z/OS Communications Server Hints and Tips

Todd Valler – tevaller@us.ibm.com
IBM Enterprise Networking Solutions

Thursday, August 13, 2015
Session: 17996

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

z/OS Communications Server Social Media

http://facebook.com/IBMCommserver

http://twitter.com/IBM_Commserver

http://tinyurl.com/zoscsblog

http://youtube.com/user/zOSCommServer

Agenda

- Stalled TCP Connections
- Unresponsive Name Servers
- EE Verify
- Ctrace Writer
- Shark Attack
- QDIO Inbound Workload Queuing (IWQ)

Stalled TCP Connections

Sending side stall

- Window size of zero
- Repeated retransmission of the same segment

- Send buffer is page fixed CSM dataspace
- When a stall is detected or storage constrained
  - New data added to send buffer is marked page-eligible
- When storage constrained
  - All unsent data on send queues of all TCP connections is marked page-eligible

Receiving side stall

- Application not reading

- Read buffer is page-able CSM dataspace or TCPIP private
- Each packet's data is mapped by a control block
- When a stall is detected during inbound packet processing
  - Read data is consolidated into large buffers
- When storage constrained
  - All connections are scanned
  - Stale data is consolidated into large buffers

Basic detection

NETSTAT ALL/-A

```
ReceiveBufferSize:   0000004096        SendBufferSize:      0000004096
ReceiveDataQueued:   0000004096
  OldQDate:          08/06/2014        OldQTime:            01:01:26
SendDataQueued:      0000000000
SendStalled:         No
```

```
ReceiveBufferSize:   0000004096        SendBufferSize:      0000004096
ReceiveDataQueued:   0000000000
SendDataQueued:      0000004096
  OldQDate:          08/06/2014        OldQTime:            01:46:16
SendStalled:         Yes
```

Enhanced detection

- Traffic Regulation Manager daemon (TRMD) must be active
- Messages written to SYSLOGD

EZZ8662I TRMD TCP receive queue constrained entry logged: 08/06/2014 01:06:41.00 , connid= 00000059 , jobname= USER662 , lipaddr= 9.42.104.77 , lport= 1033 , ripaddr= 192.168.1.99 , rport= 1034 , correlator= 4 , probeid= 040A0001 , sensorhostname=MVSF.tcp.raleigh.ibm.com , trigger= BytesQueued , dataage= 300 , bytesqueued= 4096 , queuesize= S

EZZ8664I TRMD TCP send queue constrained entry logged: 08/06/2014 01:46:49.17 , connid= 00000058 , jobname= USER662 , lipaddr= 192.168.1.99 , lport= 1034 , ripaddr= 9.42.104.77 , rport= 1033 , correlator= 5 , probeid= 040A0004 , sensorhostname= MVSF.tcp.raleigh.ibm.com , trigger= BytesQueued , dataage= 31 , bytesqueued= 4096 , queuesize= S

Automated actions

- Policy Agent must be active
- Policy action can reset connections
- TCP_QUEUE_SIZE
  - Connection send and receive queue sizes
- GLOBAL_TCP_STALL
  - 50% of active TCP connections with zero window
  - At least 1000 active TCP connections

TCP_QUEUE_SIZE

- IDSRule
  - IDSAttackCondition
    - TCP_QUEUE_SIZE
      - Very_Short
      - Short
      - Long
      - Very_Long
  - IDSAction
    - Resetconn
    - Noresetconn

TCP_QUEUE_SIZE example

```
IDSRule                         ExampleTcpQueueSize-rule
{
  ConditionType                 Attack
  Priority                      2
  IDSAttackCondition
  {
    AttackType                  TCP_QUEUE_SIZE
    TcpQueueSize                Short
    IDSExclusion
    {
      ExcludedAddrPort          192.168.1.0/24
    }
  }
  IDSAction
  {
    ActionType                  Attack  resetconn
  }
}
```

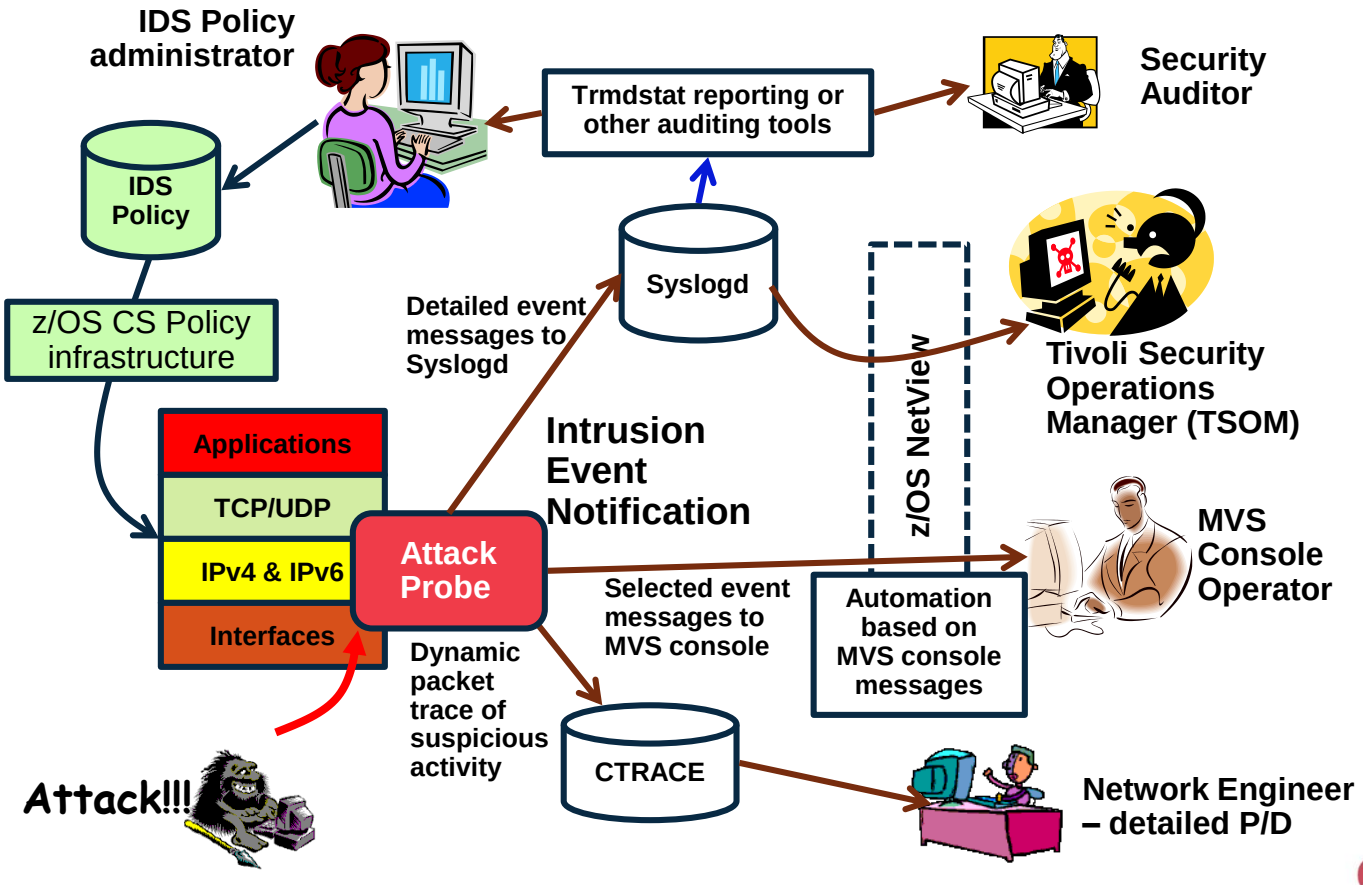
GLOBAL_TCP_STALL

- IDSRule
  - IDSAttackCondition
    - GLOBAL_TCP_STALL
  - IDSAction
    - Resetconn
    - Noresetconn
    - *IDSReportSet*
      - TypeActions Log LogDetail Yes
        - » EZZ8673I when connection reset
        - » EZZ8674I when connection is not reset

GLOBAL_TCP_STALL example

```
IDSRule                         ExampleGlobalTcpStall-rule
{
  ConditionType                 Attack
  Priority                      2
  IDSAttackCondition
  {
    AttackType                  GLOBAL_TCP_STALL
  }
  IDSAction
  {
    ActionType                  Attack  resetconn
    IDSReportSet
    {
      TypeActions               Log  LogDetail  Yes
    }
  }
}
```

Intrusion detection and prevention services on z/OS



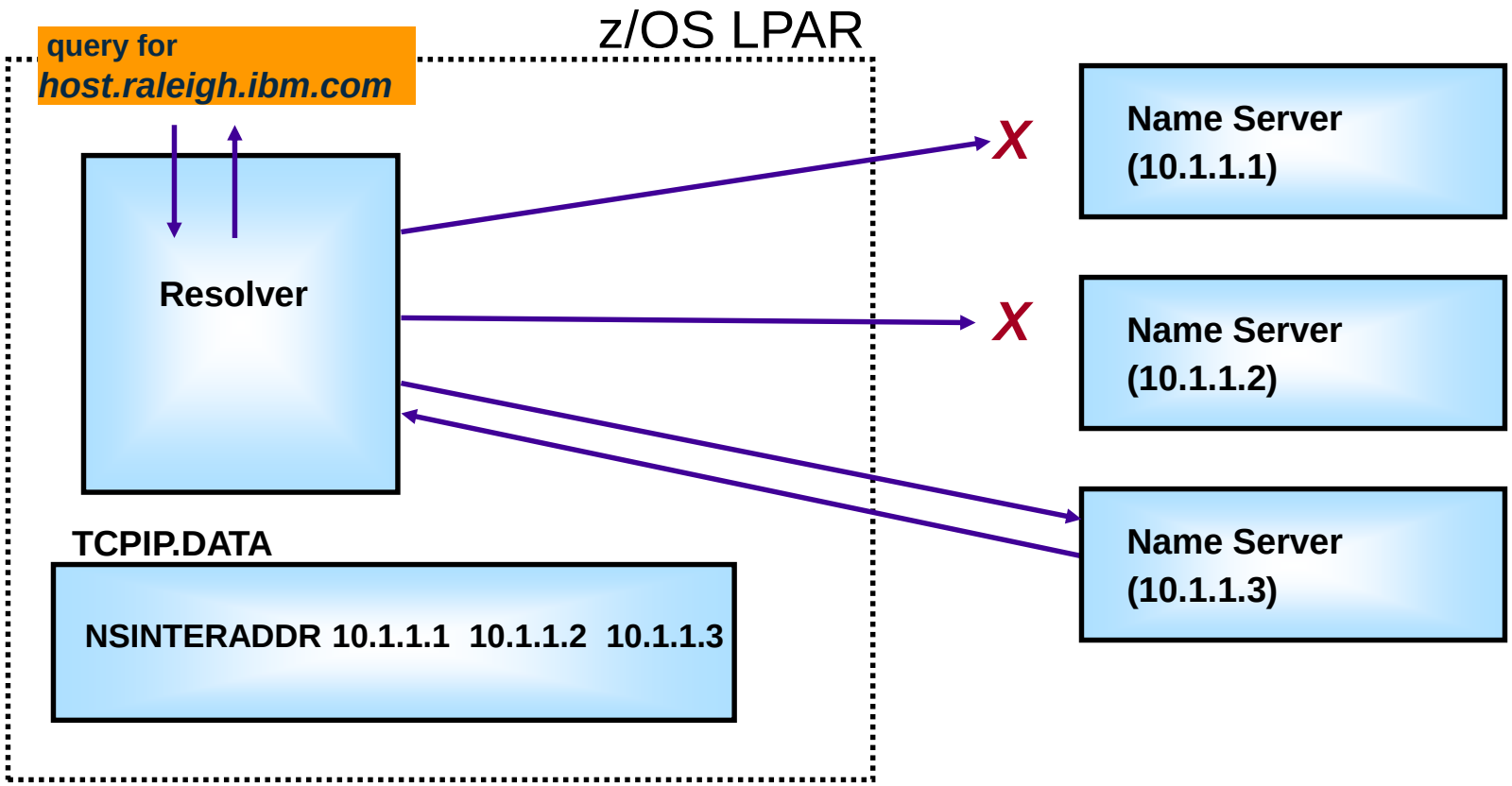
- **Events detected**
  - Scans
  - Attacks against stack
  - Flooding (both TCP and UDP)
- **Defensive methods**
  - Packet discard
  - Limit connections
  - Reset connections
- **Reporting**
  - Logging
  - Event messages to local console
  - IDS packet trace
  - Notifications to Tivoli NetView and Risk Manager
- **IDS Policy**
  - Samples supplied with z/OS CS Configuration Assistant

Unresponsive Name Servers

Dealing with unresponsive name servers

- Name server or network outages can introduce long resolver delays
- Default setting for the timeout value is 5 seconds
- Application delays
  - Outbound connections to hostnames
  - Inbound connection logging for reverse lookup

Name resolution delayed



Resolver monitors name server queries

- Resolver maintains statistics
  - Queries sent to a name server
  - Instances when the name server did not respond to a query
- Resolver examines previous five-minute aggregate of statistics every minute
  - Compares percentage of failures against an acceptable threshold value
    - If percentage exceeds the acceptable threshold, messages are issued to the console
    - Messages are issued when percentage falls below acceptable level

Enabling Resolver's monitoring function

- Resolver setup statement defined to specify the acceptable failure rate threshold

```
    .-UNRESPONSIVETHRESHOLD(25)----------.
>--+-----------------------------------+--->
    '-UNRESPONSIVETHRESHOLD(percentage)--'
```

  - The default percentage is 25 **(on by default)**
  - Value can range from 0-100
    - 0 disables the function
  - Value can be modified dynamically using MODIFY RESOLVER,REFRESH,SETUP=*file_name*

Unresponsive name server detected

- Resolver generates two messages per unresponsive name server at first detection of unresponsive state

```
EZZ9308E UNRESPONSIVE NAME SERVER DETECTED AT IP ADDRESS 9.43.25.200
EZZ9310I NAME SERVER 9.43.25.200
           TOTAL NUMBER OF QUERIES SENT          6000
           TOTAL NUMBER OF FAILURES              2100
           PERCENTAGE                              35%
```

- While a name server remains unresponsive, a new instance of EZZ9310I is issued every five minutes to display recent activity

```
EZZ9310I NAME SERVER 9.43.25.200
           TOTAL NUMBER OF QUERIES SENT          3000
           TOTAL NUMBER OF FAILURES              1650
           PERCENTAGE                              55%
```

Name server becomes responsive

- When the error rate falls below the acceptable threshold for a given five minute window, resolver takes action
  - Clears EZZ9308E from the operator console
  - Issues EZZ9309I to indicate name server is responsive
  - Issues EZZ9310I to display responsiveness
- No activity for a name server over a five minute window causes the name server to be considered responsive

```
EZZ9309I NAME SERVER IS NOW RESPONSIVE AT IP ADDRESS 9.43.25.200
EZZ9310I NAME SERVER 9.43.25.200
           TOTAL NUMBER OF QUERIES SENT          4500
           TOTAL NUMBER OF FAILURES               675
           PERCENTAGE                              15%
```

Enhanced Resolver autonomics

- Resolver continues to maintain statistics
- Monitor interval is reduced to 30 seconds
- When acceptable threshold is exceeded
  - –Stop sending application queries to unresponsive name server
  - –Resolver periodically sends DNS polling queries to the name server
  - –When DNS polling responses falls below acceptable threshold resume sending application queries

Enabling enhanced Resolver autonomics

- AUTOQUIESCE specifies the action the Resolver takes when an unresponsive name server is detected

```
   .-UNRESPONSIVETHRESHOLD(25)-------------.
>--+-------------------------------------+--->
   '-UNRESPONSIVETHRESHOLD(%,AUTOQUIESCE)--'
```

  - Percentage must be specified
  - Requires GLOBALTCPIPDATA statement
  - Requires RESOLVEVIA UDP
  - Value can be modified dynamically using MODIFY RESOLVER,REFRESH,SETUP=*file_name*

Unresponsive name server detected

- Resolver generates two messages per unresponsive name server at first detection of unresponsive state

```
EZZ9311E STOPPED USING NAME SERVER AT IP ADDRESS 10.42.35.200
EZZ9313I NAMESERVER 10.42.35.200
     TOTAL NUMBER OF QUERIES SENT          500
     TOTAL NUMBER OF FAILURES              500
     TOTAL NUMBER OF RESOLVER POLLS SENT     0
     TOTAL NUMBER OF POLL FAILURES           0

     PERCENTAGE                            100%
```

Name server becomes responsive

- When the error rate in response to probes falls below the acceptable threshold for a given thirty second window, resolver takes action
  - Clears EZZ9311E from the operator console
  - Issues EZZ9312I to indicate name server use is resumed

```
EZZ9312I RESUMED USING NAME SERVER AT IP ADDRESS 10.42.35.200
```

Health Checker for the autonomic quiescing function

- CSRES_AUTOQ_GLOBALTCPIPDATA
  - –Checks for the GLOBALTCPIPDATA setup statement if AUTOQUIESCE is coded
- CSRES_AUTOQ_TIMEOUT
  - –Checks, by default, if you have specified a value greater than five seconds (modifiable) for RESOLVERTIMEOUT when autonomic quiescing is enabled
- CSRES_AUTOQ_RESOLVEVIA
  - –Checks if you have specified RESOLVEVIA TCP when autonomic quiescing is enabled
- Performed when Resolver is started and when MODIFY RESOLVER,REFRESH command is issued

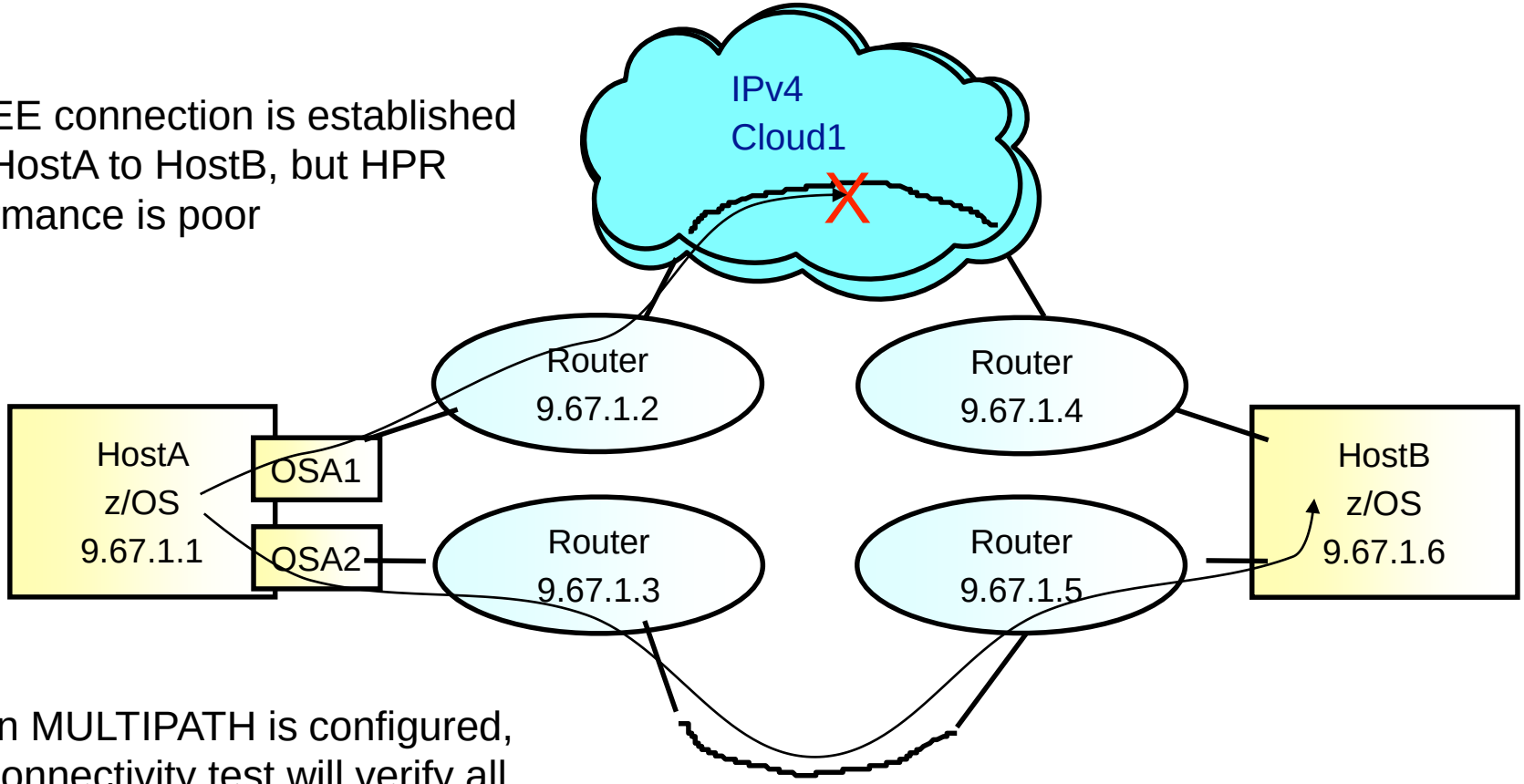
EE Verify

EE connectivity test command

- Useful in debugging various network problems
- Test an existing Enterprise Extender connection
- Assist in diagnosing why an EE connection cannot be established
- The EE connectivity test will verify:
  - EE line availability
  - Address resolution capability
  - EE partner reachability
  - Tests all five UDP ports reserved for EE
  - When MULTIPATH is enabled in the Enterprise Extender TCP/IP stack, the EE connectivity test is repeated for each valid TCP/IP interface with a route to the destination

EE connectivity test example

IPv4 EE connection is established from HostA to HostB, but HPR performance is poor



When MULTIPATH is configured, the connectivity test will verify all computed routes from HostA to HostB

EE connectivity test example…

D NET,EEDIAG,TEST=YES,IPADDR=(9.67.1.1,9.67.1.6),LIST=DETAIL

```
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = EEDIAG
IST2119I ENTERPRISE EXTENDER DISPLAY CORRELATOR: EE00000E
IST2067I EEDIAG DISPLAY ISSUED ON 10/04/05 AT 11:05:50
IST1680I LOCAL IP ADDRESS 9.67.1.1
IST1680I REMOTE IP ADDRESS 9.67.1.6
IST2023I CONNECTED TO LINE LN11
IST2126I CONNECTIVITY TEST IN PROGRESS
IST314I END
.
.
```

EE connectivity test example …

```
IST350I DISPLAY TYPE = EEDIAG
IST2130I ENTERPRISE EXTENDER CONNECTIVITY TEST INFORMATION
IST2119I ENTERPRISE EXTENDER DISPLAY CORRELATOR: EE00000E
IST2131I EEDIAG DISPLAY COMPLETED ON 10/04/05 AT 11:05:52
IST2132I LDLC PROBE VERSIONS: VTAM = V1  PARTNER = V1
IST1680I LOCAL IP ADDRESS 9.67.1.1
IST1680I REMOTE IP ADDRESS 9.67.1.6
IST924I -------------------------------------------------------
IST2133I INTFNAME: OSA1                    INTFTYPE: OSAFDDI
IST2135I   CONNECTIVITY UNSUCCESSFUL    SENSE: ***NA***   PORT: 12000
IST2137I     1  9.67.1.2                    RTT:     2
IST2137I     2  9.67.1.21          D-1      RTT:     3
IST2135I   CONNECTIVITY UNSUCCESSFUL    SENSE: ***NA***   PORT: 12001
IST2137I     1  9.67.1.2                    RTT:     2
IST2137I     2  9.67.1.21          D-1      RTT:     3
IST2135I   CONNECTIVITY UNSUCCESSFUL    SENSE: ***NA***   PORT: 12002
IST2137I     1  9.67.1.2                    RTT:     2
IST2137I     2  9.67.1.21          D-1      RTT:     4
.
.
```

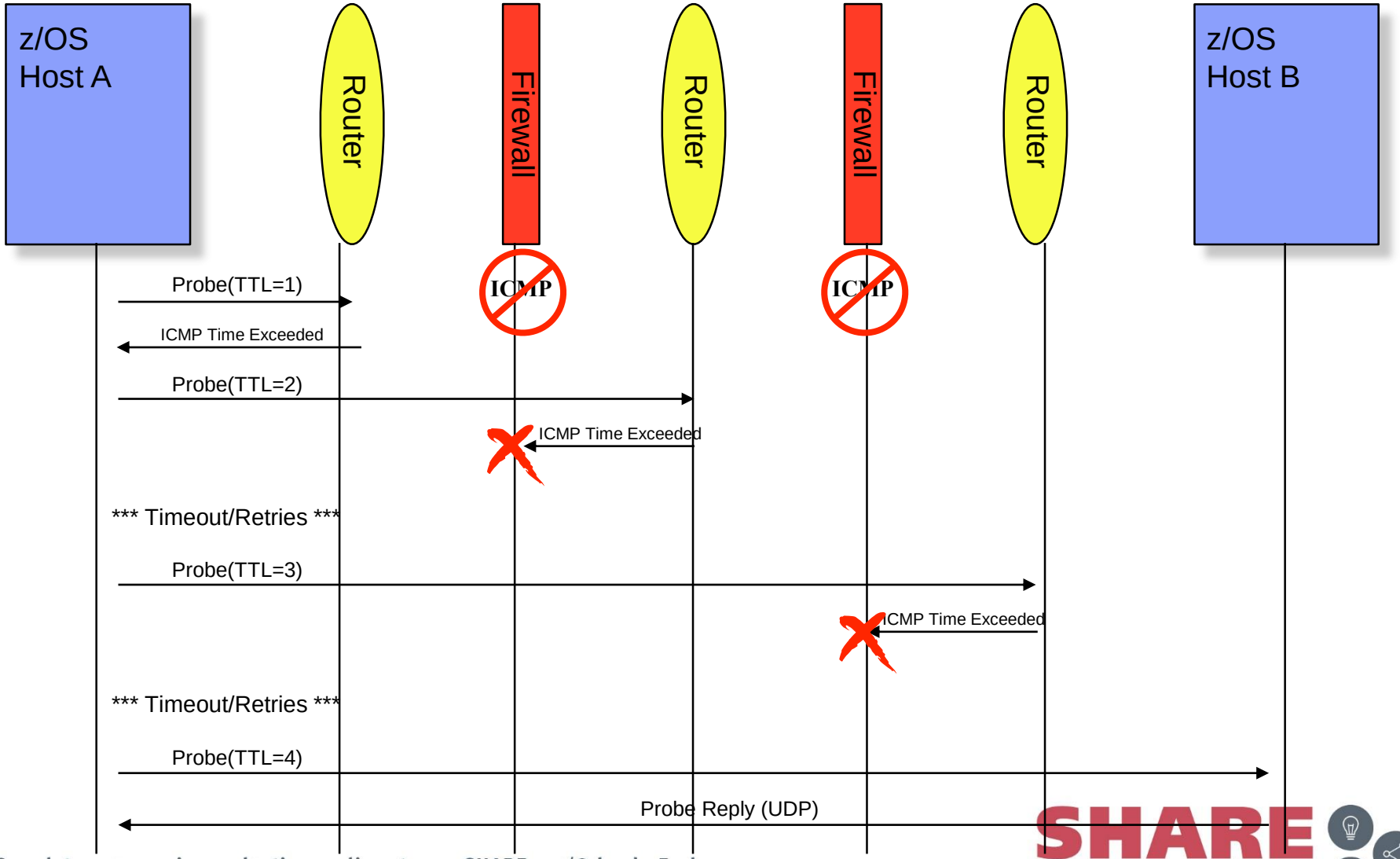
EE connectivity test example…

```
IST924I -------------------------------------------------------------
IST2133I INTFNAME: OSA1                    INTFTYPE: OSAFDDI
IST2134I   CONNECTIVITY SUCCESSFUL                              PORT: 12000
IST2137I     1 9.67.1.3                      RTT:     9
IST2137I     2 9.67.1.11                     RTT:    14
IST2137I     3 9.67.1.12                     RTT:    19
IST2137I     4 9.67.1.5                      RTT:    23
IST2137I     5 9.67.1.6                      RTT:    27
.
IST2133I INTFNAME: OSA2                    INTFTYPE: OSAFDDI
IST2134I   CONNECTIVITY SUCCESSFUL                              PORT: 12000
IST2137I     1 9.67.1.3                      RTT:     7
IST2137I     2 9.67.1.11                     RTT:    11
IST2137I     3 9.67.1.12                     RTT:    12
IST2137I     4 9.67.1.5                      RTT:    17
IST2137I     5 9.67.1.6                      RTT:    23
.
IST924I -------------------------------------------------------------
IST2039I CONNECTIVITY TEST INFORMATION DISPLAYED FOR 2 INTERFACES
IST314I END
```

EE connectivity test considerations

- Expects ICMP messages from intermediate hops
- Firewalls may be configured to block ICMP messages
  - Intermediate hops past firewall will appear as unresponsive
  - Final destination reachability can still be determined
    - Firewalls may be configured to block UDP traffic
- Firewalls must allow UDP traffic on EE UDP ports 12000-12004 (both directions)
- EE Test probe "responder" support
  - Support available for CS/Windows, CS/AIX, CS/Linux, PComm, & Cisco SNASw

Firewalls blocking ICMPs

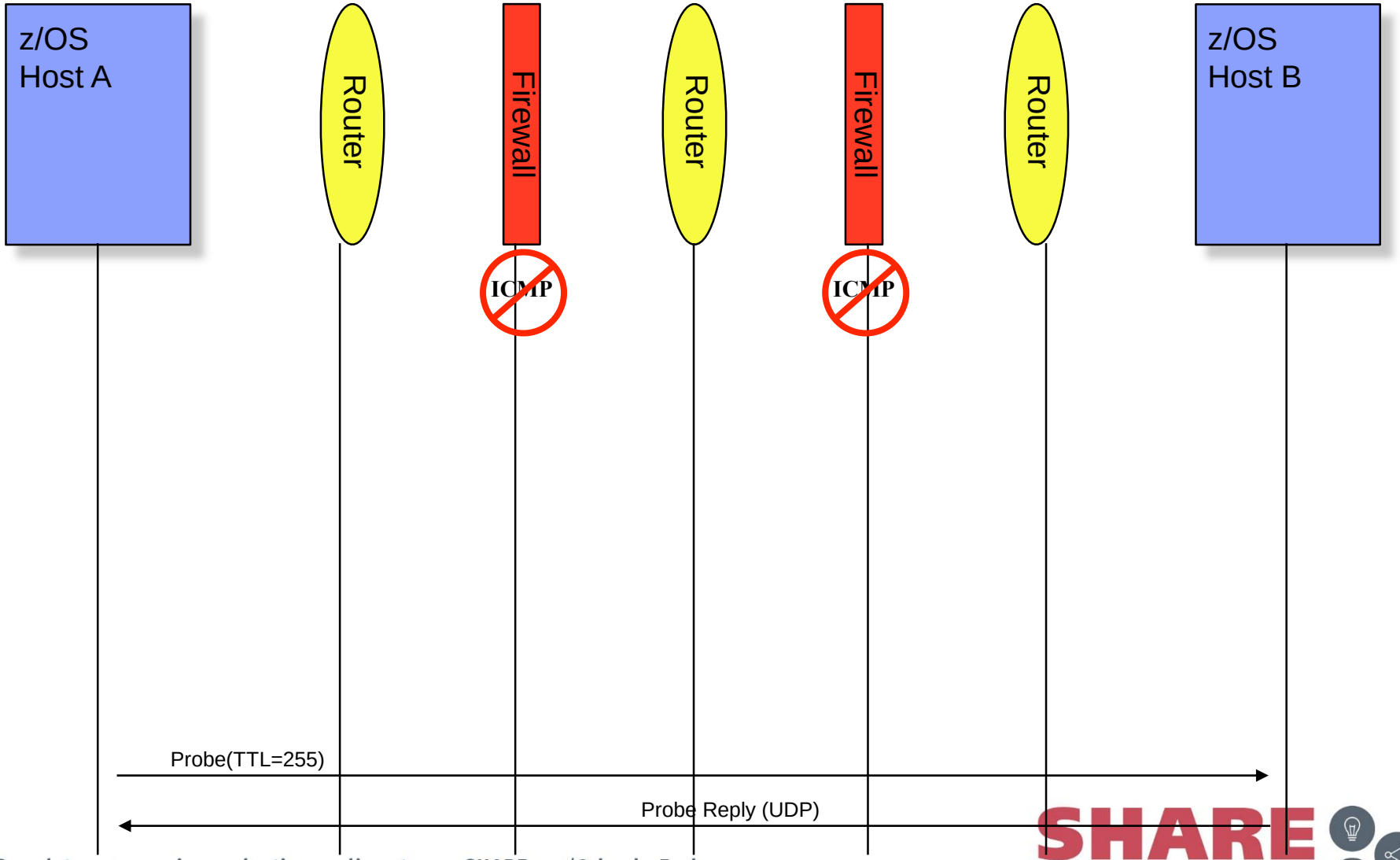


Firewall-Friendly EE connectivity test

- The TTL is set to the maximum hop limit
- Intermediate hop analysis is not possible

```
D NET,EEDIAG,TEST=YES,IPADDR=(9.67.1.1,9.67.1.5),LIST=SUMMARY
.
.
IST1680I LOCAL IP ADDRESS 9.67.1.1
IST1680I REMOTE IP ADDRESS 9.67.1.5
IST924I -------------------------------------------------------
IST2133I INTFNAME: LTRLE1A                  INTFTYPE: MPCPTP
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12000
IST2137I    *NA 9.67.1.5                    RTT:     6
 ...
IST2134I   CONNECTIVITY SUCCESSFUL                        PORT: 12004
IST2137I    *NA 9.67.1.5                    RTT:     7
IST924I -------------------------------------------------------
IST2139I CONNECTIVITY TEST RESULTS DISPLAYED FOR 1 OF 1 ROUTES
IST314I END
```

Firewalls blocking ICMPs

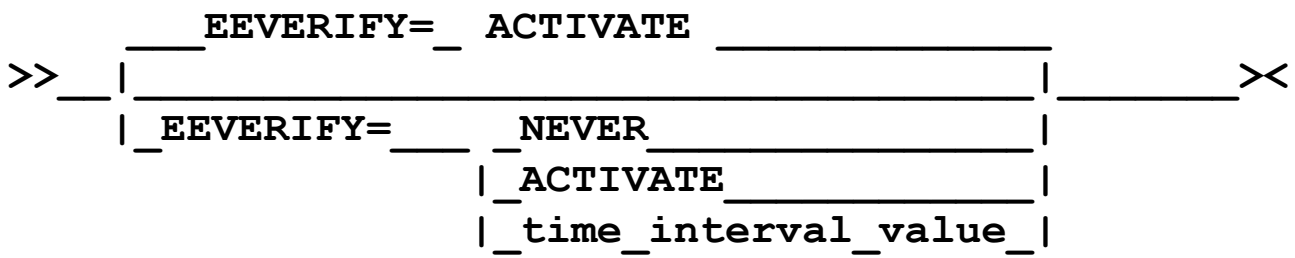


EE health verification

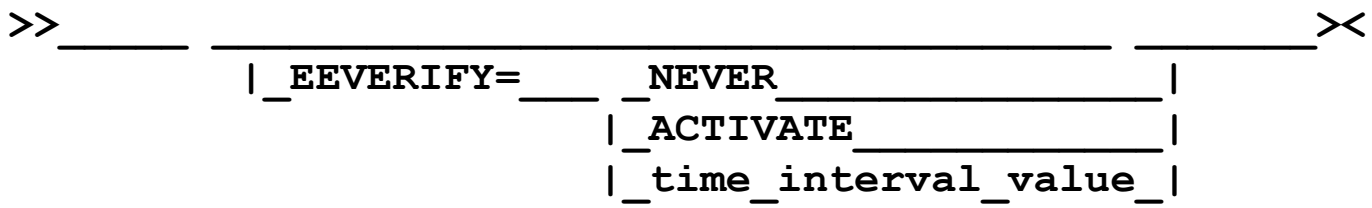
- The EE Health Verification function will verify the health of a potential EE connection by sending a probe to the remote partner using all five ports during the connection activation
  - VTAM does not activate the EE connection if the remote partner is not reachable on all ports
  - However, if the remote partner does not support the probe, VTAM will still bring up the EE connection
- EE Health Verification will also optionally verify the health of an active EE connection by sending a probe to the remote partner on all five ports at a user-specified interval
  - VTAM issues a warning message if the remote partner is not reachable on all ports, but will keep the connection active

EE health verification …

- EE Health Verification is enabled by the EEVERIFY start option



- Or the EEVERIFY GROUP/PU parameter



EE health verification …

- When health verification fails for an active connection
  - VTAM issues highlighted warning message IST2323E if it is not already present
  - IST2323E remains on the console until the condition is cleared or the message is erased by the operator
- VTAM display EE,LIST=VERIFY is used to determine which connection(s) have failed verification
- Displaying an individual EE connection shows the success or failure of EE Health Verification
- The EEDIAG,TEST=YES command can be used to further diagnose the cause of the failure

EE health verification …

```
IST2323E EE HEALTH VERIFICATION FAILED ON ONE OR MORE CONNECTIONS

d net,ee,list=eeverify
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = EE
IST2000I ENTERPRISE EXTENDER GENERAL INFORMATION
IST1685I TCP/IP JOB NAME = TCPCS
IST2003I ENTERPRISE EXTENDER XCA MAJOR NODE NAME = XCAIP
...
IST924I -------------------------------------------------------------
IST2324I EE HEALTH VERIFICATION: FAILED CONNECTION INFORMATION
IST2325I LINE LNIP1 PU SWIP2A1 ON 12/21/09 AT 15:56:39
IST2326I EE HEALTH VERIFICATION TOTAL CONNECTION FAILURES = 1
IST2017I TOTAL RTP PIPES =          1     LU-LU SESSIONS =          2
IST2018I TOTAL ACTIVE PREDEFINED EE CONNECTIONS          =          1
IST2019I TOTAL ACTIVE LOCAL  VRN EE CONNECTIONS          =          0
IST2020I TOTAL ACTIVE GLOBAL VRN EE CONNECTIONS          =          0
IST2021I TOTAL ACTIVE EE CONNECTIONS                     =          1
IST314I END
```

EE health verification …

```
d net,ee,id=SWIP2A1
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = EE
IST2001I ENTERPRISE EXTENDER CONNECTION INFORMATION
IST075I NAME = SWIP2A1, TYPE = PU_T2.1
IST1680I LOCAL IP ADDRESS 9.67.1.1
IST1680I REMOTE IP ADDRESS 9.67.1.2
IST2022I EE CONNECTION ACTIVATED ON 12/21/09 AT 16:21:57
IST2114I LIVTIME:    INITIAL =   10   MAXIMUM =    0   CURRENT =   10
IST2023I CONNECTED TO LINE LNIP1
IST2327I EE HEALTH VERIFICATION OPTION - EEVERIFY = 2 MINUTES
IST2329I EE HEALTH VERIFICATION SUCCESSFUL ON 12/21/09 AT 16:37:21
IST2341I EE HEALTH VERIFICATION HAS NEVER FAILED FOR THIS CONNECTION
IST2025I LDLC SIGNALS RETRANSMITTED AT LEAST ONE TIME    =        0
IST2026I LDLC SIGNALS RETRANSMITTED SRQRETRY TIMES       =        0
...
IST314I END
```

CTRACE Writer

CTRACE writer best practices

- Enable striping of data
  - –VSAM linear dataset
  - –Extended-Format sequential datasets
    - Specify EXTENDED for the DSNTYPE value in the data class
  - –Multiple sequential datasets
    - TRCOUTnn DD statements where nn is 01-16
    - Do not specify DCB parameters
    - Specify CONTIG on SPACE parameter
- Ensure dispatching priority is equal to or higher than work being traced

VSAM linear dataset

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
 DELETE                              +
   (hlq.CTRACE.LINEAR)               +
   CLUSTER

 DEFINE                              +
   CLUSTER(                          +
     NAME(hlq.CTRACE.LINEAR)         +
     LINEAR                          +
     MEGABYTES(10)                   +
     VOLUME(CPDLB0)                  +
     CONTROLINTERVALSIZE(32768)      +
     )                               +
   DATA(                             +
     NAME(hlq.CTRACE.DATA)           +
   )
```

Multiple sequential datasets

```
//IEFPROC EXEC PGM=ITTTRCWR,REGION=32M
//TRCOUT01  DD DSN=SYS1.CTRACE1,VOL=SER=TRACE1,UNIT=DASD,
//             SPACE=(CYL,10),DISP=(NEW,KEEP),DSORG=PS
//TRCOUT02  DD DSN=SYS1.CTRACE2,VOL=SER=TRACE2,UNIT=DASD,
//             SPACE=(CYL,10),DISP=(NEW,KEEP),DSORG=PS
//TRCOUT03  DD DSN=SYS1.CTRACE3,VOL=SER=TRACE3,UNIT=DASD,
//             SPACE=(CYL,10),DISP=(NEW,KEEP),DSORG=PS
```

COPYTRC

- Use the IPCS COPYTRC command to copy trace records to a sequential dataset
  - –VSAM linear dataset
  - –Multiple sequential datasets

```
COPYTRC TYPE(CTRACE) IDS(dslist) ODS(dsname) SPACE(pppp,ssss)

COPYTRC TYPE(CTRACE) INFILE(ddlist) OUTFILE(ddlist)
```

Shark Attack

A different way to look at network traces

- IPCS packet trace format utility provides a method to convert the trace into a format that can be viewed by Wireshark
- Wireshark is a freeware network protocol analyzer for Unix and Windows
  - Graphical interface
  - Protocol formatting
  - Protocol analysis
  - Throughput graphing
- Makes packet trace consumable by network performance teams

Converting a packet trace

- Allocate an output dataset
- Logical record length must be larger than the MTU size to accommodate pseudo Ethernet headers.

```
TSO ALLOC F(SNIFFER) DATASET('userid.sniffer.CAP') LRECL(1600)
    RECFM(VB) REUSE TRACK SPACE(15 15)
```

- Convert the trace in IPCS

```
IP CTRACE COMP(SYSTCPDA) SUB((tcpip)) SHORT OPTIONS((SNIFFER
  NOREASSEMBLY STATS))
```

- FTP the output dateset in BINARY mode to your PC

Command output

```
COMPONENT TRACE SHORT FORMAT
COMP(SYSTCPDA)SUBNAME((TCPIP))
OPTIONS((SNIFFER NOREASSEMBLY STATS))
z/OS TCP/IP Packet Trace Formatter, Copyright IBM Corp. 2000, 2013; 2013.016
DSNAME('D74L.HO55914A.TCPIP.PKT')
PTRPT04I SNIFFER(ETHERNET) option selected
.
.
.
Sniffer Report
  1,740 records written to X370812.SNIFFER.CAP
203,683 bytes written
      0 packets were abbreviated
    200 is the maximum data size
    400 packets were truncated from 200 bytes
```

QDIO Inbound Workload Queuing (IWQ)

What is IWQ

- z/OS Communications Server and OSA Express feature establish a primary input queue and one or more ancillary input queues (AIQ)
- Primary input queue (exists without IWQ) delivers all packets not routed to an AIQ
- AIQs are created for different traffic types
  - Streaming
  - Enterprise Extender
  - Sysplex Distributor

TRLE datapaths

- Each input queue requires a TRLE datapath
- Input queues are unique for IPv4 and IPv6
- OSAENTA trace requires an input queue
- 9 datapaths required to support IWQ for IPv4 and IPv6 with a datapath available for OSAENTA

```
OSAQ1     TRLE   LNCTL=MPC,                                    *
                 READ=(2D00),                                  *
                 WRITE=(2D01),                                 *
                 MPCLEVEL=QDIO,                                *
                 DATAPATH=(2D02-2D0A),                         *
                 PORTNAME=(OSAQDIO1,0)
```

INTERFACE statement

- IPAQENET or IPAQENET6
  - –INBPERF DYNAMIC WORKLOADQ
  - –VMAC

  - –READSTORAGE
    - GLOBAL (default)
      - – QDIOSTG VTAM start option value
    - MAX – 4M
    - AVG – 2M
    - MIN – 1M

Storage requirements

- QDIOSTG=???
  - MAX – 4M
  - AVG – 2M
  - MIN – 1M
  - nnn – Number of SBALs
    - Range is 3-126
    - Each SBAL is 64K
    - Maximum of ~8M

- Storage requirement is per active data path
- CMS FIXED dataspace

CSM Fixed limit

- Consider increasing the CSM Fixed limit
- SYS1.PARMLIB(IVTPRMxx)
  - FIXED MAX nnnK | nnnM
    - 1024K to 30720M
- Can be dynamically modified
  - F vtamproc,CSM,FIXED=value

- One OSA with all 9 datapaths active and 126 SBALs requires ~72M of CSM fixed storage

For more information

URL	Content
http://twitter.com/IBM_Commserver	IBM z/OS Communications Server Twitter Feed
http://facebook.com/IBMCommserver	IBM z/OS Communications Server Facebook Page
http://tinyurl.com/zoscsblog	IBM z/OS Communications Server Blog
http://ibm.com/systems/z/	IBM System z in general
http://ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://ibm.com/software/networking/commserver/zos/	IBM z/OS Communications Server
http://redbooks.ibm.com	ITSO Redbooks
http://ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical support
http://ibm.com/support/techdocs/atsmastr.nfs/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flags, presentations, whitepapers, etc.)
http://rfc-editor.org/rfcsearch.html	Request for Comments (RFC)
http://ibm.com/systems/z/os/zos/library/bkserv/	IBM z/OS Internet Library
http://ibm.com/developerworks/rfe/?PROD_ID=498	RFE Community for z/OS Communications Server
http://ibm.com/developerworks/rfe/execute?use_case=tutorials	RFE Community Tutorials