP stack defines and adds the TCP/IP checks and timer parameters to the IBMHC. It also registers and loads the dynamic exit routines used to communicate with the IBMHC.

Based on the check timer parameters provided, IBMHC runs the checks for health monitoring. TCP/IP configuration processing updates the IPv4 and IPv6 static routes in the TCP/IP stack routing tables. OMPROUTE also updates the IPv4 and IPv6 dynamic routes in the TCP/IP stack routing tables. IBMHC interacts with HCIP to update or retrieve health checker related data (for example, TCP/IP stack routing statistics). Based on the check timer parameters and health checker data from HCIP, IBMHC issues informational or warning messages as necessary.



The objective of Migration Health Checks is to provide programmatic migration checks that can give you an early warning if you are using functions that will be significantly changed or removed in future releases.



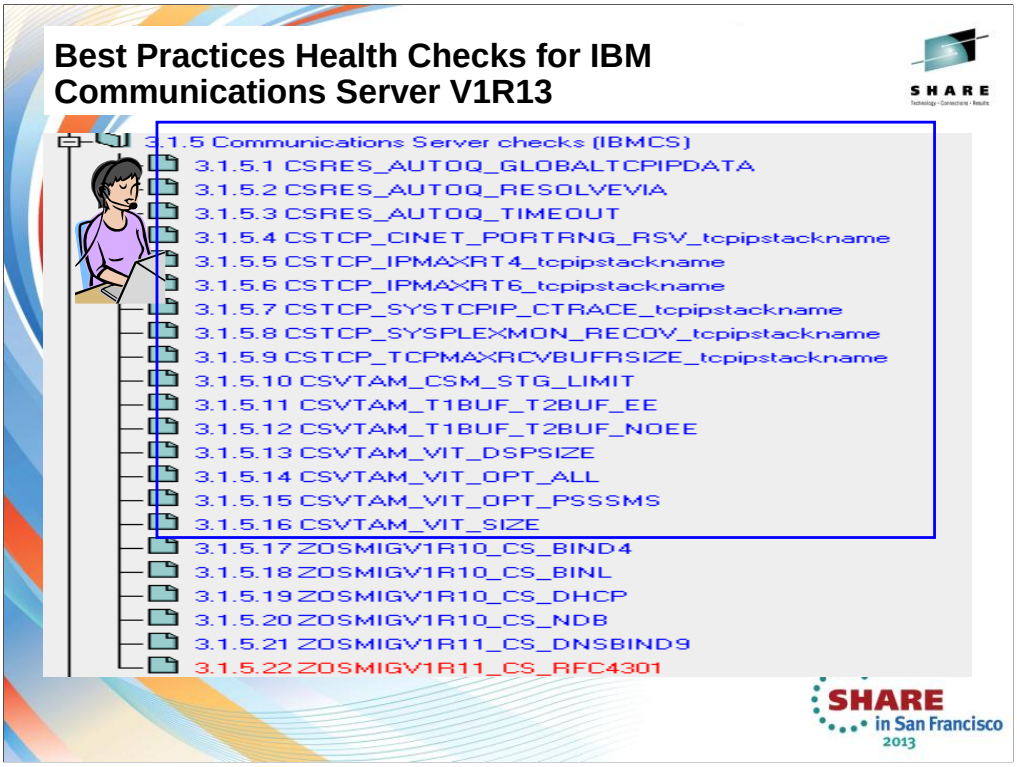
We'll be adding more checks to IBM Health Checker for z/OS periodically, both as APARs and integrated into z/OS. For the most up-to-date information on checks available, see the following Web site:

http://www.ibm.com/servers/eserver/zseries/zos/hchecker/check_table.html

EXCEPT = Status is not acceptable; investigate

SUCCESS = Following Best Practices

ENV N/ == Not Applicable to this environment



We'll be adding more checks to IBM Health Checker for z/OS periodically, both as APARs and integrated into z/OS. For the most up-to-date information on checks available, see the following Web site:

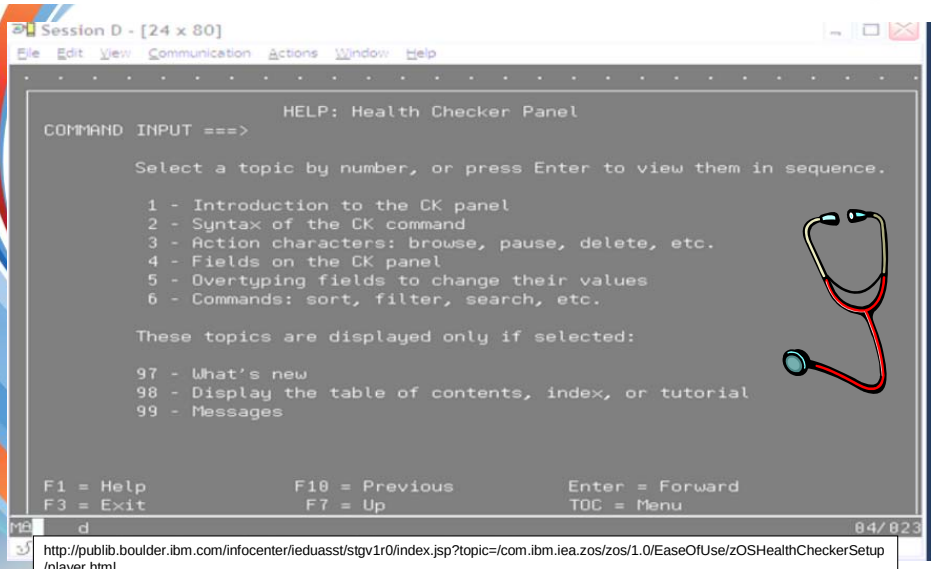
http://www.ibm.com/servers/eserver/zseries/zos/hchecker/check_table.html

EXCEPT = Status is not acceptable; investigate

SUCCESS = Following Best Practices

ENV N/ == Not Applicable to this environment

Health Checker HELP ISPF Panel in z/OS



http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp?topic=/com.ibm.iea.zos/zos/1.0/EaseOfUse/zOSHealthCheckerSetup/player.html

Health Checks for IBM Communications Server V1R13

At SDSF enter: "CK" or F HZSPROC,DISPLAY,CHECKS
To MODIFY fields, requires RACF Authorization:

```
  NP   NAME                    CheckOwner   State          Status

F HZSPROC,DISPLAY,CHECKS
HZS0200I 16.29.48 CHECK SUMMARY     049
CHECK OWNER      CHECK NAME                        STATE STATUS
…
IBMUSS           USS_MAXSOCKETS_MAXFILEPROC         AE   SUCCESSFUL
IBMCS            CSTCP_IPMAXRT6_TCPIPC              AE   SUCCESSFUL
IBMCS            CSTCP_IPMAXRT4_TCPIPC              AE   SUCCESSFUL
IBMCS            CSTCP_CINET_PORTRNG_RSV_TCPIPC     AD   ENV N/A
IBMCS            CSTCP_SYSPLEXMON_RECOV_TCPIPC      AE   EXCEPTION-LOW
IBMCS            CSTCP_TCPMAXRCVBUFRSIZE_TCPIPC     AE   SUCCESSFUL
IBMCS            CSTCP_SYSTCPIP_CTRACE_TCPIPC       AE   SUCCESSFUL
IBMCS            ZOSMIGV1R11_CS_DNSBIND9            IE   INACTIVE
IBMCS            CSVTAM_T1BUF_T2BUF_NOEE            AE   SUCCESSFUL
IBMCS            CSVTAM_VIT_OPT_ALL                 AE   SUCCESSFUL
IBMCS            CSVTAM_VIT_OPT_PSSSMS              AE   SUCCESSFUL
IBMCS            CSVTAM_CSM_STG_LIMIT               AE   SUCCESSFUL
IBMCS            CSRES_AUTOQ_RESOLVEVIA             AE   SUCCESSFUL
IBMCS            CSRES_AUTOQ_TIMEOUT                AE   SUCCESSFUL
IBMCS            CSRES_AUTOQ_GLOBALTCPIPDATA        AE   SUCCESSFUL
```

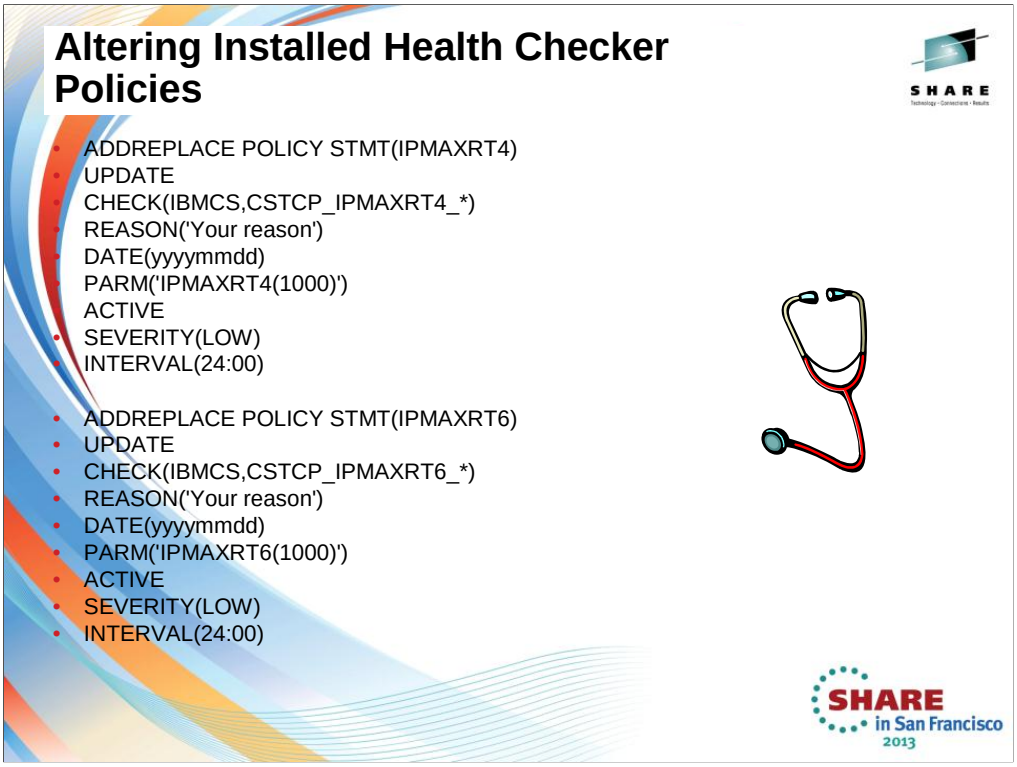
SHARE in San Francisco 2013

Some Checks have been Suppressed in this display.

EXCEPTION = Status is not acceptable; investigate

SUCCESSFUL = Following Best Practices

ENV N/A == Not Applicable to this environment



Managing checks includes tasks such as:

- Updating or overriding values defined for checks or check output, such as check interval, check severity, or check message routing code or WTO type
- Making checks active or inactive
- Requesting that the system process HZSPRMxx parmlib members
- Adding checks
- Deleting checks
- Refreshing checks (deleting then adding) checks
- Displaying check information

You can manage checks with the following interfaces:

1. **Make dynamic, temporary changes** to checks such as deactivating, adding, running, or temporarily updating check values, using:
    - **SDSF**
    - **MODIFY** command

    These types of modification require RACF authorization to HZS.MVS1.IBMCS.CSTCP_IPMAXRT6_TCPIP1.UPDATE CL(XFACILIT).

    Example:

CLASS NAME of XFACILIT HZS.** (G) and GROUP CLASS NAME of GXFACILI

For permanent changes, you must put these policies into the HZSPRMxx member.

1. **Make persistent changes** to checks that persist across check refreshes and restart of IBM Health Checker for z/OS using policies.
    - You can define policies by
        - specifying policy statements to be in your **HZSPRMxx** parmlib member or members,
        - specifying the parmlib member is in the list of parmlib members being used at the start IBM Health Checker for z/OS, and activating the policy.

#SHAREorg

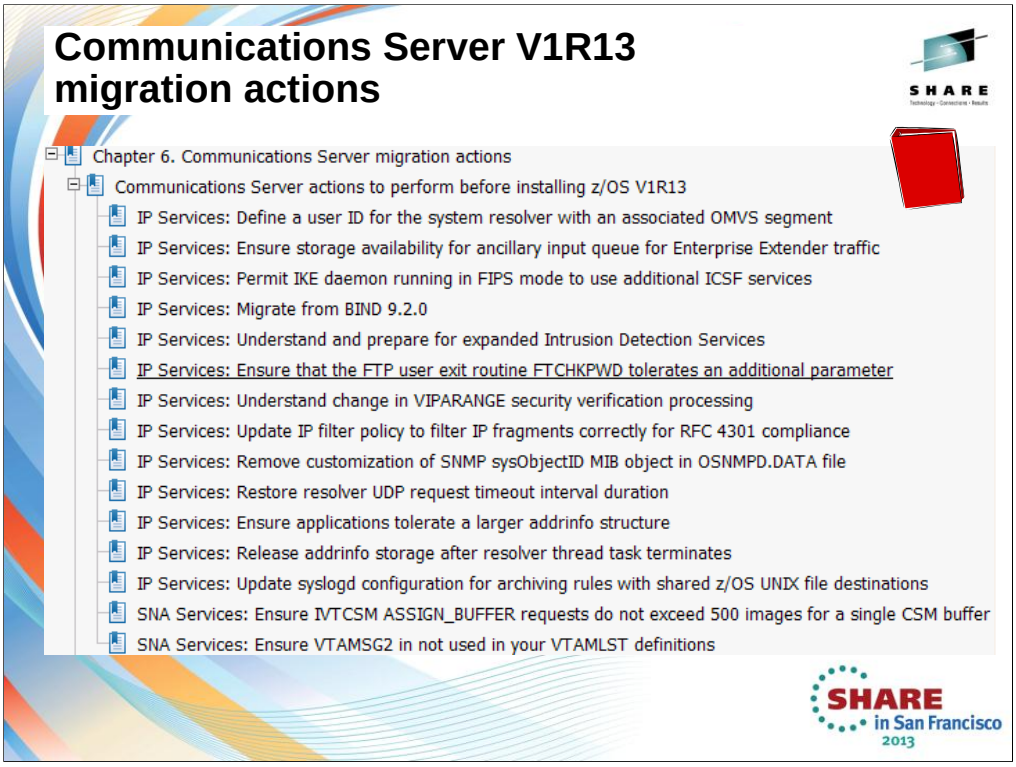
SHARE

3b: Health Check Resources: Using IBM Manuals for a Health Check

z/OS Migration (GA22-7499)

z/OS Communications Server New Function Summary (GC31-8771)

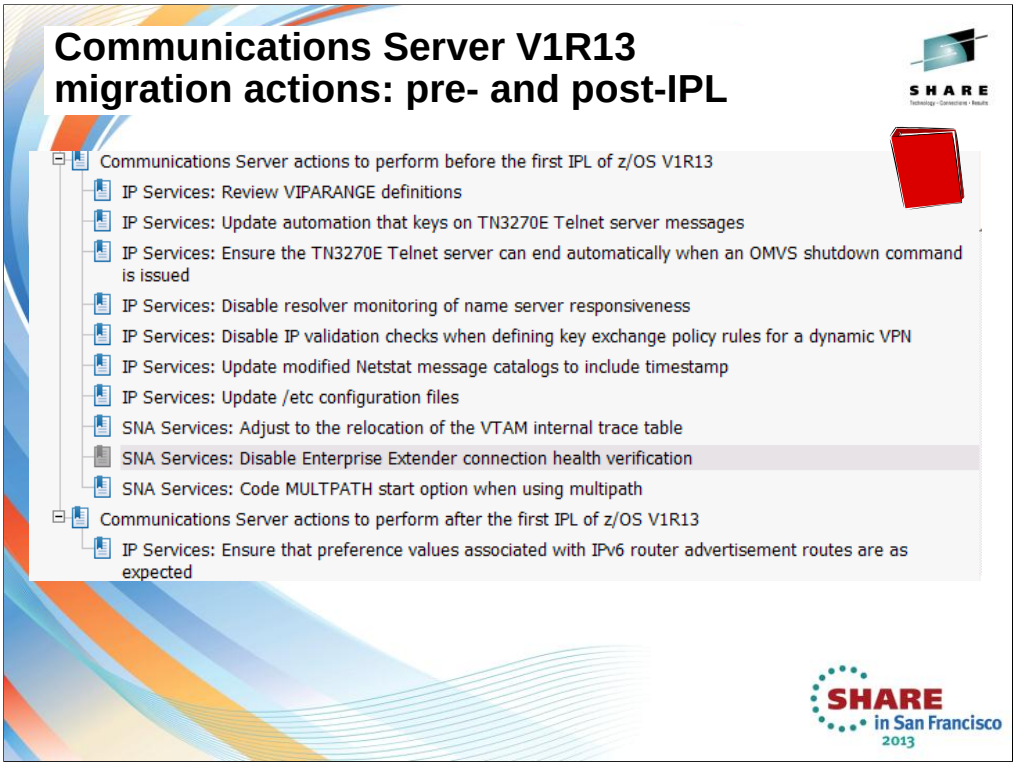
SHARE in San Francisco 2013



This is an excerpt from the table of contents of z/OS Migration (GA22-7499) .

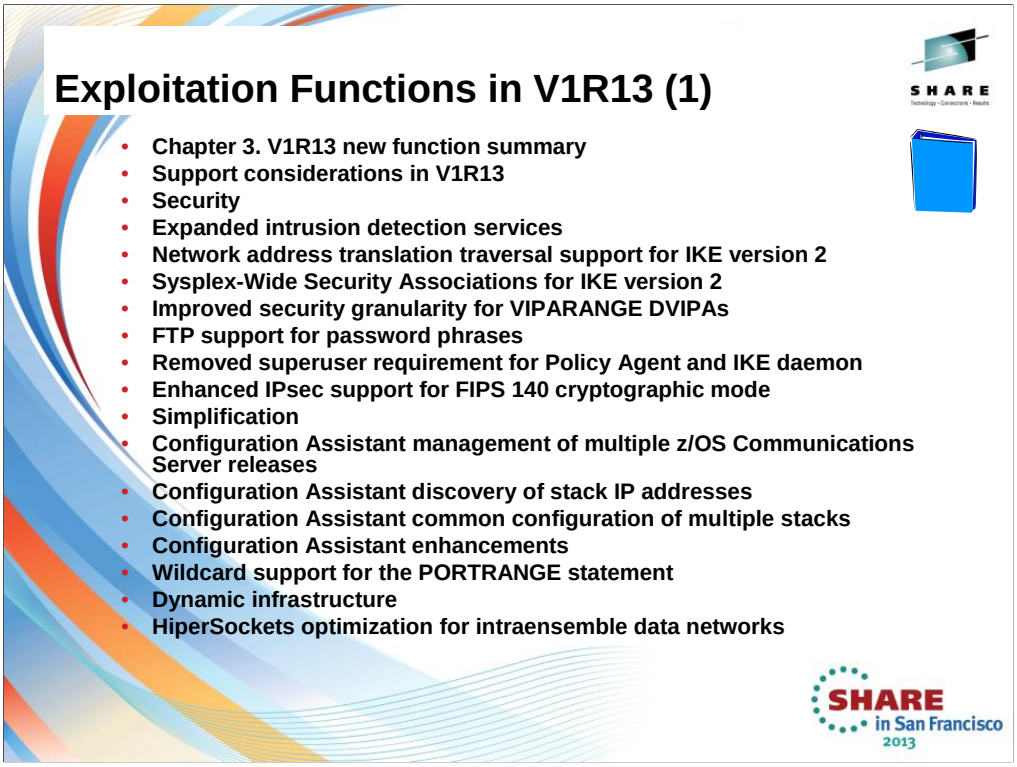
When migrating to a new release, most installations will follow the steps on these two pages. But they often do not get to the new functions that are available in the latest release.

.

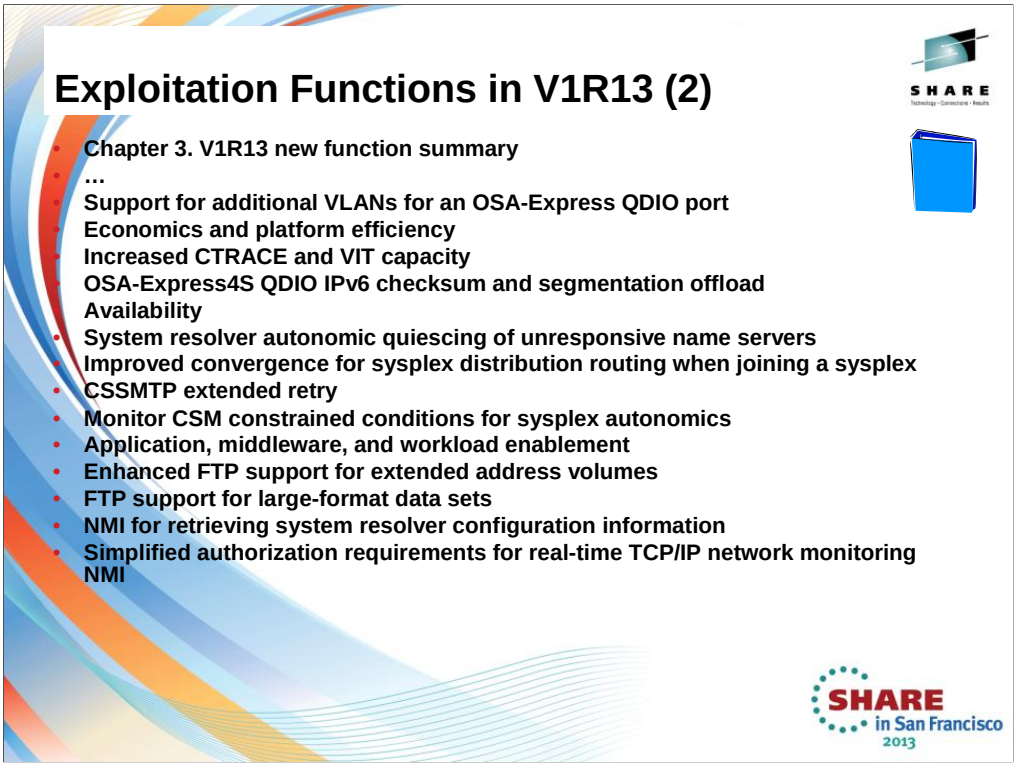


This is an excerpt from the table of contents of z/OS Migration (GA22-7499) .

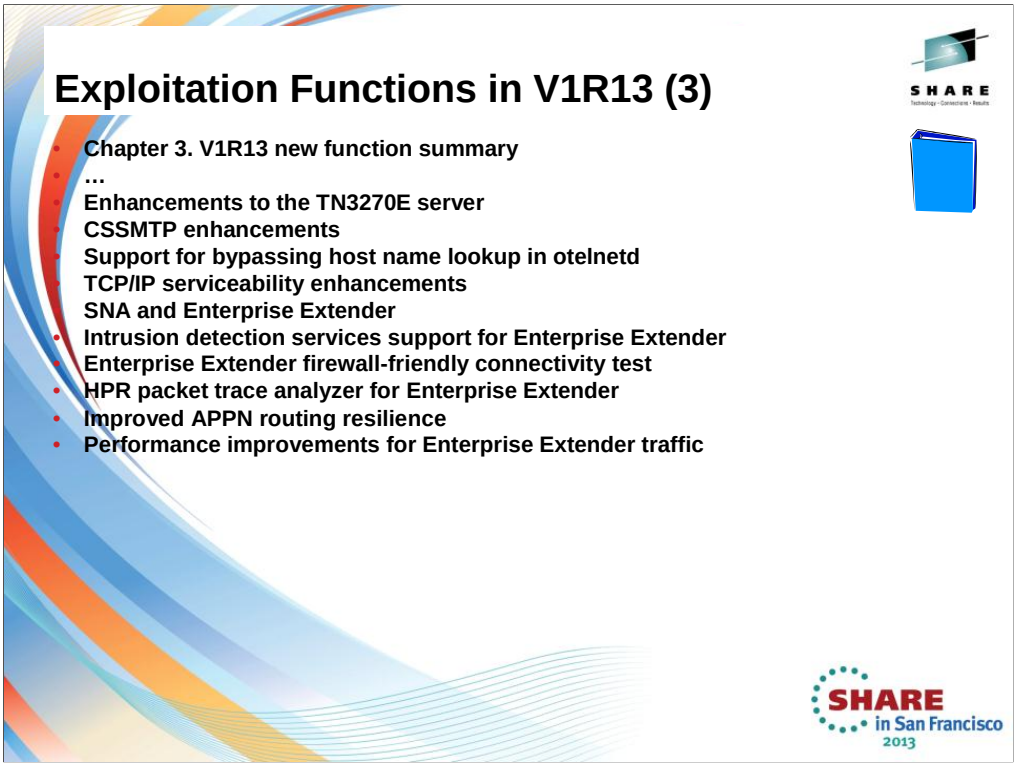
When migrating to a new release, most installations will follow the steps on these two pages. But they often do not get to the new functions that are available in the latest release. This is what the next page shows you.



This is an excerpt from the table of contents of **z/OS Communications Server New Function Summary (GC31-8771).**

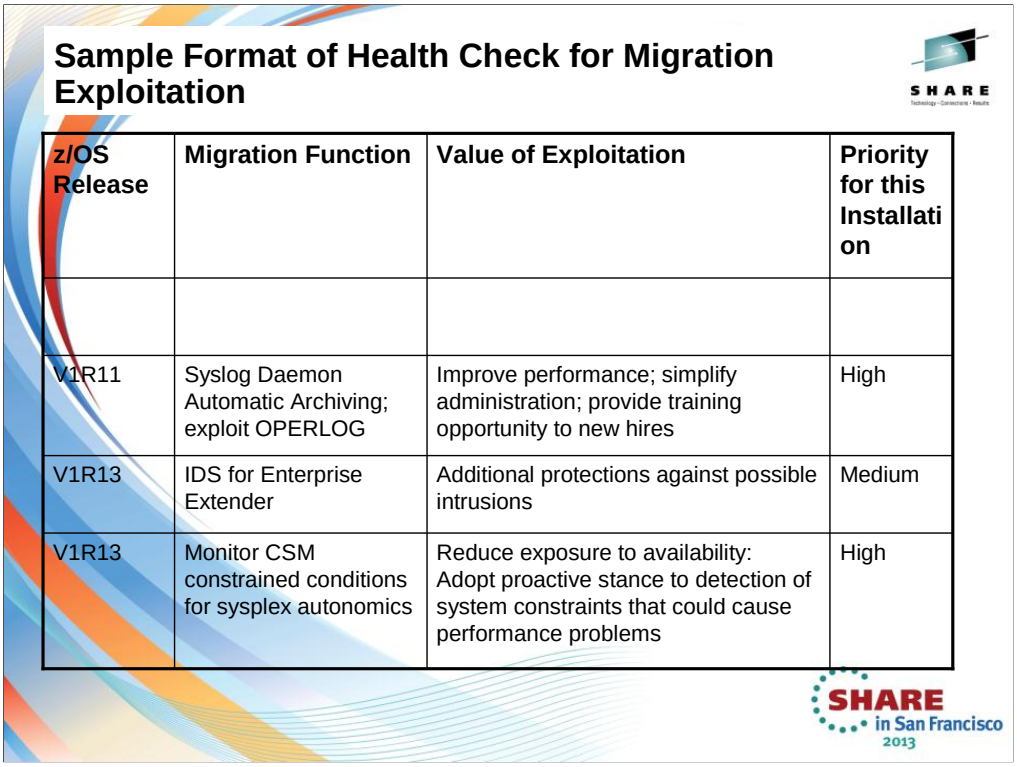


This is an excerpt from the table of contents of **z/OS Communications Server New Function Summary (GC31-8771).**



This is an excerpt from the table of contents of **z/OS Communications Server New Function Summary (GC31-8771).**

Sample Format of Health Check for Migration Exploitation



z/OS Release	Migration Function	Value of Exploitation	Priority for this Installation
V1R11	Syslog Daemon Automatic Archiving; exploit OPERLOG	Improve performance; simplify administration; provide training opportunity to new hires	High
V1R13	IDS for Enterprise Extender	Additional protections against possible intrusions	Medium
V1R13	Monitor CSM constrained conditions for sysplex autonomics	Reduce exposure to availability: Adopt proactive stance to detection of system constraints that could cause performance problems	High

This is a simple sample of the format of a health check report that has been conducted for the purposes of deciding which new release functions to exploit.

#SHAREorg

SHARE

3c. Health Check Resources: Where to Discover Best Practices?

- High Availability?
- Coding Practices?
- Performance Exposures?

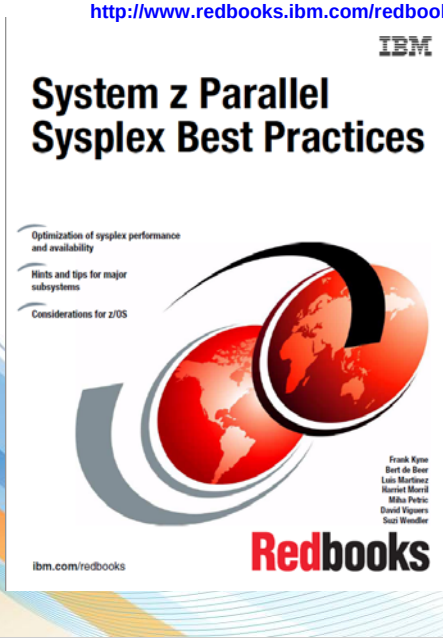
SHARE in San Francisco 2013

What is a “Best Practice”?

- A suggested or recommended practice
  - Sometimes documented as a “Best Practice” by IBM or the industry
  - At other times it is a generally followed practice that has not been formally documented
- A rule of thumb
- May be deviated from when the occasion requires it
- Often documented in:
  - RFCs from the IETF
  - Formal publications produced by a product developer
  - Conference Presentations
  - Product Websites
  - Blogs

Documents to Assist with Best Practices

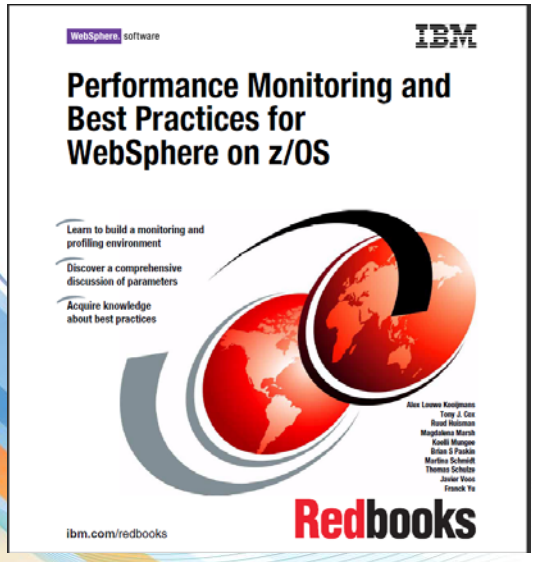
http://www.redbooks.ibm.com/redbooks/pdfs/sg247817.pdf



SHARE in San Francisco 2013

Documents to Assist with Best Practices

http://www.redbooks.ibm.com/redbooks/pdfs/sg247269.pdf



SHARE in San Francisco 2013

DeveloperWorks for Best Practices: DB2, z/OS

https://www.ibm.com/developerworks/mydeveloperworks/blogs/SusanVisser/entry/more_on_db2_for_z_os_best_practices5?lang=en

- "Best Practices for DB2 for z/OS V10 Migration Planning and Very Early experiences" Parts 1 and 2 by John Campbell
  - In this two-part webcast, John gives his perspective of what you need to understand and do when you move to DB2 10. John works with DB2 for z/OS customers around the globe and has extensive experience.
- "Best Practices for DB2 for z/OS Utilities" Parts 1 and 2 by Haakon Roberts
  - These recommendations come straight from the engineering team who produce the software and give to practical advice on what you need to do to effectively use the utilities.
- "Best Practices for DB2 for z/OS DDF Connectivity" by John Campbell
- "Best Practices for z/OS Locks and Latches by John Campbell
- "Best Practices for z/OS Local and Group Bufferpools" by John Campbell
- "Best Practices for z/OS Log Activity and Miscellaneous" by John Campbell
  - The above four titles draw on John's experiences working with customers. They summarize his recommendations in these functional areas of DB2 for z/OS.

Best Practices for Tivoli Products on z/OS

http://www.ibm.com/developerworks/wikis/download/attachments/141165182/IBM_Tivoli_zOM_and+Related_links.pdf?version=1

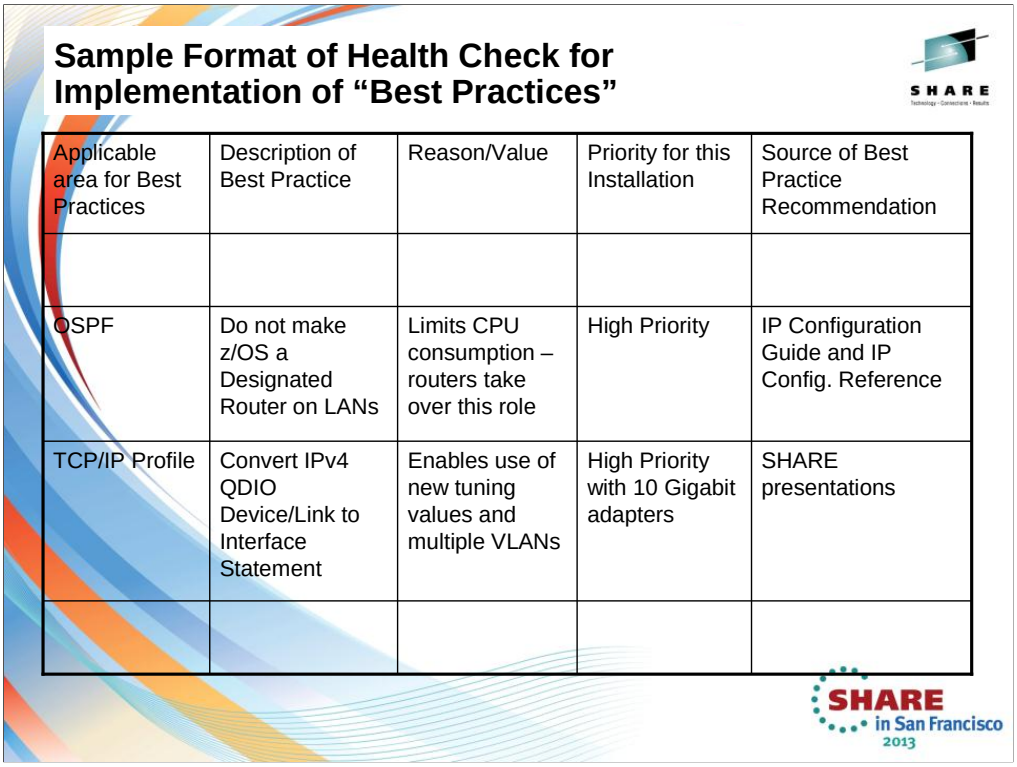
Contents

SHARE in San Francisco 2013

Using z/OS Health Checker for Best Practices

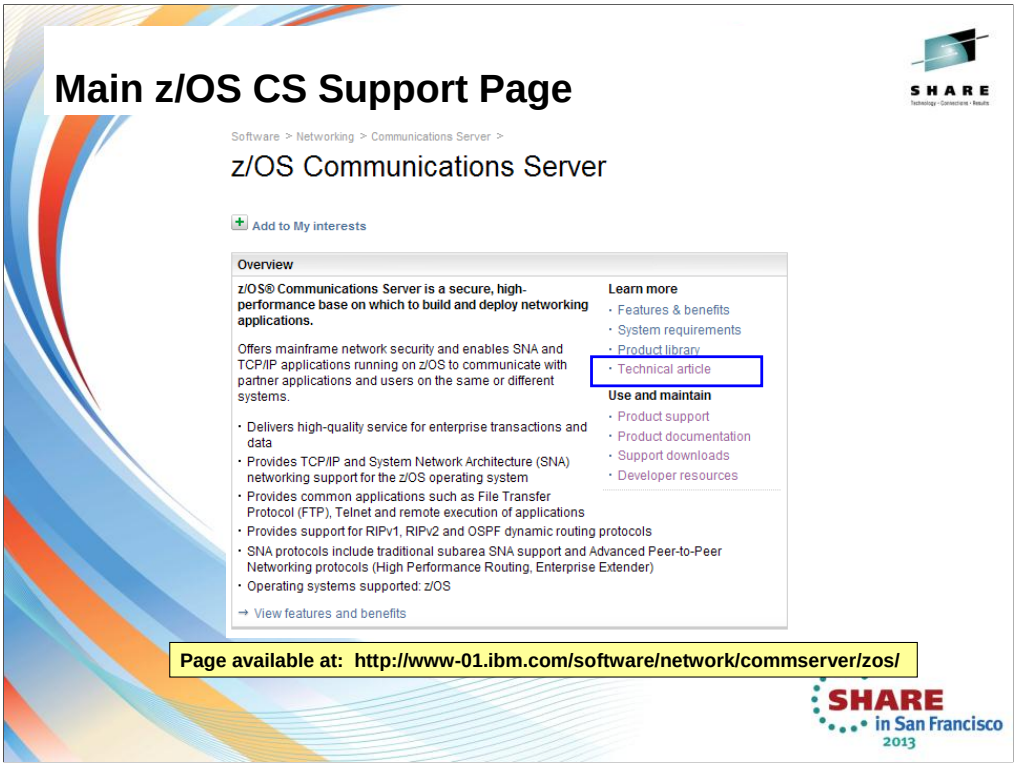
- http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp?topic=/com.ibm.iea.zos/zos/1.0/EaseOfUse/zOSHealthCheckerOverview/player.html

This page shows you how to reach a Video that explains the purposes and uses of z/OS Health Checker.

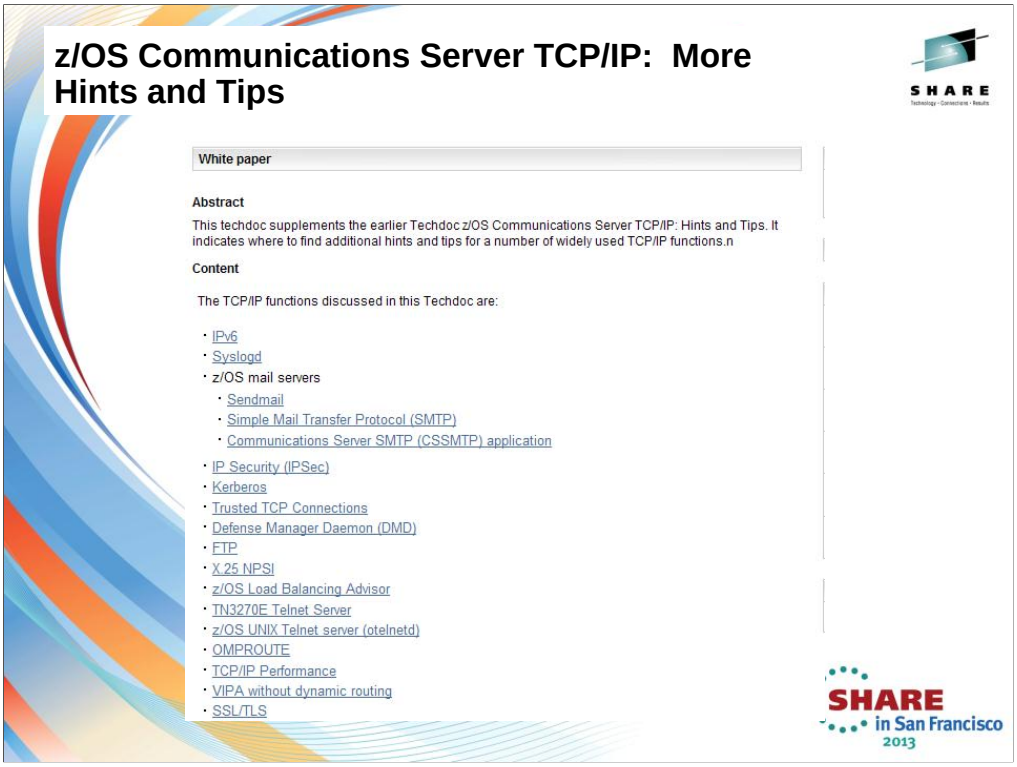


This is a simple sample of the format of a health check report that has been conducted for the purposes of deciding which new release functions to exploit.

Main z/OS CS Support Page



The page is found at: http://www-01.ibm.com/software/network/commserver/zos/

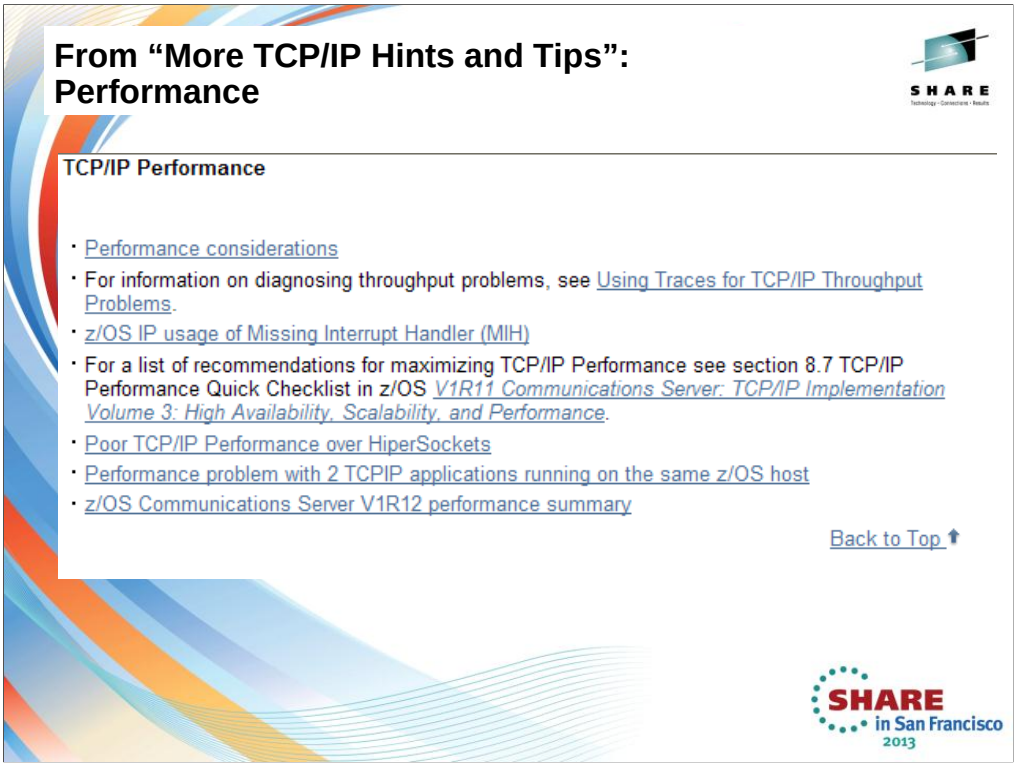


The web page for this information is http://www-01.ibm.com/support/docview.wss?uid=swg27019687

You reach this page by going to …

http://www-01.ibm.com/software/network/commserver/zos/ and then selecting “Technical Articles”.

http://www-01.ibm.com/support/docview.wss?rs=852&uid=swg27006776

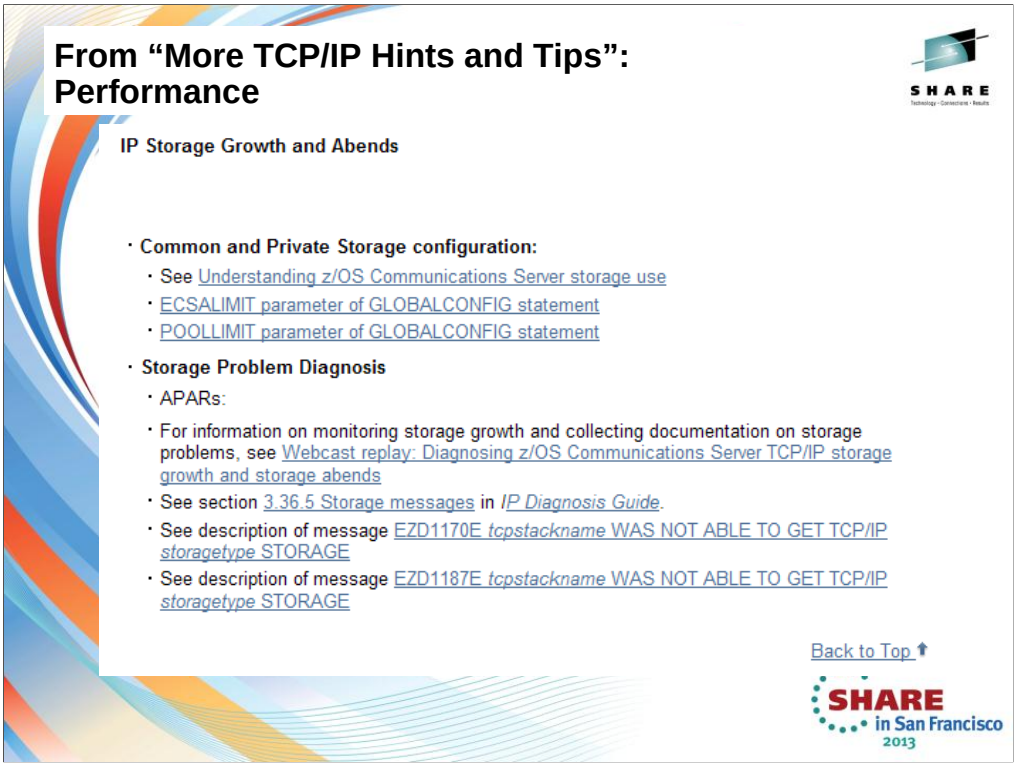


The web page for this information is http://www-01.ibm.com/support/docview.wss?uid=swg27019687

You reach this page by going to …

http://www-01.ibm.com/software/network/commserver/zos/ and then selecting “Technical Articles”.

http://www-01.ibm.com/support/docview.wss?rs=852&uid=swg27006776

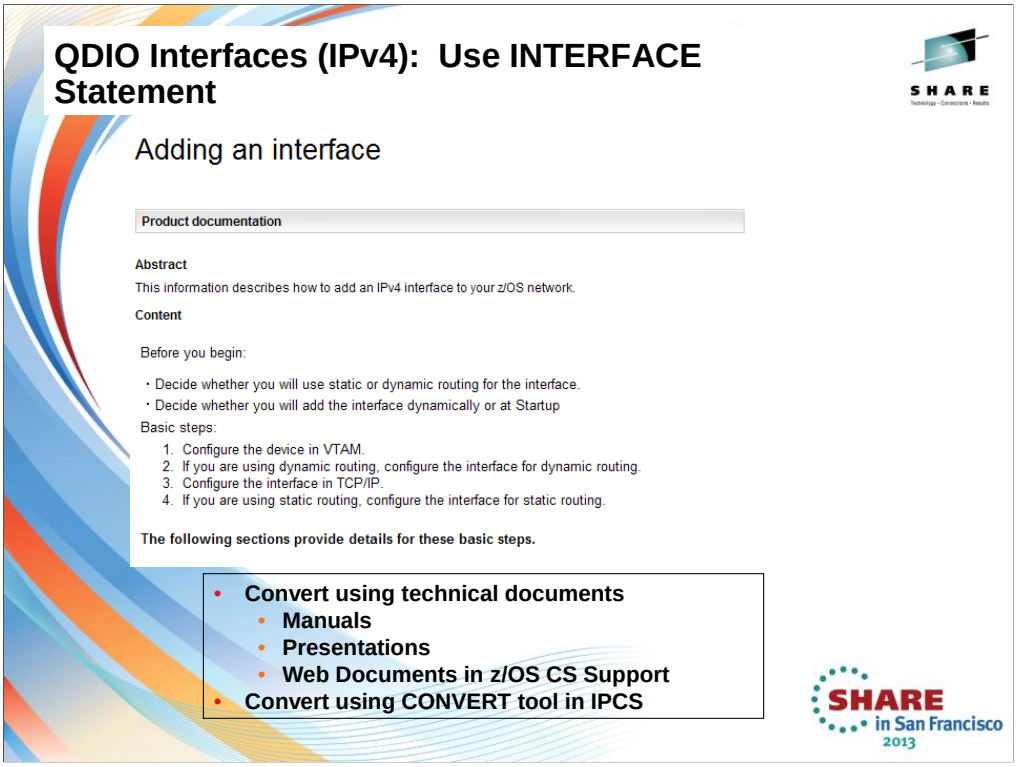


The web page for this information is http://www-01.ibm.com/support/docview.wss?uid=swg27019687

You reach this page by going to …

http://www-01.ibm.com/software/network/commserver/zos/ and then selecting “Technical Articles”.

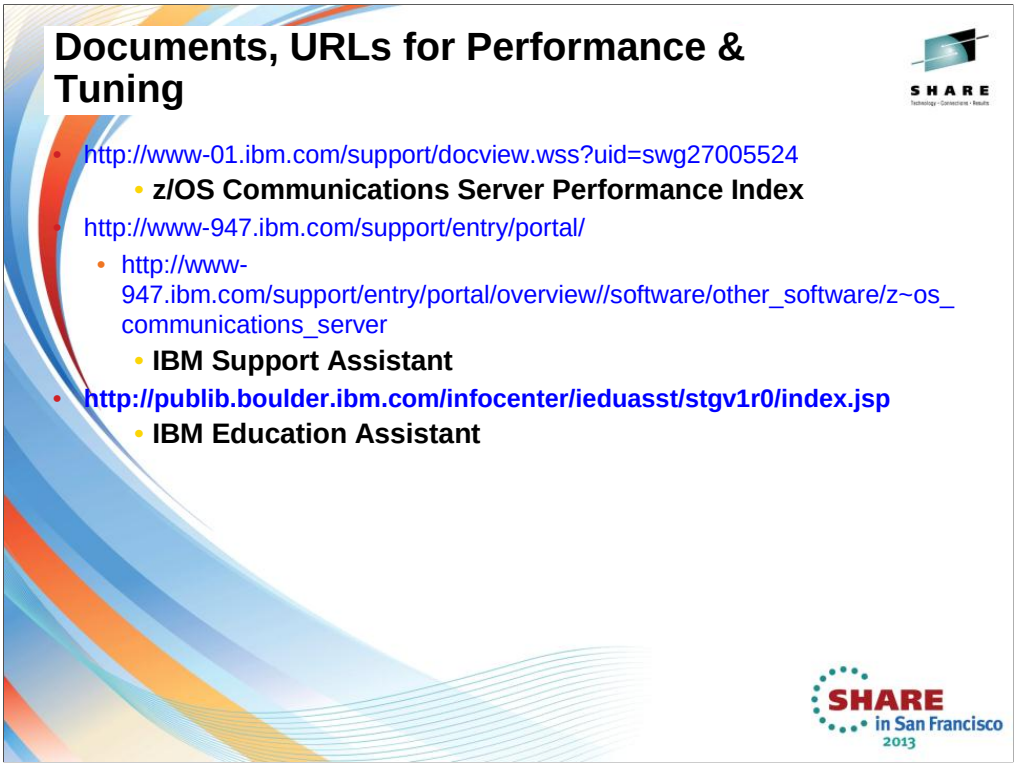
http://www-01.ibm.com/support/docview.wss?rs=852&uid=swg27006776



One Best Practice recommended in various SHARE presentations and IBM Manuals is to convert IPv4 QDIO DEVICE/LINK definitions to INTERFACE definitions. The IP Configuration Reference and Guide show you how to perform this conversion with a step-by-step approach. The IP Diagnosis Guide shows you how to use the CONVERT tool within IPCS to assist you with this conversion.

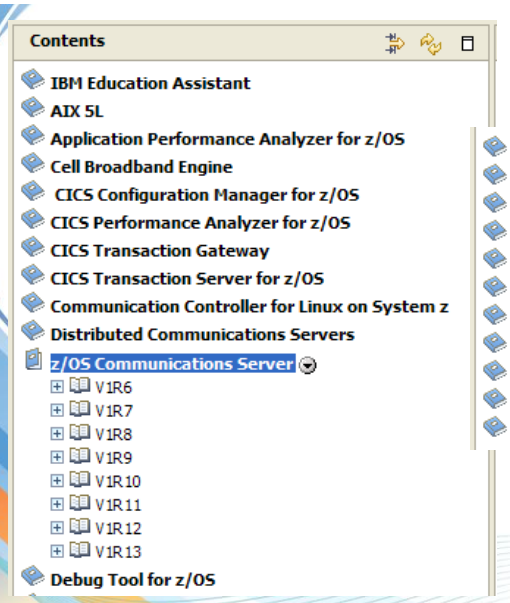
The web page depicted is available at http://www-01.ibm.com/support/docview.wss?uid=swg27011208.

This web page is reached by selecting the item for *"Adding an Interface"* from: "**z/OS Communications Server TCP/IP: More Hints and Tips**" at http://www-01.ibm.com/support/docview.wss?uid=swg27019687



See the appendix of this document to find out about Web portals like the IBM Support Assistant and IBM Education Assistant, which will help you navigate to performance and tuning sites for various components, including z/OS Communications Server.

IBM Education Assistant (1)



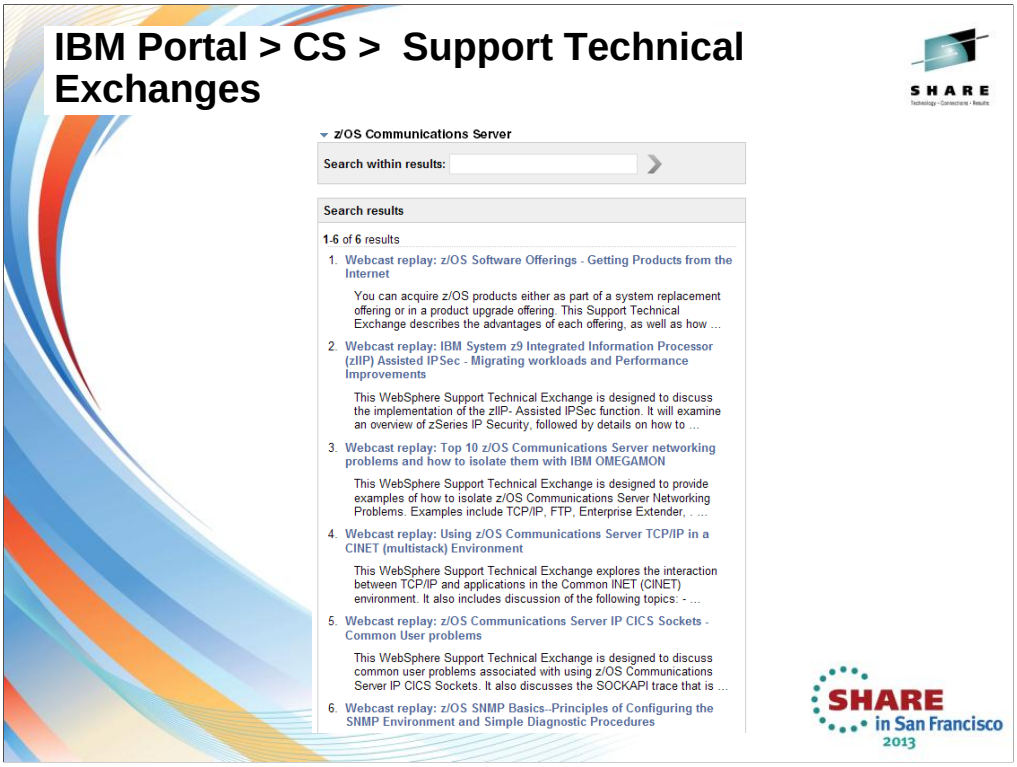
IBM Education Assistant (2)

z/OS Communications Server

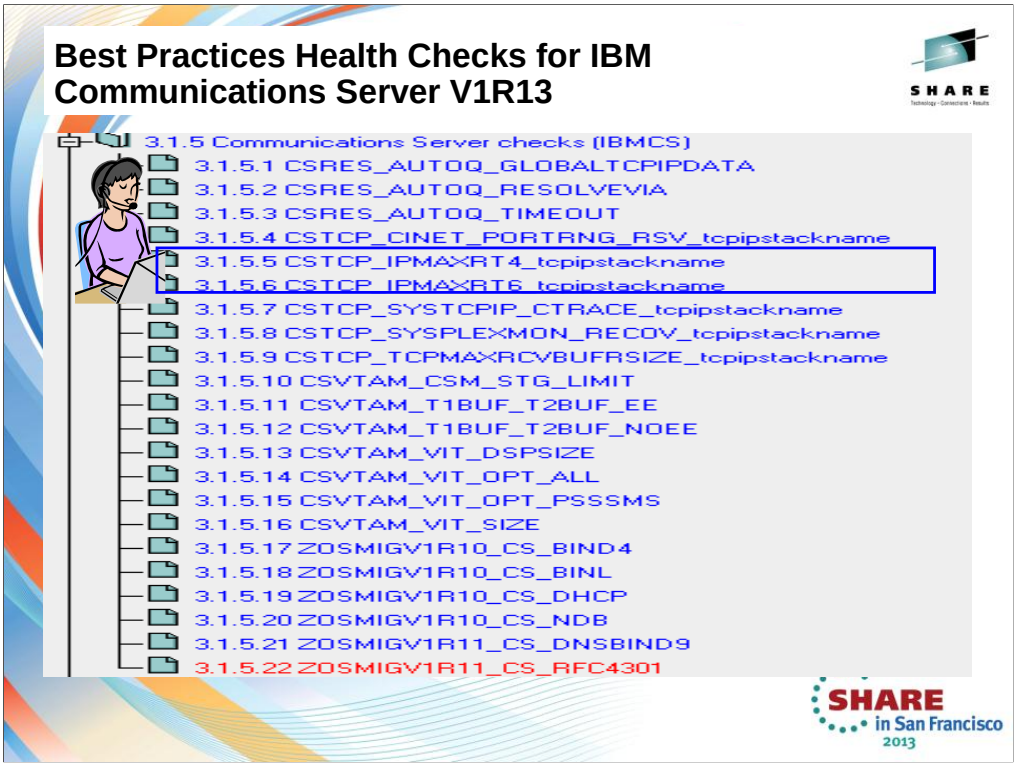
- V1R6
- V1R7
- V1R8
- V1R9
- V1R10
- V1R11
- V1R12
- V1R13

Additional resources

- z/OS Communications Server product information
- z/OS basic skills information center
- z/OS internet library
- z/OS product information



The Communications Server Support Technical Exchanges are reached from the general Support Portal. Once you choose Communications Server on that portal, you can select the Support Technical Exchanges. The illustrated page is at http://www-947.ibm.com/support/entry/portal/previous_tech_exchanges/software/other_software/z~os_communications_server



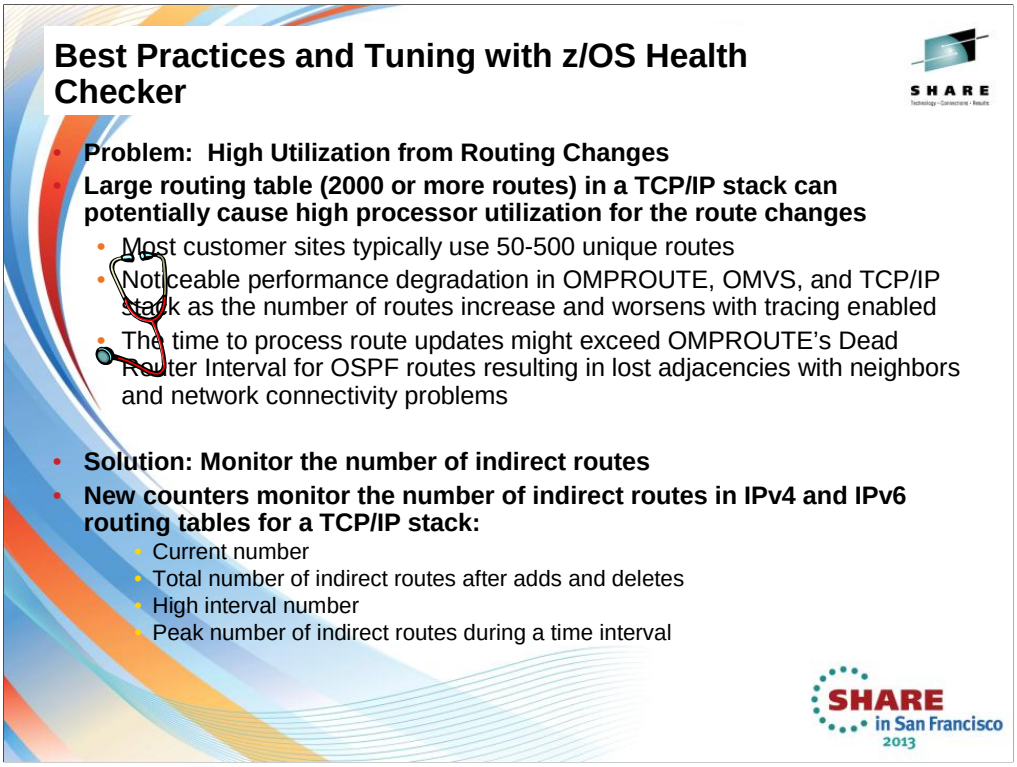
We'll be adding more checks to IBM Health Checker for z/OS periodically, both as APARs and integrated into z/OS. For the most up-to-date information on checks available, see the following Web site:

http://www.ibm.com/servers/eserver/zseries/zos/hchecker/check_table.html

EXCEPT = Status is not acceptable; investigate

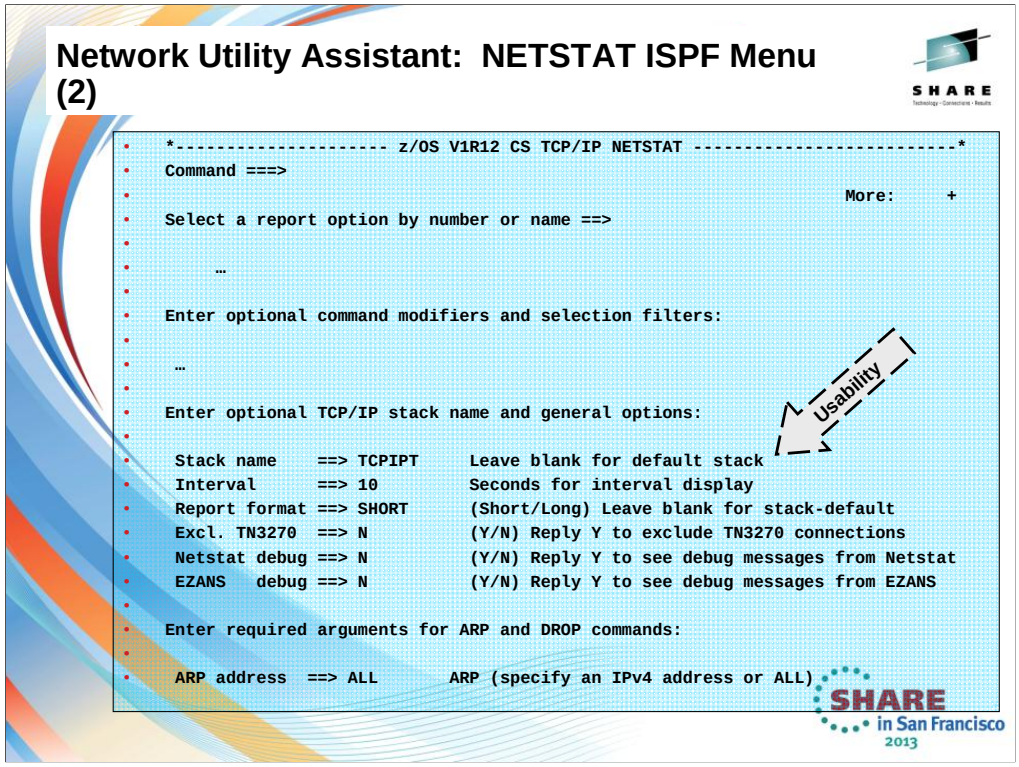
SUCCESS = Following Best Practices

ENV N/ == Not Applicable to this environment



- A routing table that is considered to be excessive (2000 routes or more) can cause inefficiency in network design and less than optimal performance for OMPROUTE and TCP/IP. Most z/OS sites appear to have 50-500 unique routes. IBM service frequently tells customers with more than 2000 routes to reduce the number of routes after determining that performance degradations in OMPROUTE and TCP/IP were caused by the excessive number of routes. The overall performance degrades further with tracing enabled.
- There have been a small number of customers over the years who have attempted to configure many thousands of routes (from both dynamic and static routing protocols) on z/OS when they only needed 100 or so. Most of the time, having many thousands of routes will not cause a problem. However, if all of the routes ever need to be deleted or added at the same time, then high processor consumption might be seen in the TCP/IP stack or in OMVS. Many thousands of routing updates have to be processed to make the routing changes.
- Also, because the OSPF routing protocol in OMPROUTE uses short-interval timers, the time to process the many thousands of routing updates might exceed the OSPF dead router intervals. This results in OSPF adjacency losses with neighbors and contributes to network connectivity problems.
- These counters are used by IBMHC for the health check monitoring and for input into the informational and warning messages. The current number is incremented and decremented at times of the route table updates. The high interval number is set to the peak number of indirect routes during a time interval and is reset to the current number for the next time interval.
- IBM Health Checker will perform checks at these times:
    1. One-time check (30 minutes after TCP/IP initialization)
        - For initial health state after routing table updates by TCP/IP and OMPROUTE
        - Not done if IBM Health Checker started 30 minutes after TCP/IP initialization or if interval check is less than 30 minutes
    2. Interval checks (defaults to 168 hours or weekly)
    3. Immediate checks (at any time) when:
        - A counter has exceeded the maximum threshold (default 2000)
        - A maximum threshold value has been dynamically modified by an operator

Network Utility Assistant: NETSTAT ISPF Menu (2)



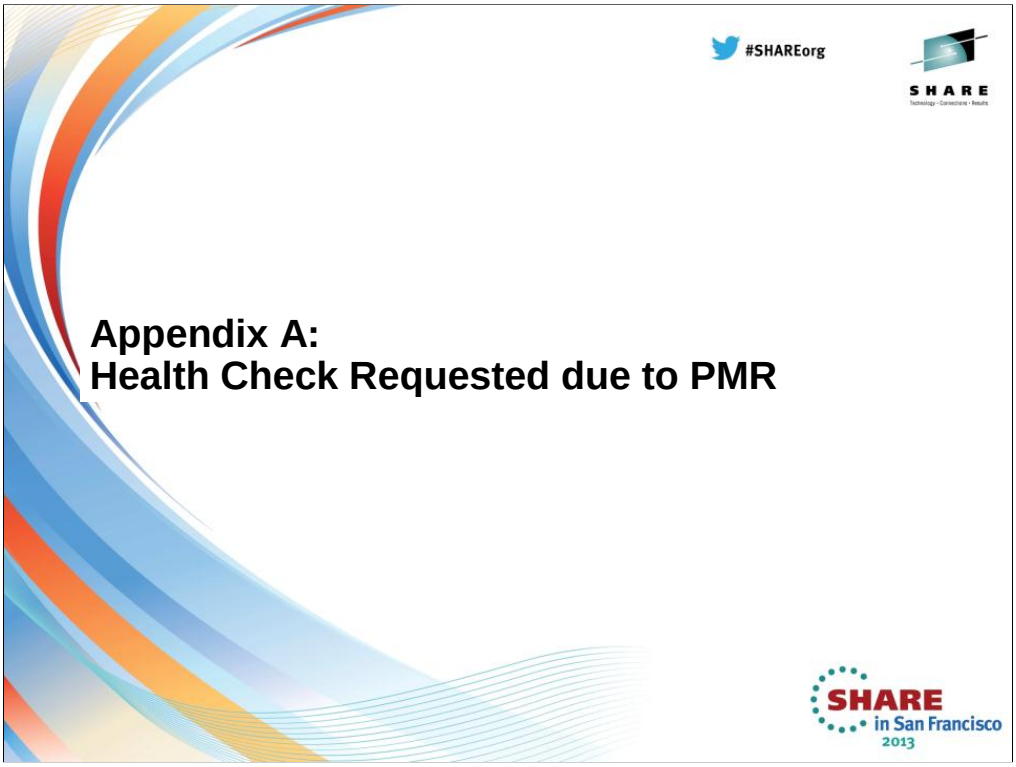
This shows you that the many parameters of the NETSTAT command can be more easily managed if you exploit the tool known as the z/OS Communications Server Network Utility Assistant.

Agenda - What you have seen …

1. Description of a “Health Check”
2. Format of a Health Check
3. Networking Documentation for an Educational Health Check
   1. Topology Diagrams
   2. Output from Networking Command Execution
   3. Resources to determine which output to request and what to analyze:
      1. *Migration efforts*
      2. *New Features*
      3. *Best Practices*
4. Sample Health Check Analysis

- We omitted an example of a completed and full report.

- **NOTE: The 75-minute version of this presentation skips pages; the two-hour version presents all pages up to the Appendices.**


#SHAREorg
SHARE
Technology · Connections · Results
Appendix A:
Health Check Requested due to PMR
SHARE
in San Francisco
2013

Reporting a Software Connections problem

1)Complete Description of error, which includes:
- 1)z/OS Version and Release numbers that error(s) occurred on
- 2)Error Messages and Sense Codes or Error Codes received in:
  - 1)User interface, and/or MVS Log, and or SYSLOGD log, and/or Job Log
- 3)Description of Topology, possibly accompanied by a relevant diagram
  - 1)Origin and Destination Node and Names and or Addresses
    - 1)Logical Connectivity of the Partners
  - 2)Origin and Destination LUs or IP Identities/addresses
- 4)Description of what – if anything – changed prior to the appearance of the error

2)Problem should be opened by the person most familiar with the above information
- 1)Not by an administrator who may not understand the facts.

Consult the SNA DIAGNOSIS Manuals and the IP Diagnosis Guide

Documents to Assist with Reporting a Problem

- *SNA Diagnosis Manual, Volume 1 (GC31-6850)*
- *SNA Diagnosis Manual, Volume 2 (GC31-6851)*

PART 1: Diagnostic Techniques

Chapter 1. Diagnosing VTAM problems: Where to begin
Chapter 2. Collecting documentation for specific types of problems
Chapter 3. Collecting documentation for TSO/VTAM problems

PART 2: Diagnostic Procedures

Chapter 4. Using DISPLAY and MODIFY operator commands
Chapter 5. Using dumps
Chapter 6. Using VTAM dump analysis tools
Chapter 7. Using traces
Chapter 8. Using the VIT analysis tool
Chapter 9. Using other problem solving tools
……..etc ……..

Documents to Assist with Reporting a Problem

- *IP Diagnosis Guide (GC31-8782)*

PART 1: General Diagnosis information

Chapter 1. Overview of diagnosis procedure
Chapter 2. Selecting tools and service aids
Chapter 3. Diagnosing abends, loops, and hangs
Chapter 4. Diagnosing network connectivity problems

Part 2. Traces and control blocks

Chapter 5. TCP/IP services traces and IPCS support
Chapter 6. IPCS subcommands for TCP/IP

Part 3. Diagnosing z/OS Communications Server components
Chapter …
Chapter 9. Diagnosing IKE daemon problems
Chapter …
Chapter 11. Diagnosing dynamic VIPA and sysplex problems
Chapter 14. Diagnosing File Transfer Protocol (FTP) problems
Chapter …
Chapter 16. Diagnosing Telnet problems
Chapter …
Chapter 29. Diagnosing Application Transparent Transport Layer Security (AT-TLS)
……etc ……

IP Diagnosis Manual – Network Connectivity Problem

- In most cases, persistent error conditions indicate an installation or configuration problem. Contact the local IBM branch office for installation assistance.
- If a software defect is suspected, collect the following information before contacting the IBM Support Center:
  - PROFILE.TCPIP
  - TCPIP.DATA
  - Output from Netstat commands. If using policy-based routing, collect Netstat ROUTE/-r output for all possible route tables involved in the failed routing.
  - Output from Ping traces
  - If using policy-based routing, output from **pasearch** commands
  - Network diagram or layout
  - **Error messages received**. Refer to *z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)* for information about messages.
  - Component traces, see Chapter 5, “TCP/IP services traces and IPCS support,” on page 45
  - If using dynamic routing protocols for IP route table management, see the following information:
    - – Chapter 32, “Diagnosing OMPROUTE problems,” on page 757
    - – Chapter 33, “Diagnosing NCPROUTE problems,” on page 787

VTAM Display of VTAMOPTS Messages (1)

```
D NET,VTAMOPTS
IST097I DISPLAY ACCEPTED
IST1188I VTAM CSV1R12 STARTED AT 20:04:13 ON 06/20/12 187
IST1349I COMPONENT ID IS 5695-11701-1C0
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I AFFDELAY = 600                  ALSREQ   = NO
IST1189I API64R   = YES                  APPNCOS  = NONE
IST1189I ASIRFMSG = OLUSSCP              ASYDE    = TERM
IST1189I AUTHLEN  = YES                  AUTORTRY = AUTOCAP
IST1189I AUTOTI   = 0                    BN       = NO
IST1189I BNDYN    = ***NA***             BNORD    = ***NA***
IST1189I BSCMDRS  = (STATS,INOPS)        BSCTMOUT = 286
IST1189I CACHETI  = 8                    CDRDYN   = YES
IST1189I CDRSCTI  = 480S                 CDSERVR  = NO
IST1189I CDSREFER = 1                    CINDXSIZ = 8176
IST1189I CMPMIPS  = 100                  CMPVTAM  = 0
IST1189I CNMTAB   = ISTMGC00             CNNRTMSG = SUPPRESS
```

VTAM Display of VTAMOPTS Messages (2)

```
IST1189I COLD     = YES                 CONFIG   = C1
IST1189I CONNTYPE = LEN                 CPCDRSC  = NO
IST1189I CPCP     = NO                  CSALIMIT = 57805K
IST1189I CSA24    = NOLIMIT             DATEFORM = MDY
IST1189I DIALRTRY = YES                 DIRSIZE  = 0
IST1189I DIRTIME  = 691200S             DISCNTIM = (15,0)
IST1189I DLRORDER = (STATNID,FIRST)     DLRTCB   = 32
IST1189I DLURSAW  = YES                 DSIRFMSG = NONE
IST1189I DSPLYDEF = 100                 DSPLYMAX = 65535
IST1189I DSPLYWLD = FULLWILD            DUPDEFS  = ALL
IST1189I DYNADJCP = YES                 DYNASSCP = YES
IST1189I DYNDLGMD = NONE                DYNHPPFX = CNR
IST1189I DYNLU    = YES                 DYNMODTB = NONE
IST1189I DYNPUPFX = CN                  DYNVNPFX = CNV
IST1189I EEPORTCK = NO                  EEVERIFY = ACTIVATE
IST1189I ENCRPREF = NONE                ENCRYPTN = 31
IST1189I ENHADDR  = YES                 ENSEMBLE = NO
```

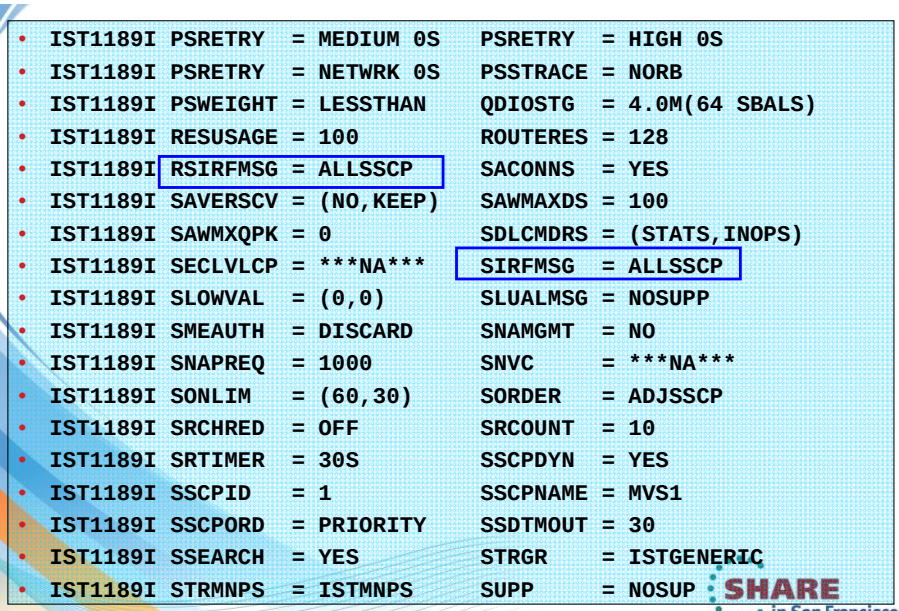
VTAM Display of VTAMOPTS Messages (3)

```
IST1189I ESIRFMSG = ALLSSCP     EXPFLTRM = 0
IST1189I FLDTAB   = ISTMSFLD    FSIRFMSG = OLUSSCP
IST1189I GWSSCP   = YES         HNTSIZE  = 4080
IST1189I HOSTNAME = *BLANKS*    HOSTPU   = MVSPUS
IST1189I HOSTSA   = 1           HOTIOTRM = 0
IST1189I HPR      = (RTP,RTP)   HPRARB   = RESPMODE
IST1189I HPRCLKRT = STANDARD    HPRITMSG = BASE
IST1189I HPRNCPBF = NO          HPRPSDLY = 0
IST1189I HPRPSMSG = ALL         HPRPST   = LOW          480S
IST1189I HPRPST   = MEDIUM 240S HPRPST   = HIGH         120S
IST1189I HPRPST   = NETWRK  60S HPRSESLM = NOLIMIT
IST1189I HPRSTALL = 0           HSRTSIZE = 9973
IST1189I INITDB   = ALL         INOPDUMP = OFF
IST1189I IOINT    = 180         IOMSGLIM = 100
IST1189I IOPURGE  = 60S         IPADDR   = 0.0.0.0
IST1189I IPINFO   = SENDALL     IQDCHPID = DF
IST1189I IQDIOSTG = 7.8M(126 SBALS)   IRNSTRGE = 0
IST1189I ISTCOSDF = INDLU       LIMINTCP = ***NA***
```

VTAM Display of VTAMOPTS Messages (4)

```
IST1189I LIST     = C1          LSIRFMSG = NONE
IST1189I MAINTLVL = *BLANKS*    MAXEETST = 500
IST1189I MAXHNRES = 100         MAXLOCAT = 5000
IST1189I MAXLURU  = 6144        MAXSSCPS = 10
IST1189I MAXSUBA  = 127         MIHTMOUT = 1800
IST1189I MPCACT   = WAIT        MSGLEVEL = CS390
IST1189I MSGMOD   = NO          MULTPATH = NO
IST1189I MXSAWBUF = 10000       MXSSCPRU = 4096
IST1189I MXSUBNUM = 511         NCPBUFSZ = 512
IST1189I NETID    = NET1        NMVTLOG  = NPDA
IST1189I NNSPREF  = ***NA***    NODELST  = *BLANKS*
IST1189I NODETYPE = NN          NQNMODE  = NQNAME
IST1189I NSRTSIZE = *BLANKS*    NUMTREES = 100
IST1189I OSIEVENT = PATTERNS    OSIMGMT  = YES
IST1189I OSITOPO  = ILUCDRSC    OSRTSIZE = 43
IST1189I PDTRCBUF = 2           PIUMAXDS = 200
IST1189I PLUALMSG = NOSUPP      PMTUD    = TCPVALUE
IST1189I PPOLOG   = YES         PSRETRY  = LOW 0S
```

VTAM Display of VTAMOPTS Messages (5)



```
IST1189I PSRETRY  = MEDIUM 0S    PSRETRY  = HIGH 0S
IST1189I PSRETRY  = NETWRK 0S    PSSTRACE = NORB
IST1189I PSWEIGHT = LESSTHAN     QDIOSTG  = 4.0M(64 SBALS)
IST1189I RESUSAGE = 100          ROUTERES = 128
IST1189I RSIRFMSG = ALLSSCP      SACONNS  = YES
IST1189I SAVERSCV = (NO,KEEP)    SAWMAXDS = 100
IST1189I SAWMXQPK = 0            SDLCMDRS = (STATS,INOPS)
IST1189I SECLVLCP = ***NA***     SIRFMSG  = ALLSSCP
IST1189I SLOWVAL  = (0,0)        SLUALMSG = NOSUPP
IST1189I SMEAUTH  = DISCARD      SNAMGMT  = NO
IST1189I SNAPREQ  = 1000         SNVC     = ***NA***
IST1189I SONLIM   = (60,30)      SORDER   = ADJSSCP
IST1189I SRCHRED  = OFF          SRCOUNT  = 10
IST1189I SRTIMER  = 30S          SSCPDYN  = YES
IST1189I SSCPID   = 1            SSCPNAME = MVS1
IST1189I SSCPORD  = PRIORITY     SSDTMOUT = 30
IST1189I SSEARCH  = YES          STRGR    = ISTGENERIC
IST1189I STRMNPS  = ISTMNPS      SUPP     = NOSUP
```

VTAM Display of VTAMOPTS Messages (6)

```
IST1189I SWNORDER = (CPNAME,FIRST)     TCPNAME  = *BLANKS*
IST1189I TDUDIAG  = 1000               TNSTAT   = OFF
IST1189I TOPOTIME = 20:04        TRANSLAT = (0,1,2,3,4,5,6,7)
IST1189I UNRCHTIM = (0,0)              UPDDELAY = 60S
IST1189I USSTAB   = *BLANKS*           VARYWLD  = FULLWILD
IST1189I VERIFYCP = NONE               VFYRED   = YES
IST1189I VFYREDTI = OFF                VOSDEACT = NO
IST1189I VRTG     = NO                 VRTGCPCP = YES
IST1189I VTAMEAS  = 32001              WARM     = NO
IST1189I XCFGRPID = ***NA***           XCFINIT  = YES
IST1189I XNETALS  = YES
IST314I END
```

VTAM 'Function" Display of VTAMOPTS Messages

```
D NET,VTAMOPTS,FUNCTION=MESSAGES
IST097I DISPLAY ACCEPTED
IST1188I VTAM CSV1R12 STARTED AT 20:04:13 ON 06/20/12 024
IST1349I COMPONENT ID IS 5695-11701-1C0
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I ASIRFMSG = OLUSSCP              CNMTAB   = ISTMGC00
IST1189I CNNRTMSG = SUPPRESS             DSIRFMSG = NONE
IST1189I DSPLYDEF = 100                  DSPLYMAX = 65535
IST1189I DSPLYWLD = FULLWILD             ESIRFMSG = ALLSSCP
IST1189I FLDTAB   = ISTMSFLD             FSIRFMSG = OLUSSCP
IST1189I HPRITMSG = BASE                 HPRPSMSG = ALL
IST1189I IOINT    = 180                  IOMSGLIM = 100
IST1189I LSIRFMSG = NONE                 MSGLEVEL = CS390
IST1189I MSGMOD   = NO                   PLUALMSG = NOSUPP
IST1189I PPOLOG   = YES                  RSIRFMSG = ALLSSCP
IST1189I SIRFMSG  = ALLSSCP              SLOWVAL  = (0,0)
IST1189I SLUALMSG = NOSUPP               SUPP     = NOSUP
IST1189I VARYWLD  = FULLWILD
IST314I END
```

Connection Problems – What is the Source IP Address? (1)

```
D TCPIP,TCPIP1,N,CONN
EZZ2500I NETSTAT CS V1R12 TCPIP1 617
USER ID  CONN     LOCAL SOCKET          FOREIGN SOCKET        STATE
BPXOINIT 00007F5B 0.0.0.0..10007        0.0.0.0..0            LISTEN
FTPCCL1  0000A08D 192.168.20.82..21     192.168.20.81..1050   ESTBLSH
FTPCCL1  0000000D 0.0.0.0..21           0.0.0.0..0            LISTEN
INETD4   00007F5D 0.0.0.0..513          0.0.0.0..0            LISTEN
INETD4   00007F5C 0.0.0.0..623          0.0.0.0..0            LISTEN
TN3270   0000000E 0.0.0.0..23           0.0.0.0..0            LISTEN
TN3270   0000A090 192.168.20.82..23     192.168.0.118..1581   ESTBLSH
7 OF 8 RECORDS DISPLAYED
END OF THE REPORT
```

Connection Problems – How is Source IP Address Derived?

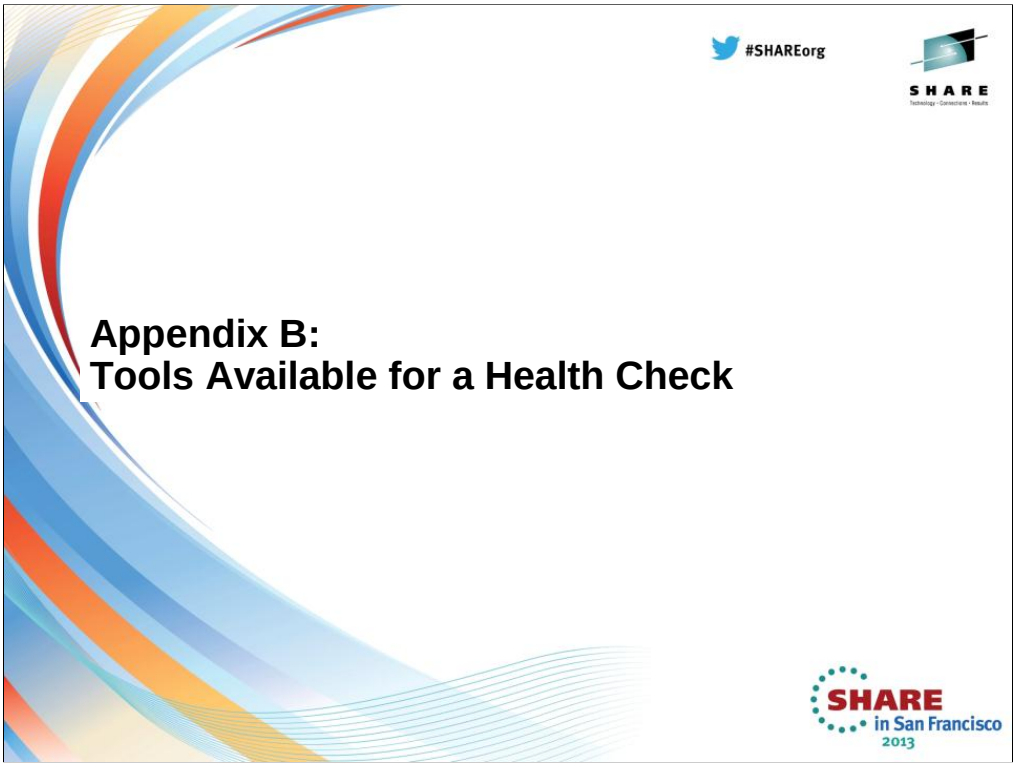
- 1. Sendmsg( ) using the IPV6_PKTINFO ancillary option specifying a nonzero source address (RAW and UDP sockets only)
- 2. Setsockopt( ) IPV6_PKTINFO option specifying a nonzero source address (RAW and UDP sockets only)
- 3. Explicit bind to a specific local IP address
- 4. bind2addrsel socket function (AF_INET6 sockets only)
- 5. PORT profile statement with the BIND parameter
- 6. SRCIP profile statement (TCP connections only)
- 7. TCPSTACKSOURCEVIPA parameter on the IPCONFIG or IPCONFIG6 profile statement (TCP connections only)
- 8. SOURCEVIPA: Static VIPA address from the HOME list or from the SOURCEVIPAINTERFACE parameter
- 9. HOME IP address of the link over which the packet is sent

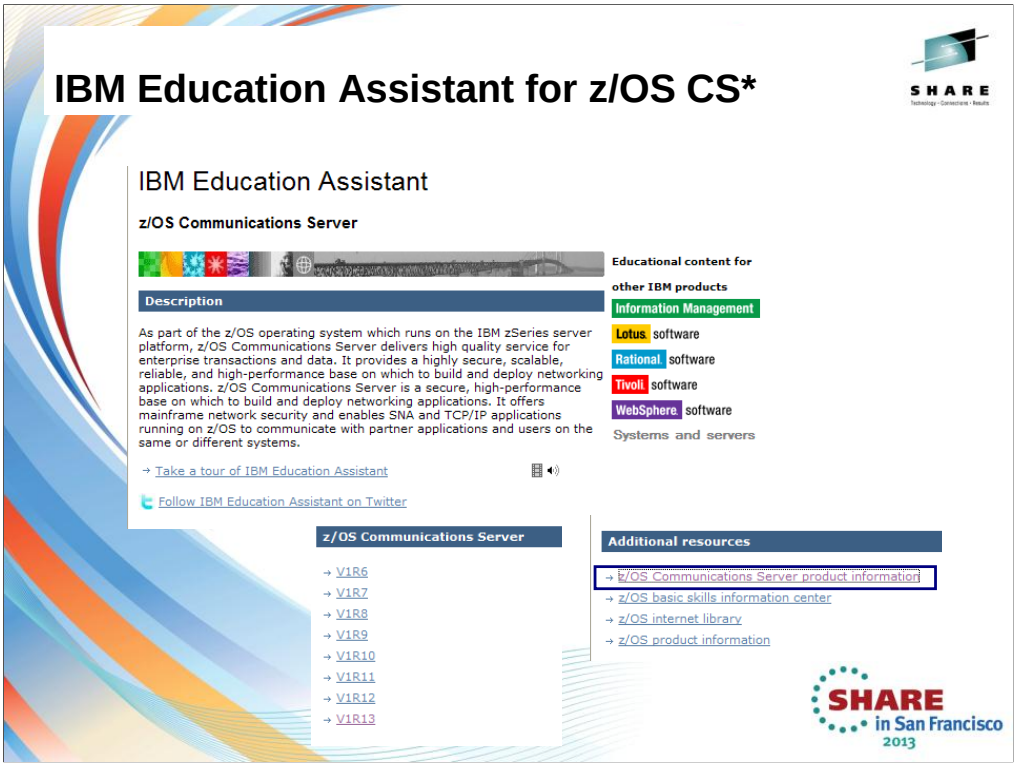
Connection Problems – What is the Source IP Address? NETSTAT SRCIP (1)


```
NETSTAT SRCIP
MVS TCP/IP NETSTAT CS V1R13 TCPIP Name: TCPCS 20:30:49
Source IP Address Based on Job Name:
Job Name Type Flg Source
-------- ---- --- ------
*        IPV4 C    9.67.5.16
*        IPV6 C    DVIPA66
T*       IPV4 S    9.67.5.15
T*       IPV6 S    2000::9:67:5:15
TCPUSR1* IPV4 B    9.67.5.12
TCPUSR2* IPV6 B    DVIPA62
TCPUSR3* IPV6      TEMPADDRS
TCPUSR4* IPV6      PUBLICADDRS
U*       IPV4 C    9.67.5.14
U*       IPV6 C    DVIPA64
USER*    IPV6 C    2000::9:67:5:13
USER1*   IPV4 C    9.67.5.13
USER12   IPV4 C    9.67.5.11
U27      IPV6 C    2000::9:67:5:11
…
```

Connection Problems – What is the Source IP Address? NETSTAT SRCIP (3)

```
NETSTAT SRCIP
MVS TCP/IP NETSTAT CS V1R13 TCPIP Name: TCPCS 20:30:49
…
Source IP Address Based on Destination:
Destination:   10.1.0.0/16
Source:        9.1.1.2
Destination:   10.1.1.1
Source:        9.1.1.1
Destination:   2001:0db8::0522:f103
Source:        2000::9:67:5:10
Destination:   2001:0db8::/32
Source:        DVIPA66
```


#SHAREorg
SHARE
Technology · Connections · Results
Appendix B:
Tools Available for a Health Check
SHARE
in San Francisco
2013



“CS*” stands for Communications Server

http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp?topic=/com.ibm.iea.commserv_v1/commserv/1.10z/install/cfgasst/player.html Takes you to this screen, from which you choose z/OS Communications Server product information.

This selection takes you to the subsequent screen.

z/OS Communications Server Downloads

http://www-01.ibm.com/software/network/commserver/zos/

Select “Support downloads” – takes you to next screen:

http://www-01.ibm.com/support/search.wss?rs=852&tc=SSSN3L&rank=8&dc=D400&dtm

z/OS Communications Server

Add to My interests

Overview

z/OS® Communications Server is a secure, high-performance base on which to build and deploy networking applications.

Offers mainframe network security and enables SNA and TCP/IP applications running on z/OS to communicate with partner applications and users on the same or different systems.

- Delivers high-quality service for enterprise transactions and data
- Provides TCP/IP and System Network Architecture (SNA) networking support for the z/OS operating system
- Provides common applications such as File Transfer Protocol (FTP), Telnet and remote execution of applications
- Provides support for RIPv1, RIPv2 and OSPF dynamic routing protocols
- SNA protocols include traditional subarea SNA support and Advanced Peer-to-Peer Networking protocols (High Performance Routing, Enterprise Extender)
- Operating systems supported: z/OS

→ View features and benefits

Learn more

- Features & benefits
- System requirements
- Product library
- Technical article

Use and maintain

- Product support
- Product documentation
- Support downloads
- Developer resources

Available z/OS CS Downloads

Select “Support downloads” – from

http://www-01.ibm.com/software/network/commserver/zos/

takes you to next screen:

http://www-01.ibm.com/support/search.wss?rs=852&tc=SSSN3L&rank=8&dc=D400&dtm

Download results

Download

for z/OS Communications Server

Results

Technical support | Information centers | Publications

1 - 4 of 4 items found* Modified date

1. The IBM z/OS Communications Server Network Utility Assistant 2011-02-24
The IBM z/OS Communications Server Network Utility Assistant tool is a TSO/ISPF front-end to the z/OS Communications Server TSO NETSTAT line-mode command.
[More items like this found in Enterprise Connectivity]

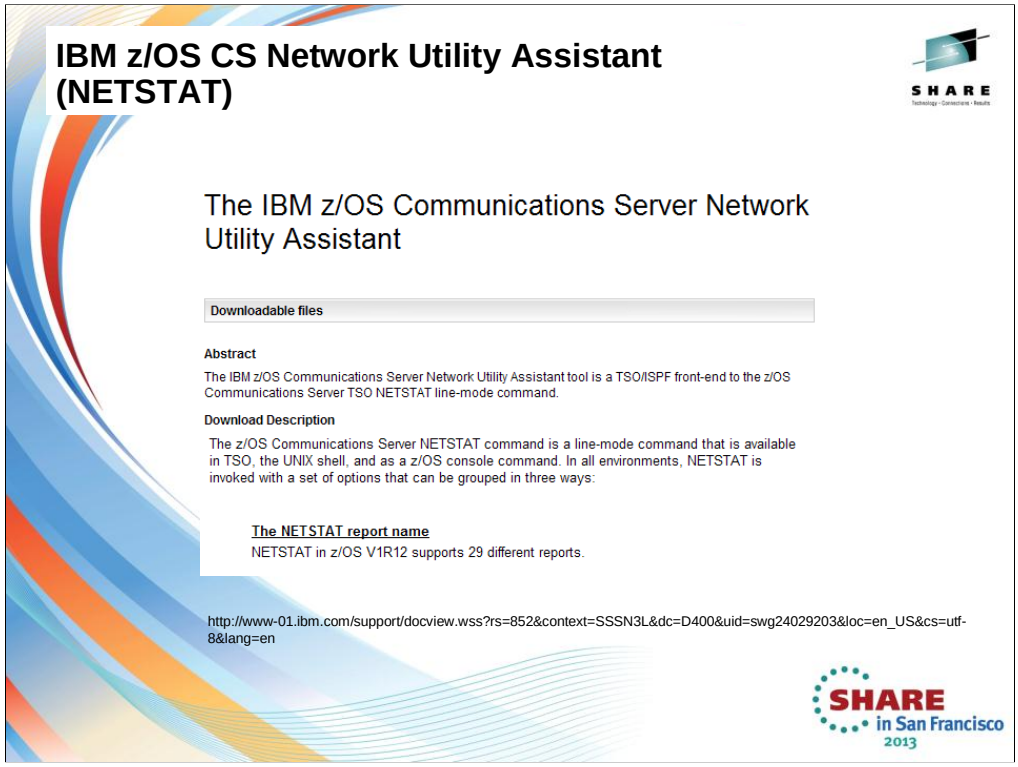
2. IBM Configuration Assistant for z/OS Communications Server 2010-08-26
IBM Configuration Assistant for z/OS Communications Server provides centralized configuration of AT-TLS, IP Security, NSS, PBR, QoS, IDS, and DMD policies.
[More items like this found in Enterprise Connectivity]

3. Directory Services Management Exit (DSME) Sample code 2010-01-05
Sample implementation of a Directory Services Management Exit (DSME).
[More items like this found in Enterprise Connectivity]

4. IBM Service Assistant for z/OS Communications Server 2009-02-02
The IBM Service Assistant for z/OS Communications Server provides tools useful in diagnosing and analyzing z/OS Communications Server.
[More items like this found in Enterprise Connectivity]

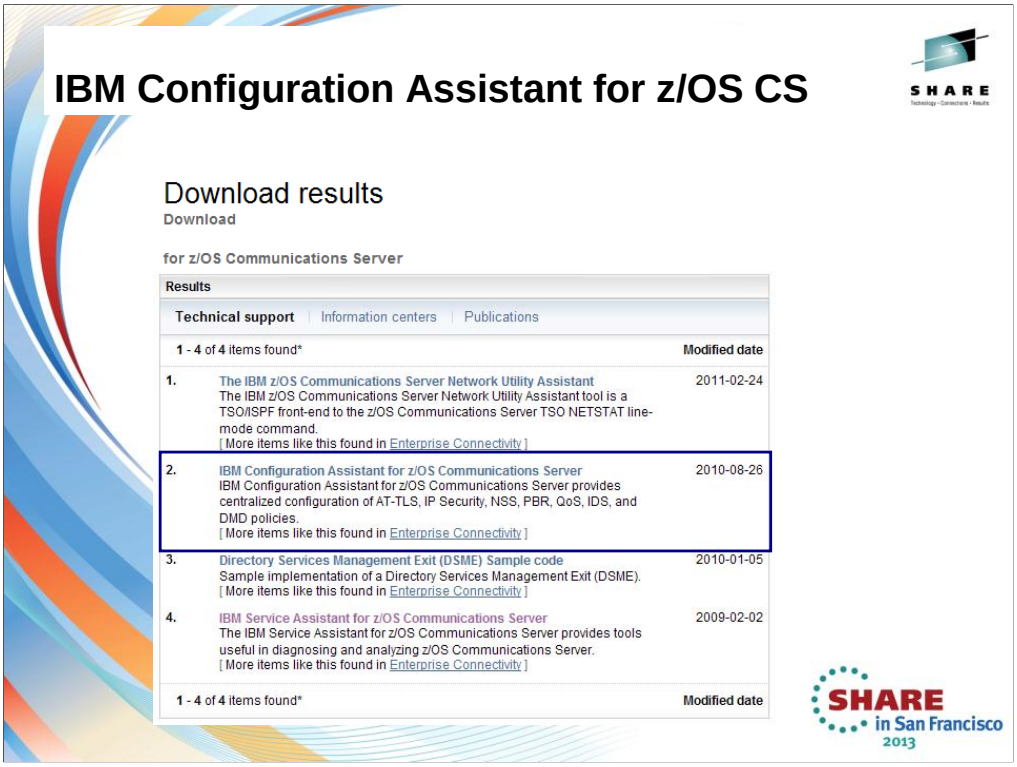
1 - 4 of 4 items found* Modified date

IBM z/OS CS Network Utility Assistant (NETSTAT)



http://www-01.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=D400&uid=swg24029203&loc=en_US&cs=utf-8&lang=en

IBM Configuration Assistant for z/OS CS

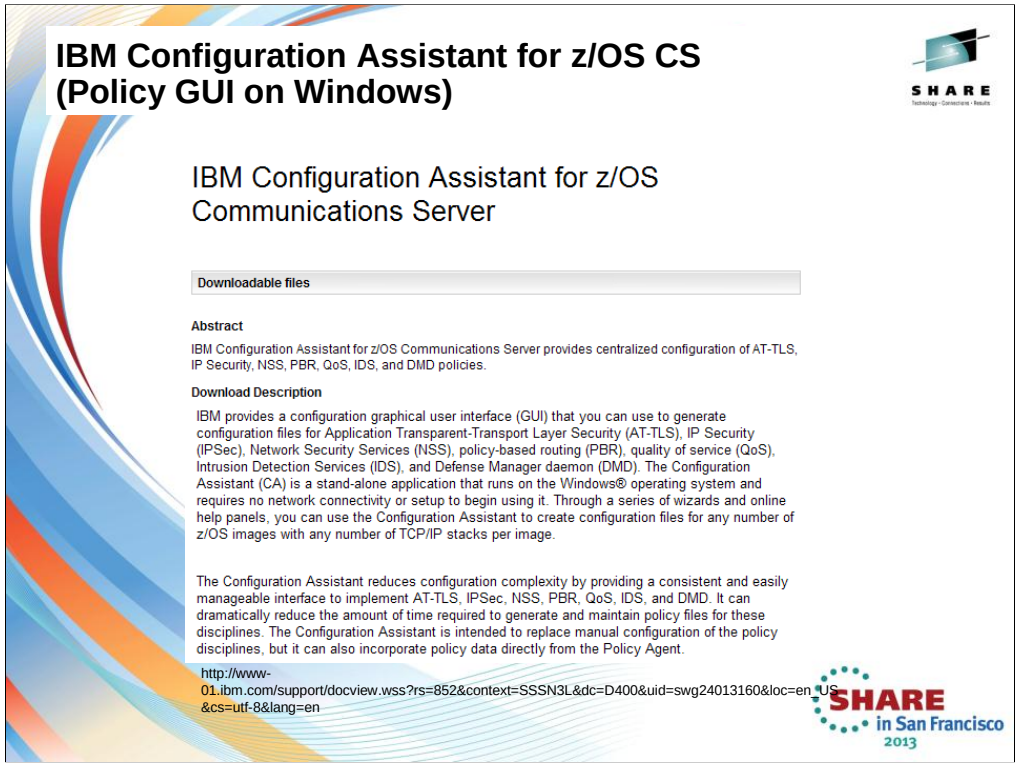


Select “Support downloads” – from: http://www-01.ibm.com/software/network/commserver/zos

takes you to next screen:

http://www-01.ibm.com/support/search.wss?rs=852&tc=SSSN3L&rank=8&dc=D400&dtm

IBM Configuration Assistant for z/OS CS (Policy GUI on Windows)



IBM Configuration Assistant for z/OS Communications Server

Downloadable files

Abstract

IBM Configuration Assistant for z/OS Communications Server provides centralized configuration of AT-TLS, IP Security, NSS, PBR, QoS, IDS, and DMD policies.

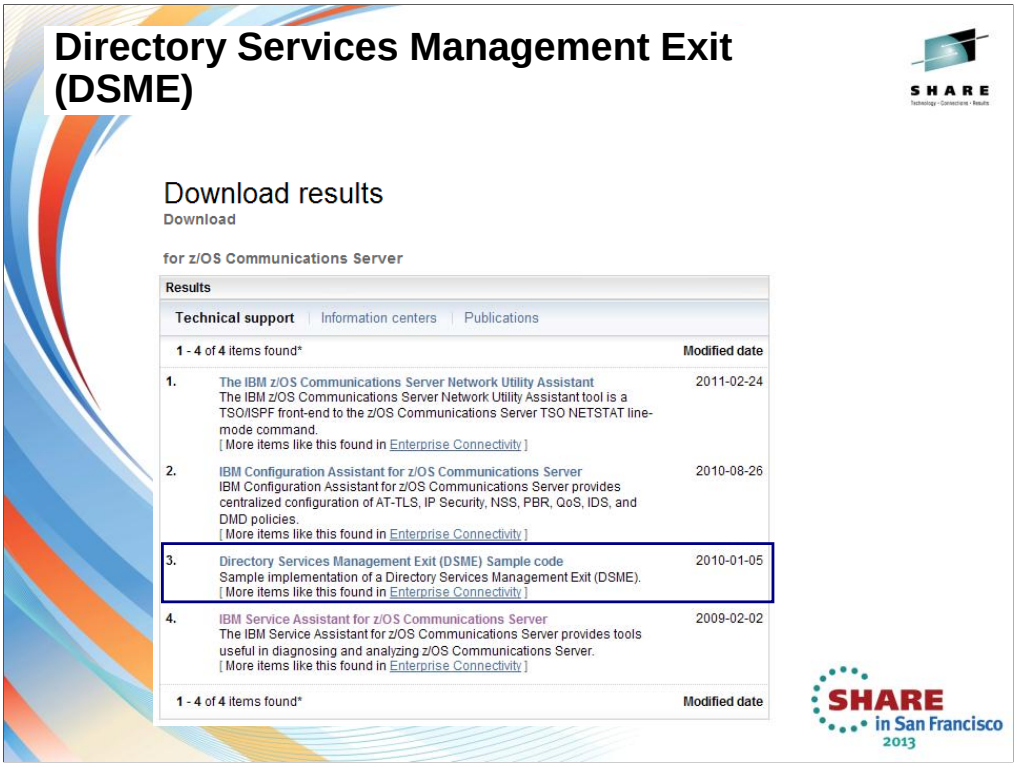
Download Description

IBM provides a configuration graphical user interface (GUI) that you can use to generate configuration files for Application Transparent-Transport Layer Security (AT-TLS), IP Security (IPSec), Network Security Services (NSS), policy-based routing (PBR), quality of service (QoS), Intrusion Detection Services (IDS), and Defense Manager daemon (DMD). The Configuration Assistant (CA) is a stand-alone application that runs on the Windows® operating system and requires no network connectivity or setup to begin using it. Through a series of wizards and online help panels, you can use the Configuration Assistant to create configuration files for any number of z/OS images with any number of TCP/IP stacks per image.

The Configuration Assistant reduces configuration complexity by providing a consistent and easily manageable interface to implement AT-TLS, IPSec, NSS, PBR, QoS, IDS, and DMD. It can dramatically reduce the amount of time required to generate and maintain policy files for these disciplines. The Configuration Assistant is intended to replace manual configuration of the policy disciplines, but it can also incorporate policy data directly from the Policy Agent.

http://www-01.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=D400&uid=swg24013160&loc=en_US&cs=utf-8&lang=en

Directory Services Management Exit (DSME)



Select “Support downloads” – from: http://www-01.ibm.com/software/network/commserver/zos/

takes you to next screen:

http://www-01.ibm.com/support/search.wss?rs=852&tc=SSSN3L&rank=8&dc=D400&dtm

DSME Sample

Directory Services Management Exit (DSME) Sample code

Downloadable files

Abstract

Sample implementation of a Directory Services Management Exit (DSME).

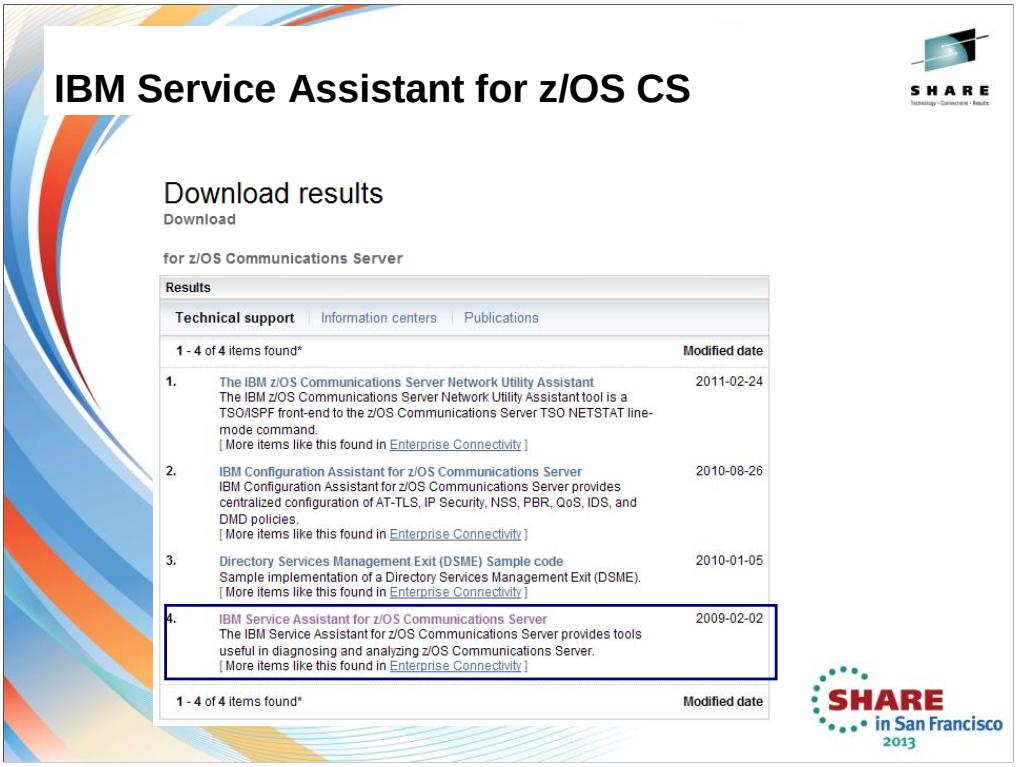
Download Description

This sample Directory Services Management Exit (DSME) code provides a base from which customers can develop their own customized DSME. The sample DSME provides:

- Entry linkage and register savearea setup
- Establishment of the basic DSME environment
- Addressability to the DSME parameter list
- Basic implementation of the following DSME functions:
  - begin
  - end
  - search authorization
  - EBN selection
  - CD server selection
  - alternate CD server selection
  - central resource registration selection

http://www-01.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=D400&uid=swg24014056&loc=en_US&cs=utf-8&lang=en

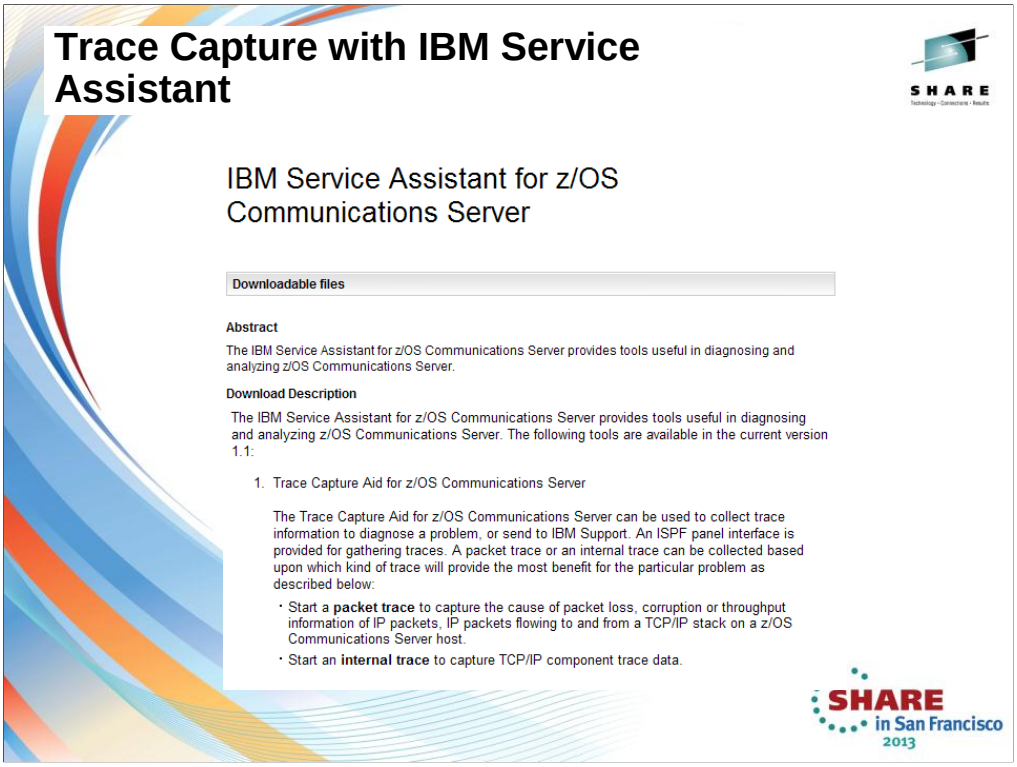
IBM Service Assistant for z/OS CS



Select “Support downloads” – from: http://www-01.ibm.com/software/network/commserver/zos/

takes you to next screen:

http://www-01.ibm.com/support/search.wss?rs=852&tc=SSSN3L&rank=8&dc=D400&dtm



IBM Support Assistant (ISA) is chartered to improve customer satisfaction by increasing the customers' ability to resolve software challenges themselves.

How? The IBM Support Assistant…

…is an extensible client application that is installed on your desktop computer.

…is a framework that allows other IBM software products to plug into it to provide you with self-help information.

…has a modular design allowing the **easy integration of new Support Assistant enablers as more IBM products make them available** whether by downloading them or by installation from the product media.

The ISA framework was designed to be used on distributed platforms

Specifically, one of the options in ISA is a documentation gathering tool, based off of scripts

At the occurrence of a problem, the customer can simply click a button, and a standard set of documentation will be gathered from the troubled system

While this works great on platforms such as Linux and Windows, it is not so easily accomplished on the z platform

There is a possibility of creating scripts that will execute JCL (via FTP) on the mainframe to gather documentation, but this has not yet been attempted

Additionally, such an implementation would require fairly detailed mainframe configurations for FTP, JES, and any application for which documentation is to be collected

If we cannot take advantage of the documentation gathering function, why do we need ISA for CommServer?

For one thing, ISA also provides a page of common links, like

- The support page
- Troubleshooting links
- Educational links
- News feeds

Also, for customers who are accustomed to using ISA for other products, it is important that CommServer have a plugin available for the purposes of visibility and customer satisfaction

#SHAREorg

SHARE

The Doctor is In: Conducting a z/OS Communications Server TCP/IP Health Check

End of Presentation

SHARE in San Francisco 2013