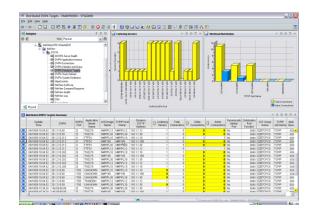# How to Manage TCP/IP with NetView for z/OS V5R4
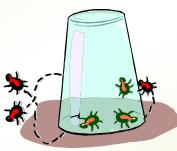
Ernie Gilman

IBM

August 5th 2010

Session 7618

AGENDA

- **Addressing Networking Challenges with IBM NetView for z/OS V5.4**

z/OS Communication Server Network Management

1. Real Time TCP/IP Packet Trace
2. Real time OSA Trace
3. OSA Monitoring
4. IP Stacks
5. DVIPA
6. TCP/IP Connections
7. Telnet Server
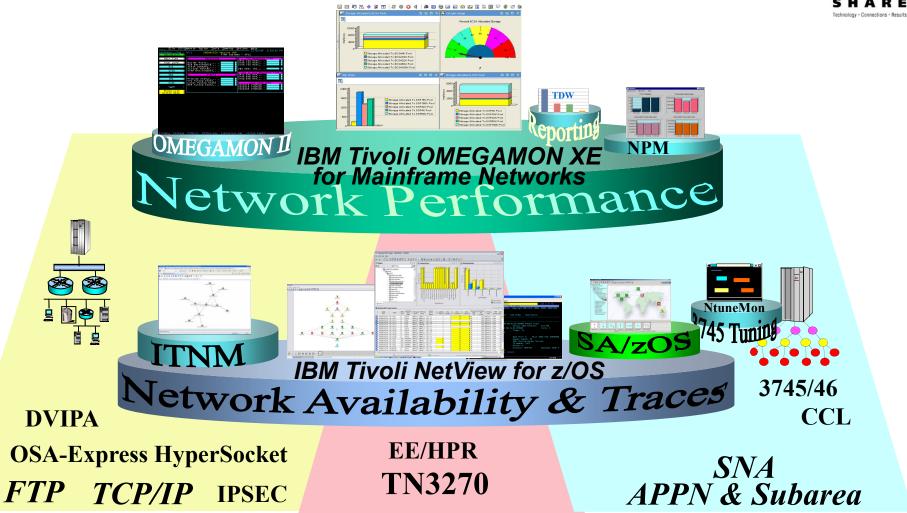8. SNA over IP EE/HPR

Next, Overview of Network Management

When did NetView start managing TCP/IP?

Release	Year	Major New TCP/IP Functions
Tivoli NetView for z/OS V5R4	2009	Real time Trace, TEP Enhancements
Tivoli NetView for z/OS V5R3	2007	TEP Agent DVIPA and TCP/IP workspaces
Tivoli NetView for z/OS V5R2	2005	TCP/IP and SNMP Enhancements
Tivoli NetView for z/OS V5R1	2002	TCP/IP and SNMP Enhancements, Web GUI
Tivoli NetView for OS/390 V1R4	2001	TCP/IP and SNMP Enhancements
Tivoli NetView for OS/390 V1R3	1999	TCP/IP and SNMP Enhancements

IBM z/OS Network Performance Monitoring and Management

OMEGAMON II

IBM Tivoli OMEGAMON XE for Mainframe Networks

TDW

Reporting

NPM

Network Performance

ITNM

IBM Tivoli NetView for z/OS

SA/zOS

NtuneMon

3745 Tuning

Network Availability & Traces

3745/46 CCL

DVIPA

OSA-Express HyperSocket

FTP   TCP/IP   IPSEC

EE/HPR

TN3270

SNA
APPN & Subarea

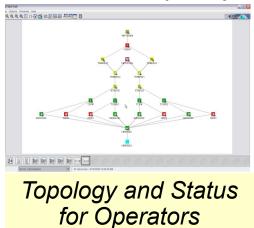*Next, Data collection and User Interfaces*
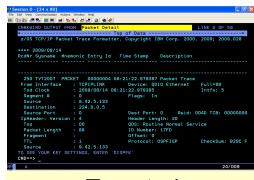
z/OS Network Performance Data Collection and User Interfaces

Network Management Console (NMC)

Topology and Status for Operators
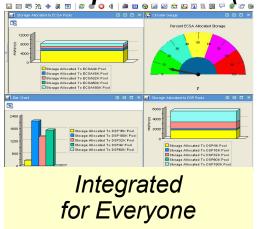
3270

Targeted for Specialists

Tivoli Enterprise Portal (TEP)

Integrated for Everyone

NetView for z/OS

OMEGAMON XE for Mainframe Networks

NLDM API | Trace API | VTAM API | TCP/IP API | SNMP

z/OS Communications Server NMI APIs

Network Management Interface API (NMI)

✓Fast
✓Scalable
✓Reliable

Next, what is the TEP?

What is the Tivoli Enterprise Portal (TEP)?

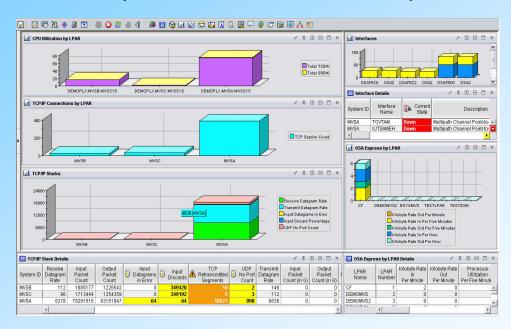## Common user interface
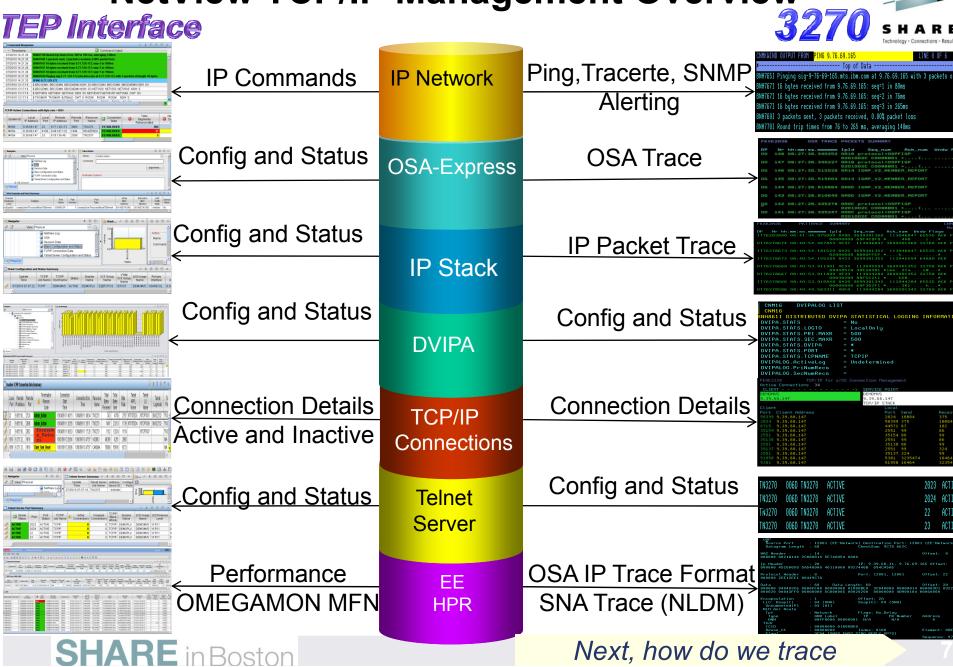
▸ Manage z/OS and distributed resources from a single browser interface.

▸ Displays data in graphs, charts and table formats

▸ View real time and historical data, at the same time

- **Easy to configure, right from the TEP**

- **Out of the box Best Practices**

▸ Workspaces, Situations, and Expert Advice

Next, an Overview
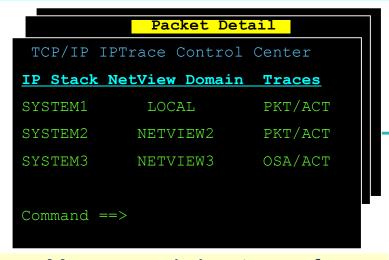
NetView TCP/IP Management Overview

TEP Interface

3270

SHARE — Technology · Connections · Results

IP Commands	**IP Network**	Ping, Tracerte, SNMP Alerting
Config and Status	**OSA-Express**	OSA Trace
Config and Status	**IP Stack**	IP Packet Trace
Config and Status	**DVIPA**	Config and Status
Connection Details Active and Inactive	**TCP/IP Connections**	Connection Details
Config and Status	**Telnet Server**	Config and Status
Performance OMEGAMON MFN	**EE HPR**	OSA IP Trace Format SNA Trace (NLDM)

Real Time Traces

- Formatted Real-Time Traces
- Gather, format and refresh packets – With a new trace user interface
  - ▸ IP Packet Trace
    - Requires z/OS Communications Server V9 later
  - ▸ OSA-Express2 Network Traffic
    - Requires z/OS Communications Server V1R11 or later and OSA-Express2 Card
  - Reduced overhead by leveraging NetView Dataspaces

```
                    Packet Detail
   TCP/IP IPTrace Control Center

   IP Stack NetView Domain    Traces

   SYSTEM1      LOCAL         PKT/ACT

   SYSTEM2      NETVIEW2      PKT/ACT

   SYSTEM3      NETVIEW3      OSA/ACT


   Command ==>
```

z/OS

NetView For z/OS **Trace Dataspaces**

NMI API

Communication Server for z/OS

z/OS

NetView2

z/OS

NetView3

Manage and view traces for all stacks on all LPARS from one central NetView
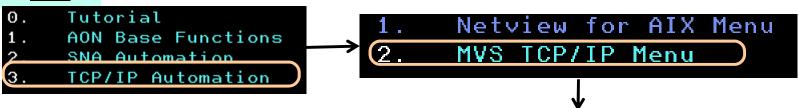
Next, lets look at a scenario

Real Time Traces from Menu or Command

Issue AON

```
0.      Tutorial
1.      AON Base Functions
2.      SNA Automation
3.      TCP/IP Automation
```
→
```
1.      Netview for AIX Menu
2.      MVS TCP/IP Menu
```

IP Management options:

```
1.  Issue Ping
2.  MVS IP Session Status
3.  Issue Tracerte Command
4.  Issue Commands
5.  SNMP MENU
6.  IP Server Management
7.  IP Resource Manager
8.  SNMP View
9.  CISCOWorks Blue Inter-network Status Monitor
10. TCP/IP Trace Control Center.  SP: _____
```

Or issue IPSTRACE

Status of All Traces on All Stacks

Service Point/ Stack	Proc Name	NetView Domain	Trace Status
DEMOMVS	TCPIP	LOCAL	CTRACE/ACT PKT/ACT OSA/ACT
DEMOMVS2	TCPIP	CNM17	CTRACE/ACT OSA/ACT
DEMOMVS3	TCPIP	CNM18	CTRACE/ACT OSA/ACT

PKT/ACT = Active Packet Trace.
OSA/ACT = Active OSA Trace.

Status of All Traces on Selected Stack

Select TCP/IP Packet Trace hit Enter

```
FKXK2A01              IPTrace Control Center                        CNM16


Service Point/Stack: DEMOMVS              Proc: TCPIP          Domain: LOCAL

                         Status/Owner     Start                  For      Writer

_   CTRACE     SYSTCPIP  ACTIVE/NA        NA                     NA       *NONE*


s_  PKTTRACE   SYSTCPDA  ACTIVE/MS519     2010-07-19-10:14:17    NA       *NONE*


_   OSATRACE   SYSTCPOT  ACTIVE/NA        NA                     NA       *NONE*
```

Manage TCP/IP PKTS Trace

```
FKXK2A22        PKTTRACE  Control  SYSTCPDA  ACTIVE     for NVDomain: LOCAL
                                                            z/OS    : V1R11
Service Point/Stack: DEMOMVS     TCPNAME: TCPIP
PKTS: ACTIVE          On Task: AUTOPKTS      GTF: NO

Start Time: 2010-07-19-10:14:17                    Writer:  *NONE*

  Options: 1-START/ADD 2-STOP  3-VIEW PACKETS
                                                    _____Ports_____   Record
    Infc/Link           Stat Prot IP Address/Prefix     Src PortNm Dest  Count

3 _ ALL                          *   *                     *    *    *
  _ LOOPBACK           ON   *   *                          *    *    *   63754750
  _ EELINK1            ON   *   *                          *    *    *   0
  _ OSAFBC0L           ON   *   *                          *    *    *   12204744
  _ EZASAMEMVS         ON   *   *                          *    *    *   16508
  _ EZAXCFS3           ON   *   *                          *    *    *   0
  _ EZAXCFS2           ON   *   *                          *    *    *   0




Command ===>
F1=Help        F2=Main Menu     F3=Return   F4=Stop SYSTCPDA  F5=Refresh   F6=Roll
F7=Backward    F8=Forward       F9=Assist   F10=PKTS Management            F12=Cancel
```

Turn ON or OFF TCP/IP PKT Traces

Set FILTERS

View Packets

Set Filters

```
FKXK2A24                  Display Packet Control                    LOCAL

  Service Point/Stack: DEMOMVS   Proc: TCPIP      Infc Name: ALL


  LAddr  *

  RAddr  9.76.69.165

  PORTNUM  *          LPort: *        RPort: *       Protocol 1   1-ALL
                                                                  2-TCP
                                                                  3-UDP
  Time: Start   *                                                 4-OSPF
        End     *                                                 5-     (Number)


  MaxRecs: 1   1-Last     100       Truncate:   65535
               2-First




Command ===>
F1=Help                          F3=Return        F4=View Packets         F6=Roll
           F8=Extended Options                                            F12=Cancel
```

SET FILTERS

NUMBER OF RECORDS

Summary View of Packets

```
FKXK2A26        PKTTRACE   SUMMARY                              CNM16
                                                                More:
DP    Nr hh:mm:ss.mmmmmm IpId     Seq_num     Ack_num  Wndw Flags
IT76283880 08:41:34.975009 848D 3699301360  113946847 65535 ACK PSH
                     00000000 69F4C8F8 *.....4H8 ....i...*
OT76278674 08:40:54.467843 4E37  113946847 3699301360 32760 ACK PSH

IT76278673 08:40:54.181529 8425 3699301352  113946847 65535 ACK PSH
                     02000000 8800FFEF *....h... .........*
IT76278672 08:40:54.155289 8423 3699301352  113945594 64880 ACK

OT76278668 08:40:53.911901 4E34  113945594 3699301352 32758 ACK PSH
                     8994857A 40E2A381 *ime: Sta ...z@...*
OT76278667 08:40:53.911899 4E33  113944284 3699301352 32758 ACK
                     00030200 88F5C211 *....h5B. .........*
IT76278666 08:40:53.910848 8420 3699301342  113944284 65535 ACK PSH
                     00000000 68F3D2F1 *.....3K1 ....h...*
OT76278586 08:40:49.563311 4DFA  113944284 3699301342 32760 ACK PSH
```

Scroll up and down

F5: Refresh data space with new trace records

```
Command ===>
F1=Help                    F3=Return      F4=Details  F5=Refresh
F7=Backward F8=Forward     F9=Commands                F11=Right
```

View Formatted Packet Detail

```
CNMKWIND OUTPUT FROM   Packet Detail                        LINE 20 OF 93
   Source            : 9.39.68.147
   Destination       : 9.76.69.165

  TCP
   Source Port       : 23     (telnet)   Destination Port: 2697  ()
   Sequence Number   : 113945594          Ack Number: 3699301352
   Header Length     : 32                 Flags: Ack Psh
   Window Size       : 32758              CheckSum: A1B6 6AEF Urgent Data Pointer:
    Option           : NOP
    Option           : NOP
    Option           : Timestamp          Len: 10 Value: 3D8F07B3 Echo: 001B7125

Telnet: 1253
04E3 CMD        IAC,EOR

Ip Header           : 20                 IP: 9.39.68.147, 9.76.69.165 Offset:  0
000000 45680519 4E340000 40060000 09274493  094C45A5

Protocol Header     : 32                 Port: 23, 2697              Offset: 14
000000 00170A89 06CAABFA DC7EDBE8 80187FF6  A1B60000 0101080A 3D8F07B3 001B7125
```

Commands from Packets Summary

```
FKXK2A28        PKTTRACE  SUMMARY  COMMANDS                    D52NV
                                            Select 1 for Ping
                                                                     U
DP    Nr hh:mm:ss.mmmmmm IpId    Seq_num    *****************************
IO   255 08:21:29.707500 2E35 protocol=OSP   _1 Command
                         02010044 C0096701
IO   253 08:21:25.991207 05F8 protocol=OSP     1. Ping      (RAddr)
                         02010044 C0096A01      2. TraceRte (RAddr)
IO   251 08:21:23.572996 0C0D protocol=OSP     3. Hostnames
                         02010044 C0096601      4. Connections
IO   250 08:21:22.979387 17FD protocol=OSP     5. SNMP      (RAddr)
                         02010044 C0096801      6. SNMP      (Stack)
IO   249 08:21:22.852632 08A7 protocol=OSP
                         02010044 C0096C01
IO   248 08:21:21.910456 1795 protocol=OSP
                         02010044 C0097501    F1=Help       F3=Return
OO   247 08:21:20.849382 079D protocol=OSP   F6=Roll       F12=Cancel
                         02010044 C0096B01  *****************************
IU   246 08:21:20.269648 14FB protocol=UDP
                         57B20110 00010000 *........ W........*
```

Commands are issued against the IP resource of the selected Packet.

RADDR issue command to the external address STACK issue command to the local IP Stack

```
Command =:
F1=Help                    F3=Return      F4=Details  F5=Refresh          F6=Roll
F7=Backward F8=Forward     F9=Commands                 F11=Right          F12=Cancel
```

Ping and TRACERTE Results

```
CNMKWIND OUTPUT FROM   PING 9.76.69.165                          LINE 0 OF 6
*----------------------------- Top of Data -----------------------------*
BNH765I Pinging sig-9-76-69-165.mts.ibm.com at 9.76.69.165 with 3 packets of le
BNH767I 16 bytes received from 9.76.69.165: seq=1 in 80ms
BNH767I 16 bytes received from 9.76.69.165: seq=2 in 76ms
BNH767I 16 bytes received from 9.76.69.165: seq=3 in 265ms
BNH769I 3 packets sent, 3 packets received, 0.00% packet loss
BNH770I Round trip times from 76 to 265 ms, averaging 140ms
*----------------------------- Bottom of Data --------------------------*
```

```
CNMKWIND OUTPUT FROM   TRACERTE 9.76.69.165                      LINE 0 OF 13
*----------------------------- Top of Data -----------------------------*
BNH810I Tracing IP route to 9.76.69.165 max 30 hops
BNH811I 1: net68router.demopkg.ibm.com (9.39.68.1) 0ms 1ms 0ms
BNH811I 2: aus-pd-9a-v794.austin.ibm.com (9.3.53.195) 2ms 2ms 6ms
BNH811I 3: aus-co-a-v836.austin.ibm.com (9.41.2.145) 1ms 1ms 1ms
BNH811I 4: aus-bd-a-ge4.austin.ibm.com (9.41.2.2) 1ms 2ms 1ms
BNH811I 5: aus-sc-b-v257.austin.ibm.com (9.41.1.14) 0ms 0ms 1ms
BNH811I 6: aus-p9-a.austin.ibm.com (9.41.4.6) 1ms 1ms 1ms
BNH811I 7: 9.64.34.114 (9.64.34.114) 7ms 7ms 7ms
BNH811I 8: CT003-R02-12008-POS1-0-101.wan.ibm.com (9.64.5.81) 54ms 54ms 54ms
BNH811I 9: sbr-sc-a-ge3-1.sby.ibm.com (9.45.4.11) 59ms 60ms 60ms
BNH811I 10: sbr-id-1a-ge0-1.sby.ibm.com (9.45.104.3) 58ms 59ms 60ms
BNH811I 11: SIG03523.sby.ibm.com (9.45.101.150) 61ms 60ms 58ms
BNH811I 12: sig-9-76-69-165.mts.ibm.com (9.76.69.165) 77ms 78ms 74ms
```

Extended Formatting options

```
FKXK2A25        Display Packets Control Extended Options        CNM16

 Service Point/Stack: DEMOMVS  Proc: TCPIP      Infc Name: ALL

   4  1-Summary    1  1-Local    4  1-PortSel    1  1-Segment    LineSize: 80
      2-Full          2-GMT          2-Both          2-NoSegment  Cleanup:  500
      3-Short                        3-Ascii
      4-Tally                        4-Ebcdic
                                     5-Hex


 Format: __  1-Detail      Stats: _1 1-Summary      Basic: __ 1-Detail
             2-Summary             2-Detail                   2-Summary


 Reassem: 65535 , 1  1-Summary    Session: 3  1-Detail      __ 1-Dump  65535
                     2-Detail                  2-State
                     3-NoReassem                3-Summary


 Streams: 128    , __ 1-Summary
                     2-Detail




 Command ===>
 F1=Help                     F3=Return      F4=Display Packets      F6=Roll
 F7=Query Opts                                                      F12=Cancel
```

Example of Packet Analysis

```
Window Stats:                        Inbound,         Outbound
  Number of windows:                     31,               15
  Maximum window size:                    0,            32760
  Largest window advertised:          65535,            32760
  Average window advertised:          65383,            32757
  Smallest window advertised:         64880,            32754
  Window scale factor:                    0,                0
  Window frequency:                  0.2277,           0.1101 Windows/s
  Time Stamp updates:                    33,               31
  Total Round Trip Time:           1.391616,       135.852032 ( 0.79%), (77.96%
  Average Round Trip Time:         0.000000,         0.000000
  Maximum Data in Pipe:                  14,             2743
  Maximum retransmisson:                  0,                0

Number of:                           Inbound,         Outbound
  Packets:                               52,               48
   (x) Untraced Packets:                  0,                0
   (.) In-order data:                    20,               16 (38.46%), (33.33%
   (a) Acknowledgments:                   4,                0 ( 7.69%), ( 0.00%
   (+) Data and ACK:                     11,               15 (21.15%), (31.25%)
   (u) Duplicate ACKs:                    3,                0 ( 5.76%), ( 0.00%)
   (w) Window size updates:               1,                1 ( 1.92%), ( 2.08%)
   (z) Zero window sizes:                 0,                0 ( 0.00%), ( 0.00%)
   (p) Window probes:                     0,                0 ( 0.00%), ( 0.00%)
   (k) Keepalive segments:                0,                0 ( 0.00%), ( 0.00%)
   (r) Retransmissions:                   0,                1 ( 0.00%), ( 2.08%)
   (o) Out-of-order:                      0,                0 ( 0.00%), ( 0.00%)
   (d) Delayed ACKs:                     13,               15 (25.00%), (31.25%)
   (f) Fragments:                         0,                0 ( 0.00%), ( 0.00%)
   (!) Dropped:                           0,                0 ( 0.00%), ( 0.00%)
```

Next. lets look at OSA Trace

OSA-Express2 Real Time Trace

- Supports tracing of OSA packets with **OSA-Express2** Network Traffic

- Analyzer Requires OSA Express 2 card or higher

- Requires **z/OS V1R11** Communications Server or later

- Allows for capture and formatting of
  - Ethernet data (Ethernet type, source/destination MAC addresses, VLAN tag, LLC fields)
  - IPv4 & IPv6 data
  - ARP packets
  - SNA transmission headers
  - **Enterprise Extender**
  - Direction indicators
  - Discard code
  - Interface identification

- Syntax and behavior similar to TCP/IP packet trace

- Simultaneous Capture Filters
  - IP Address Protocol, Ethernet type, Port, Device, VLAN, MAC Address

OSA Trace Control

```
FKXK2A30      OSATRACE  Control  SYSTCPOT  ACTIVE       for NVDomain: LOCAL
                                                                 z/OS      : V1R11
Service Point/Stack: TVT2007    TCPNAME: TCPIP7
OPKTS: ACTIVE       On Task: AUTOOPKT    GTF: NO

Star traced packets.          4-08:18:56                    Writer:  *NONE*


  Options: 1-START    2-STOP   3-VIEW PACKETS


   OSA Port  Stat/ Length Data      Record      Time  Discard   Nofilter
             Auth

3  OSAA      ON    224    1024      2147483647 10080 EXCEPTION ALL
             LOGICAL      0         118         6     0
_  OSA1      OFF   224    1024      2147483647 10080 EXCEPTION NONE
             UNKNOWN      0         0           0     0
_  _____  NEW   224    1024      2147483647 10080 EXCEPTION NONE




Command ===>
F1=Help                            F3=Return   F4=Stop SYSTCPOT  F5=Refresh   F6=Roll
F7=Backward  F8=Forward   F9=Filters    F10=PKTS Management           F12=Cancel
```

OSA Tracing is active

NetView domain and z/OS level

NetView is collecting traced packets.

Capture Filters

Select OSA Port

F9: Apply Capture Filters   F4: Stop OSA Tracing

OSA Filters

```
FKXK2A31        OSATRACE  Filters  SYSTCPOT   ACTIVE     for NVDomain: LOCAL
                                                         z/OS      : V1R11
Service Point/Stack: TESTMVS              Proc: TCPIP

OSA Port Name: OSAF7C0P                   Clear Filters: NO    (YES/NO)

-----------------------------------------------------------------------------
 Protocol  | Ethernet  | Port   | Device   | VLAN ID  | Mac Address
           | Type      |        | ID       |          |
           |           |        |          |          |
 UDP       | _____   | 12000  | _____  | _____  | _____
 _____   | _____   | 12001  | _____  | _____  | _____
 _____   | _____   | 12002  | _____  | _____  | _____
 _____   | _____   | 12003  | _____  | _____  | _____
 _____   | _____   | 12004  | _____  | _____  | _____
 _____   | _____   | _____  | _____  | _____  | _____
 _____   | _____   | _____  | _____  | _____  | _____
 _____   | _____   | _____  | _____  | _____  | _____
-----------------------------------------------------------------------------


Command ===>
F1=Help                    F3=Return    F4=Update Filters              F6=Roll
        F8=IP Addesses                                               F12=Cancel
```

Example of Enterprise Extender UDP ports to trace

View OSA Express Packet Summary

```
FKXK2A36          OSA TRACE PACKETS SUMMARY                    D52NV
                                                                 :+
DP    Nr hh:mm:ss.mmmmmm IpId     Seq_num    Ack_num  Wndw Flags
OO   148 08:27:36.340252 0A16 protocol=OSPFIGP
                         0201002C C0096B01 *....{.,. ...,..k.*
OO   147 08:27:36.340227 0A16 protocol=OSPFIGP
                         0201002C C0096B01 *....{.,. ...,..k.*
OG   146 08:27:30.515029 0A14 IGMP_V2_MEMBER_REPORT

OG   145 08:27:30.515004 0A14 IGMP_V2_MEMBER_REPORT

OG   144 08:27:28.610664 0A0D IGMP_V2_MEMBER_REPORT

OG   143 08:27:28.610640 0A0D IGMP_V2_MEMBER_REPORT

OO   142 08:27:26.335278 0A0C protocol=OSPFIGP
                         0201002C C0096B01 *....{.,. ...,..k.*
OO   141 08:27:26.335247 0A0C protocol=OSPFIGP
                         0201002C C0096B01 *....{.,. ...,..k.*



Command ===>
F1=Help                  F3=Return     F4=Details  F5=Refresh       F6=Roll
F7=Backward F8=Forward                             F11=Right        F12=Cancel
```

Latest Enhancements for TCP/IP Packet Trace Formatter

NetView users will see Packet Trace formatting enhancements from Communications Server for z/OS.
These updates can be applied to previous Versions of Communications Server for z/OS

Software > Networking > Communications Server >

Support & downloads

z/OS Communications Server

Features and benefits

System requirements

Library

News

Trials and demos

How to buy

Events

Training and certification

Services

Support

SYSTCPDA: z/OS Communications Server TCP/IP Packet Trace Formatter

Downloadable files

Abstract
This is the downloadable package for the z/OS Communication Service Packet Trace Formatter

Download Description
This program will format packet trace records created by the z/OS Communications Server SYSTCPDA trace component.

Change History
Release Date - 07/03/2004

Prerequisites
z/OS Communications Server

Document information

Product categories:

Software

Networking

Enterprise Connectivity

z/OS Communications Server

Operating system(s): **z/OS**

Software version: **1.8, 1.9, 1.10, 1.11**
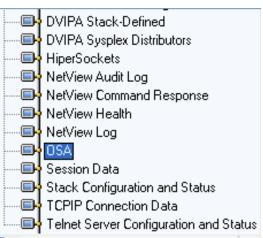
Reference #: 4007395

http://www-01.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=D400&uid=swg24007395

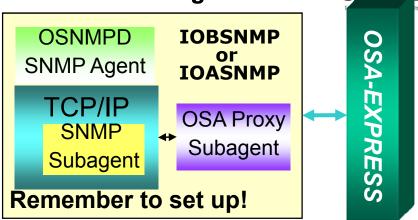*Next, look at OSA within a Topology*

Management of OSA-EXPRESS

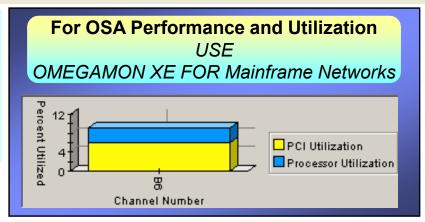*NetView for z/OS OSA Channels and Ports Status and Configuration*

- DVIPA Stack-Defined
- DVIPA Sysplex Distributors
- HiperSockets
- NetView Audit Log
- NetView Command Response
- NetView Health
- NetView Log
- **OSA**
- Session Data
- Stack Configuration and Status
- TCPIP Connection Data
- Telnet Server Configuration and Status

OSNMPD SNMP Agent

IOBSNMP or IOASNMP

TCP/IP SNMP Subagent

OSA Proxy Subagent

OSA-EXPRESS

Remember to set up!

OSA in TEP Requires RODM

OSA Channels and Ports Summary

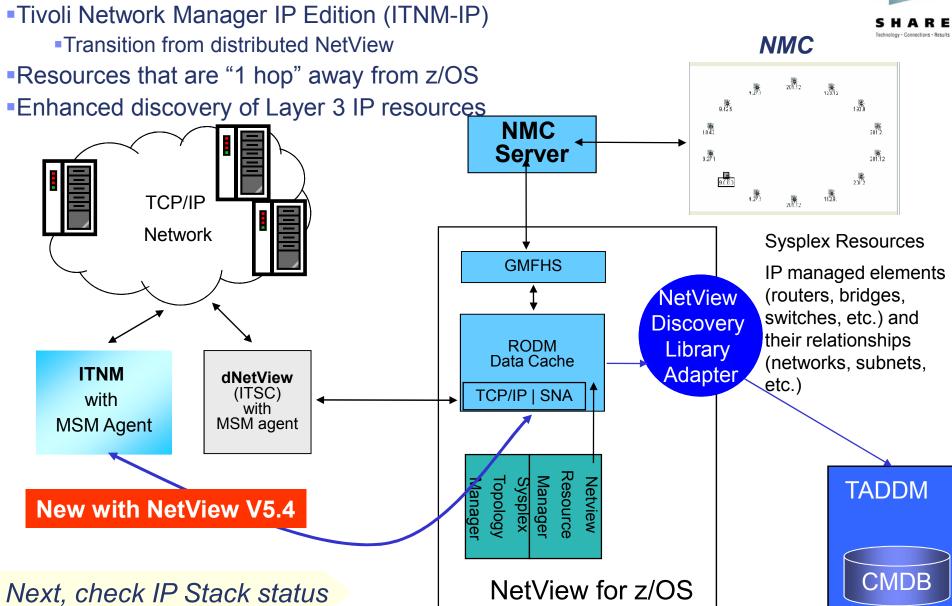| Collection Time	Channel Number	Channel Hardware Level	Subtype	Port Name	Port Number	Port Type	Active MAC Address	Bu Ac
07/27/09 14:07:58	09	osaExp300	oneThousandBaseTEthernet	OSAA	0	oneThousandBaseTEthernet	00145EB712C6	00145

Is my OSA Configured Wrong?

What is the MAC Address and Port?

Is the Configured Speed incorrect?

Is it in Service Mode?

Next, Let's check the Hypersocket

For OSA Performance and Utilization
USE
OMEGAMON XE FOR Mainframe Networks

Percent Utilized — PCI Utilization / Processor Utilization — Channel Number
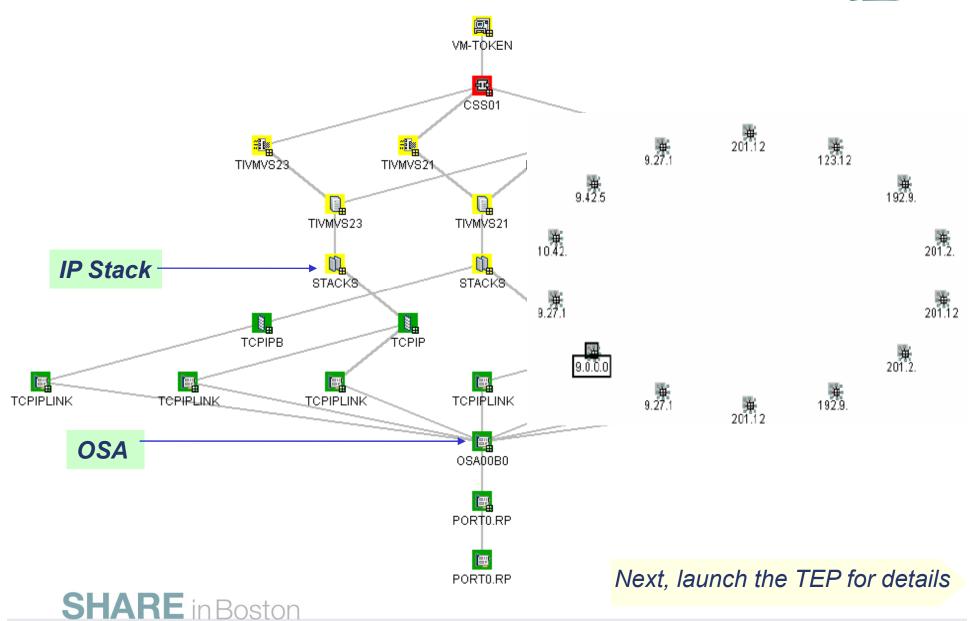
NetView for the z/OS Network Discovery

- Tivoli Network Manager IP Edition (ITNM-IP)
  - Transition from distributed NetView
- Resources that are "1 hop" away from z/OS
- Enhanced discovery of Layer 3 IP resources

NMC

NMC Server

TCP/IP Network

GMFHS

RODM Data Cache

TCP/IP | SNA

Topology Manager | Sysplex Manager | Netview Resource Manager

ITNM with MSM Agent

dNetView (ITSC) with MSM agent

NetView Discovery Library Adapter

Sysplex Resources

IP managed elements (routers, bridges, switches, etc.) and their relationships (networks, subnets, etc.)

New with NetView V5.4

TADDM

CMDB

NetView for z/OS

Next, check IP Stack status

IP Topology from the NMC

IP Stack

OSA

Next, launch the TEP for details

TCP/IP IP Stack Status and Configuration

NetView Health
NetView Log
OSA
Session Data
Stack Configuration and Status
TCPIP Connection Data
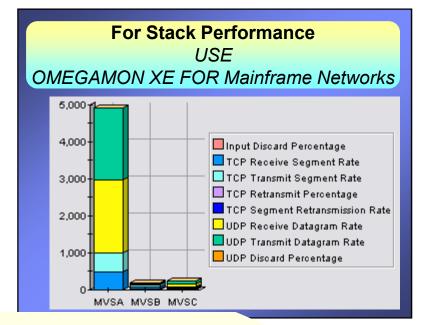Telnet Server Configuration and Status

Stack Configuration and Status Summary

	Update Time	TCPIP Job Name	TCPIP Host Name	Status	Sysplex Name	XCF Group Name	VTAM XCF Group Name	zOS Image Name	Primary Interface	IP Address	IPv6 Enabled	IPSec Enabled	AT-TLS Enabled	Source VIPA Enabled	TCP Stack Source VIPA Enabled	Segmentation Offload Enabled	zIIP IP Security Enabled	Sysplex WLM Polling Interval	
🔵	04/12/09 17:03:16	TCPIPB	NMPIPL12B	INACTIVE	NVDPLEX1	EZBTCPCS	ISTXCF	NMPIPL12	TCPIPLINK	9.42.40.79	Yes	No	No	No	No	No	No	0	V
🔵	04/12/09 17:03:14	TCPIP	NMPIPL12	ACTIVE	NVDPLEX1	EZBTCPCS	ISTXCF	NMPIPL12	TCPIPLINK	9.42.45.12	Yes	No	No	No	No	No	No	0	V
🔵	04/12/09 10:10:41	TCPIP	NMPIPL30	ACTIVE	NVDPLEX1	EZBTCPCS	ISTXCF	NMPIPL30	TCPIPLINK	9.42.45.30	Yes	No	No	No	No	No	No	0	V
🔵	04/12/09 10:10:05	TCPIP	NMP190	ACTIVE	NVDPLEX1	EZBTCPCS	ISTXCF	NMP190	TCPIPLINK	9.42.45.190	Yes	No	No	No	No	No	No	0	V
🔵	04/12/09 10:10:05	TCPIP	NMPIPL10	ACTIVE	NVDPLEX1	EZBTCPCS	ISTXCF	NMPIPL10	TCPIPLINK	9.42.45.10	Yes	No	No	No	No	No	No	0	V

🖉 DVIPA Stack Summary
🖉 Telnet Server Configuration and Status
🖉 Link Wizard...
🖉 Link Anchor...

Is the IP Stack up?

Is Segmentation Offload Enabled?

Is zIIP IP Security offload Enabled?

For Stack Performance
USE
OMEGAMON XE FOR Mainframe Networks

Legend:
- Input Discard Percentage
- TCP Receive Segment Rate
- TCP Transmit Segment Rate
- TCP Retransmit Percentage
- TCP Segment Retransmission Rate
- UDP Receive Datagram Rate
- UDP Transmit Datagram Rate
- UDP Discard Percentage
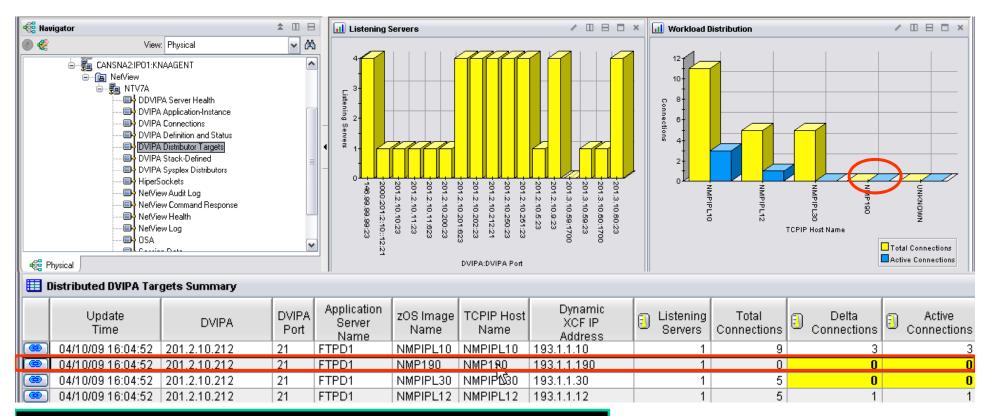
DVIPA Management

Notice FTP connections are not distributed evenly over DVIPA Targets. This could be caused by WLM or XCF issues.

Distributed DVIPA Targets Summary

	Update Time	DVIPA	DVIPA Port	Application Server Name	zOS Image Name	TCPIP Host Name	Dynamic XCF IP Address	Listening Servers	Total Connections	Delta Connections	Active Connections
	04/10/09 16:04:52	201.2.10.212	21	FTPD1	NMPIPL10	NMPIPL10	193.1.1.10	1	9	3	3
	04/10/09 16:04:52	201.2.10.212	21	FTPD1	NMP190	NMP190	193.1.1.190	1	0	0	0
	04/10/09 16:04:52	201.2.10.212	21	FTPD1	NMPIPL30	NMPIPL30	193.1.1.30	1	5	0	0
	04/10/09 16:04:52	201.2.10.212	21	FTPD1	NMPIPL12	NMPIPL12	193.1.1.12	1	5	1	1

There are Similar 3270 NetView DVIPA Commands
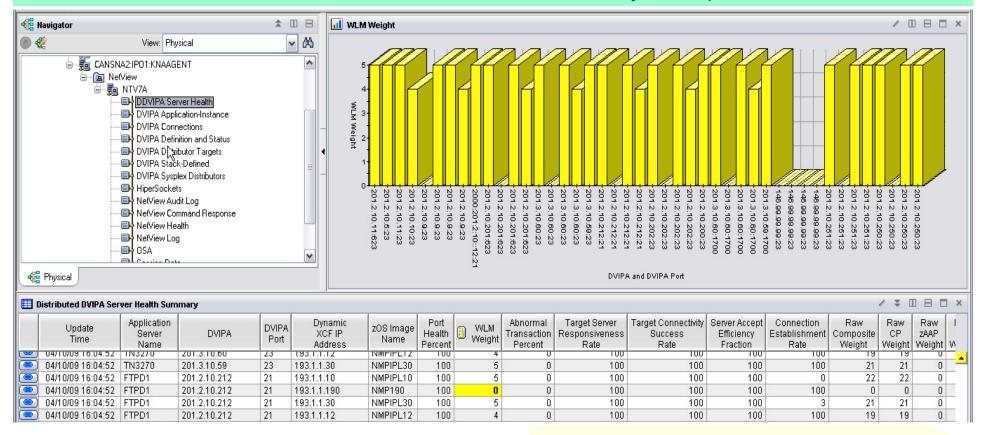
Next, check the DVIPA Server Health

Distributed DVIPA Server Health

Look at methods and weights, they Influence where connections go

- **Weights**: *WLM, zAAP, CP, zIIP,and Composite*
- **Methods:** *ROUNDROBIN, BASEWLM, SERVERWLM, WEIGHTEDACTIVE, TARGETCONTROLLED*

NetView DVIPA Server Health and Unhealthy Workspaces:

Distributed DVIPA Server Health Summary

	Update Time	Application Server Name	DVIPA	DVIPA Port	Dynamic XCF IP Address	zOS Image Name	Port Health Percent	WLM Weight	Abnormal Transaction Percent	Target Server Responsiveness Rate	Target Connectivity Success Rate	Server Accept Efficiency Fraction	Connection Establishment Rate	Raw Composite Weight	Raw CP Weight	Raw zAAP Weight	
	04/10/09 16:04:52	TN3270	201.3.10.60	23	193.1.1.12	NMPIPL12	100	4	0	100	100	100	100	19	19	0	
	04/10/09 16:04:52	TN3270	201.3.10.59	23	193.1.1.30	NMPIPL30	100	5	0	100	100	100	100	21	21	0	
	04/10/09 16:04:52	FTPD1	201.2.10.212	21	193.1.1.10	NMPIPL10	100	5	0	100	100	100	0	22	22	0	
	04/10/09 16:04:52	FTPD1	201.2.10.212	21	193.1.1.190	NMP190	100	0	0	100	100	100	100	0	0	0	
	04/10/09 16:04:52	FTPD1	201.2.10.212	21	193.1.1.30	NMPIPL30	100	5	0	100	100	100	3	21	21	0	
	04/10/09 16:04:52	FTPD1	201.2.10.212	21	193.1.1.12	NMPIPL12	100	4	0	100	100	100	100	19	19	0	

Next, Look at DVIPA Expert Advice

DVIPA Expert Advice Provided with Situations
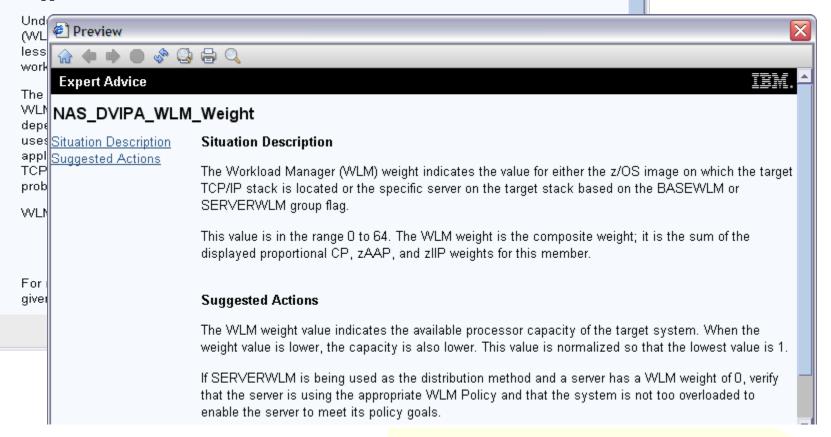
NAS_DVIPA_Port_Health_Percent

Situation Description
Suggested Actions

Situation Description

The port health percent indicates the health of the server application on the target port. If several server applications share the port, it is the average of the individual values for all the server applications sharing the port.

Suggested Actions

Und
(WL
less
work

The
WLM
depe
uses
appl
TCP
prob

WLM

For
give

Preview

Expert Advice

IBM.

NAS_DVIPA_WLM_Weight

Situation Description
Suggested Actions

Situation Description

The Workload Manager (WLM) weight indicates the value for either the z/OS image on which the target TCP/IP stack is located or the specific server on the target stack based on the BASEWLM or SERVERWLM group flag.

This value is in the range 0 to 64. The WLM weight is the composite weight; it is the sum of the displayed proportional CP, zAAP, and zIIP weights for this member.

Suggested Actions

The WLM weight value indicates the available processor capacity of the target system. When the weight value is lower, the capacity is also lower. This value is normalized so that the lowest value is 1.

If SERVERWLM is being used as the distribution method and a server has a WLM weight of 0, verify that the server is using the appropriate WLM Policy and that the system is not too overloaded to enable the server to meet its policy goals.

Next, Look at TCP/IP Connections

TCP/IP Connections

User calls complaining that TCP/IP connections fails all the time.
We see that the connection failed due to Excessive Retransmissions.
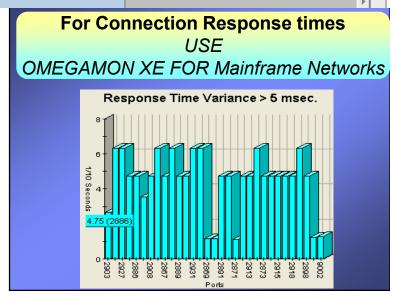
- How often is this connection failing?
- What is the number and percent of segments that were retransmitted
- What is the window size?
- Problem could be caused by high CPU at the remote resource.

Inactive TCPIP Connection Data Summary

	Local Port	Remote IP Address	Remote Port	⚠ Termination Reason Code	Connection Start Time	Connection End Time	Resource Name	Total Bytes Received	Total Bytes Sent	Byte Rate	Telnet APPL Name	Telnet LU Name	Telnet Logmode	Te Prc
	23	9.65.156....	2724	Admin_Action	10/04/09 11:46:15	10/04/09 11:48:04	TN3270	343	4700	2787	NT74TSO3	NTCP7401	SNX32702	TN3:
	23	9.65.156....	2686	Admin_Action	10/04/09 11:20:55	10/04/09 11:35:11	TN3270	1497	23313	1739	NT74TSO4	NTCP7409	SNX32702	TN3:
	23	9.65.156....	2662	Excessive_Retrans	10/04/09 11:06:03	10/04/09 11:17:26	TN3270	1102	12024	1154		NTCP7407		TN3:
	1093	9.27.132....	1918	Client_Sent_Reset	10/01/09 13:28:54	10/01/09 13:47:57	V420N3	46395	4251	2660				N/A
	1095	9.27.132....	1918	Client_Sent_Reset	10/01/09 13:29:06	10/01/09 13:47:57	CANSNA	70808	55916	6723				N/A

Retransmissions

For Connection Response times
USE
OMEGAMON XE FOR Mainframe Networks

Response Time Variance > 5 msec.

4.75 (2886)

1/10 Seconds

Ports

Next, see the termination reason codes

Connection Termination Reason Codes

SendErr	An error occurred during a send using FRCA(AFPA), possibly because the stack is stopping.
FIN	A persistent socket used by FRCA(AFPA) is closed by a FIN.
Stack_Terminating	The connection is stopping because the stack is stopping.
Last_DVIPA_Term	The last stack that can own the dynamic VIPA bound to the socket is stopping..
Intrusion_Detect	Intrusion detection found the connection to be malicious and closed the connection
ACK_In_LAST_ACK	The acknowledgment that was received is in the lastack state.
NetAccess_Denied	The connection is denied because of a NetAccess rule.
Admin_Action	The connection is stopped because of an administrator action
App_Laddr_Deleted	The connection is stopped because the local IP address bound by the application was deleted
App_Close_NoAccept	The connection stopped - the application closed the socket before performing an accept().
App_Closed	The application using the socket closed the connection using a close().
OrderlyPascalClose	A pascal routine issued an orderly close request.
Pascal_Disconnect	A pascal routine issued a disconnect request.
Pascal_AcceptError	An error occurred during a pascal accept.
Client_Sent_Reset	The connection is stopped because the client sent a reset.
Excessive_Retrans	The connection is closed because the same packet is being retransmitted multiple times.
Window_To_Zero	The connection is closed -TCP window is reduced to zero and window probes not Ack.
Keepalive_ Not_Ackn	The connection is closed because multiple keepalive probes were not acknowledged.
Finwait2_Timeout	The connection is stopped because the stack timed out waiting for a fin in the finwait-2 state.

Connections in 3270
NetView IPSTAT Command
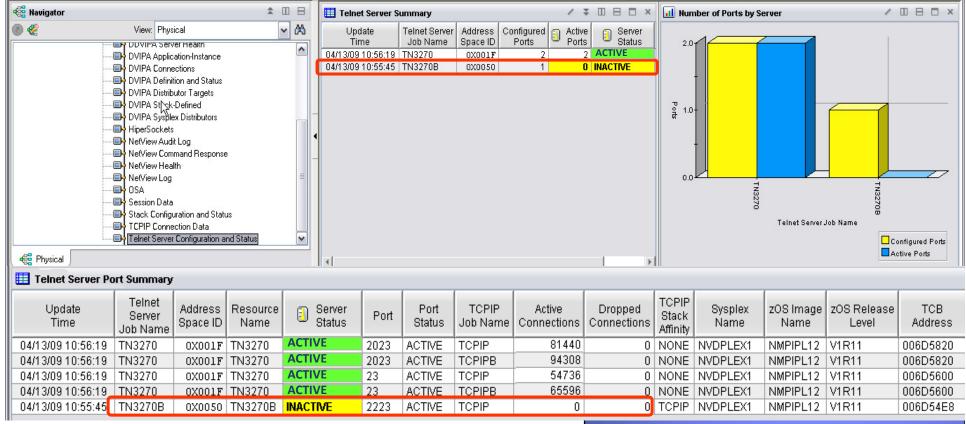
```
FKXK2221            TCP/IP for z/OS Connection Managament
                                      SERVICE
       CLIENT - - - - - - - - - - - - >  POINT - - - - - - - - - - - - >  CONNECTION
                                      TESTMVS                          2076
       9.76.69.165                    9.39.68.148                      23

Client :  IP Address           9.76.69.165                               :
Port   :  Port                 2076               Commands               :
2076   :  Connection ID        00A2C2F3         _  1. Ping                :
34451  :  LU                   TCP00085            2. Tracerte            :
59564  :  APPL                 CNM1908C            3. Drop                :
13225  :  Send                 186145              4. ARP Cache           :
9002   :  Receive              2233                5. SNMP Commands       :
13224  :  Send Window          131070              6. Display Conn        :
13220  :  Conn ResourceName    TN3270              7. Quiesce Port        :
13222  :                                           8. Resume Port         :
13220  :                                           9. Conn Details        :
13221  :                                           10. Connection Status  :
1920   :    F1=Help    F4=LU Cmds    F5=APPL Cmds   F6=Roll    F12=Cancel  :

Command ===>
F1=Help       F2=Main Menu    F3=Return                            F6=Roll
F7=Backward   F8=Forward      F9=Filters                           F12=Cancel
```

Next, Telnet Server status
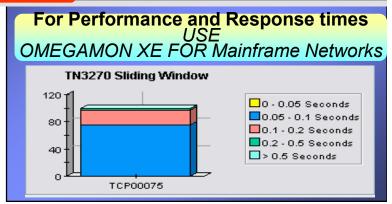
NetView TEP Shows Telnet Server Configuration & Status

Navigator — View: Physical

- DDVIPA Server Health
- DVIPA Application-Instance
- DVIPA Connections
- DVIPA Definition and Status
- DVIPA Distributor Targets
- DVIPA Stack-Defined
- DVIPA Sysplex Distributors
- HiperSockets
- NetView Audit Log
- NetView Command Response
- NetView Health
- NetView Log
- OSA
- Session Data
- Stack Configuration and Status
- TCPIP Connection Data
- Telnet Server Configuration and Status

Physical

Telnet Server Summary

Update Time	Telnet Server Job Name	Address Space ID	Configured Ports	Active Ports	Server Status
04/13/09 10:56:19	TN3270	0X001F	2	2	ACTIVE
04/13/09 10:55:45	TN3270B	0X0050	1	0	INACTIVE

Number of Ports by Server

Ports — Telnet Server Job Name (TN3270, TN3270B)
Legend: Configured Ports, Active Ports

Telnet Server Port Summary

Update Time	Telnet Server Job Name	Address Space ID	Resource Name	Server Status	Port	Port Status	TCPIP Job Name	Active Connections	Dropped Connections	TCPIP Stack Affinity	Sysplex Name	zOS Image Name	zOS Release Level	TCB Address
04/13/09 10:56:19	TN3270	0X001F	TN3270	ACTIVE	2023	ACTIVE	TCPIP	81440	0	NONE	NVDPLEX1	NMPIPL12	V1R11	006D5820
04/13/09 10:56:19	TN3270	0X001F	TN3270	ACTIVE	2023	ACTIVE	TCPIPB	94308	0	NONE	NVDPLEX1	NMPIPL12	V1R11	006D5820
04/13/09 10:56:19	TN3270	0X001F	TN3270	ACTIVE	23	ACTIVE	TCPIP	54736	0	NONE	NVDPLEX1	NMPIPL12	V1R11	006D5600
04/13/09 10:56:19	TN3270	0X001F	TN3270	ACTIVE	23	ACTIVE	TCPIPB	65596	0	NONE	NVDPLEX1	NMPIPL12	V1R11	006D5600
04/13/09 10:55:45	TN3270B	0X0050	TN3270B	INACTIVE	2223	ACTIVE	TCPIP	0	0	TCPIP	NVDPLEX1	NMPIPL12	V1R11	006D54E8

NetView TNPTSTAT Connand

```
BNH497I NUMBER OF TELNET SERVER PORTS: 4
    TN3270   006D TN3270   ACTIVE              2023   ACTIVE
    TN3270   006D TN3270   ACTIVE              2024   ACTIVE
    TN3270   006D TN3270   ACTIVE              22     ACTIVE
    TN3270   006D TN3270   ACTIVE              23     ACTIVE
```

Next, manage network availability

For Performance and Response times
USE
OMEGAMON XE FOR Mainframe Networks

TN3270 Sliding Window
Legend: 0 - 0.05 Seconds, 0.05 - 0.1 Seconds, 0.1 - 0.2 Seconds, 0.2 - 0.5 Seconds, > 0.5 Seconds
TCP00075

TCPIP Availability

```
 1.  Issue Ping
 2.  MVS IP Session Status
 3.  Issue Tracerte Command
 4.  Issue Commands
 5.  SNMP MENU
 6.  IP Server Management
 7.  IP Resource Manager
 8.  SNMP View
 9.  CISCOWorks Blue Inter-network Status Monitor
10.  TCP/IP Trace Control Center. SP: _____
```

▪Issue alert when remote printers are down.

▪Then Network Automation

NetView Availability and Automation with AON

- Issue alert when remote printers are down.

- Then Network Automation

```
FKXK2700              TCP/IP for 390 Resource Management        More: - +
                                                                REFRESH: 0
  Select an AON control file or monitoring command and press ENTER
  1 = ADD/START 2 = DISPLAY/CHANGE   3 = DELETE   4 = START   5 = STOP
                          Resource      TCP/IP       Actmon
          Resource        Type          Stack        Definition    M Status
          -----------     ---------     ---------    ------------  - -------
   _      FTPD1           IPPORT        DEMOMVS                    A NORMAL
   _      IOASNMP         IPPORT        DEMOMVS                    A NORMAL
   _      OPRINTER        IPHOST        DEMOMVS                    R DOWN
   _      OSAF6D0         IPINFC        DEMOMVS                    A NORMAL
   _      OSNMPD          IPPORT        DEMOMVS                    A NORMAL
   _      SMTP            IPPORT        DEMOMVS                    A NORMAL
   _      SNMPQE          IPPORT        DEMOMVS                    A NORMAL
   _      TIMWEB1         IPPORT        DEMOMVS                    A NORMAL
   _      TIVNMIP         IPHOST        DEMOMVS      ALLHOSTS      A NORMAL
   _      TIVSAIOMT       IPHOST        DEMOMVS      ALLHOSTS      A NORMAL
   _      TIVTEPS         IPHOST        DEMOMVS      ALLHOSTS      A NORMAL
   _      TN3270          IPPORT        TN3270S                   A NORMAL


Command ===>
F1=Help        F2=Main Menu    F3=Return    F4=Commands    F5=Refresh    F6=Roll
F7=Backward    F8=Forward      F9=Display Options                        F12=Cancel
```

Next, look at EE and HPR

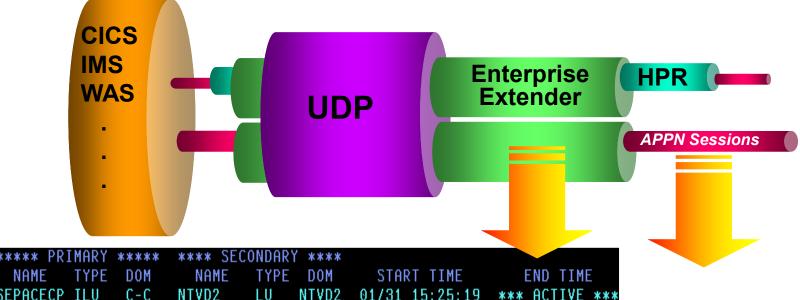# EE formatting from OSA Express Trace

After Formatting with Extended options

```
UDP
  Source Port      : 12001 (EE-Network) Destination Port: 12001 (EE-Network)
  Datagram Length  : 68                 CheckSum: 9C78 662C

MAC Header         : 14                                      Offset:  0
000000 0021A144 2C000014 5E74A954 0800

Ip Header          : 20                 IP: 9.39.68.11, 9.76.69.165 Offset:  E
000000 45C00058 5A540000 40110000 0927440B  094C45A5

Protocol Header    : 8                  Port: 12001, 12001       Offset: 22
000000 2EE12EE1 00449C78

Data               : 60      Data Length: 60                    Offset: 2A
000000 040403C6 0880FF00 00000000 01000BE0  3C040008 00000014 000003D1 03228560
000020 00043FF0 00000000 5C000005 00020200  00000000 4B900104 00060000

Encapsulation      : 1                  Offset: 2A
 LLC: Dsap(I)      : 04 (SNA)           Ssap(C): 04 (SNA)
  Unnumbered(P)    : 03 (UI)
 NLH Anr Route
  Tpf              : Network            Flags: No_Delay
    Type             ANR Label            TP          ER Number       Address
    BNN              80FF0000 00000001  N/A            N/A               0
 Thdr
  TCID             : 00000000 01000BE0
  Reuse_Ct         : 00000000           Index: 0100            Element: 0BE0
  Flag1            : 3C04 (SMSG EMSG STRQ REPLY OPTS)
  Offset           : 32                 Length: 20             Sequence: 977
```

List APPN Sessions that Transverse over EE

CICS
IMS
WAS
.
.
.

UDP

Enterprise Extender

HPR

APPN Sessions

```
***** PRIMARY *****   **** SECONDARY ****
  NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME        END TIME
SEPACECP ILU   C-C    NTVD2    LU   NTVD2  01/31 15:25:19  *** ACTIVE ***
NTVD2    LU    NTVD2  SEPACECP ILU   C-C   01/31 15:25:19  *** ACTIVE ***
NTD2MVS  LU    NTVD2  SEPACECP ILU   C-C   01/31 15:24:11  *** ACTIVE ***
SEPACECP ILU   C-C    NTD2MVS  LU   NTVD2  01/31 15:24:11  *** ACTIVE ***
```
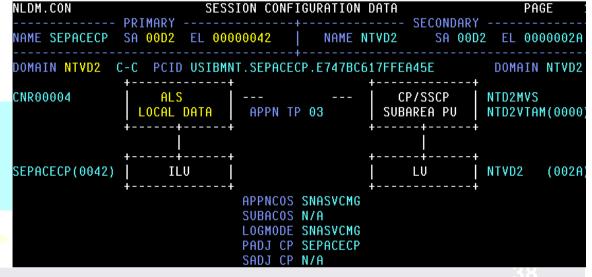
NetView for z/OS
NLDM (Session Monitor)

*NLDM SESS name * ACTREF*

```
NLDM.CON                     SESSION CONFIGURATION DATA                   PAGE
----------------- PRIMARY ----------------+----------- SECONDARY -----------
NAME SEPACECP   SA 00D2   EL 00000042   |   NAME NTVD2      SA 00D2   EL 0000002A

DOMAIN NTVD2   C-C   PCID USIBMNT.SEPACECP.E747BC617FFEA45E              DOMAIN NTVD2

CNR00004        +-----------+    ---           ---    +-----------+    NTD2MVS
                |    ALS    |                          |  CP/SSCP  |    NTD2VTAM(0000)
                | LOCAL DATA|    APPN TP 03            | SUBAREA PU|
                +-----+-----+                          +-----+-----+
                      |                                      |
                +-----+-----+                          +-----+-----+
SEPACECP(0042)  |    ILU    |                          |    LU     |    NTVD2   (002A)
                +-----------+                          +-----------+

                              APPNCOS SNASVCMG
                              SUBACOS N/A
                              LOGMODE SNASVCMG
                              PADJ CP SEPACECP
                              SADJ CP N/A
```

- See sessions that transverse EE connections
- Are sessions going over correct EE?

Next, look at HPR Topology

38

Added with APAR OA16305

HPR Topology in NetView Session Monitor (NLDM)

```
NLDM.AR APPN SESSION ROUTE CONFIGURATION                              PAGE 1
-- PRIMARY ---+-- SECONDARY --+------------- PCID --------------+- DOMAIN -
NAME ECHOA69  | NAME ECHOA29  | NETA.A69M.D2030CADFE6B236A      | CNM99
--------------+---------------+-------------------------------------+----------

  +--------+
  |   CP   |
  |A69M    | SEC-SA: 000F
  +----+---+
TG021 |   HPR-ABCDEF1234567890
  +----+---+
  | CP(ICN) |
  |A99M     |
  +----+----+
IN-TG |
  +----+----+
  | SUBAREA |
  | NODE(S) |
  +---------+
```

HPR indicates a TG that is part of an HPR pipe whose TCID number is shown. VTAM reports path switches and NLDM reflects them in the route.

Next, look at tracing HPR/EE

APPN Trace Formatting in NetView - NLDM

```
NLDM.PIUT                    SESSION TRACE DATA                    PAGE      1
---------- ----- PRIMARY -------------+--------- SECONDARY --------------+- DOM -
NAME NDCMVSA    SA 0010 EL 00000008 | NAME PCOM      SA 0010 EL 00010555 | CNM16
---------------------------------------+---------------------------------------+-------
SEL#    TIME    SEQ# DIR    TYPE    ******** REQ/RESP HEADER ******** RULEN SENS N
( 1) 09:27:22 3E12 P-S LOCATEN   FMH.OC.ER.......BBCB............    105
( 2) 09:27:27 3E13 P-S LOCATEN   FMH.OC.ER.......BBCB............    105
( 3) 09:27:32 3E14 P-S LOCATEN   FMH.OC.ER.......BBCB............    105
( 4) 09:27:37 3E15 P-S LOCATEN   FMH.OC.ER.......BBCB............    105
( 5) 09:27:42 3E16 P-S LOCATEN   FMH.OC.ER...PAC.BBCB............    105
( 6) 09:27:42 0079 S-P (+)RSP    ....OC.NR...PAC...............      3
( 7) 09:27:47 3E17 P-S LOCATEN   FMH.OC.ER.......BBCB............    105




















END OF DATA
ENTER SEL# (RU DETAIL), SEL# AND F (FORMATTED RU), OR COMMAND
CMD==> 1 F
```

New APPN Trace Formatting

NetView TCP/IP Commands Summary

- This is a subset of TCP/IP commands
- Information is also available through TEP NetView workspaces

Command	Descriptions
AON	Panel Driven TCP/IP Management
HIPERSOC	Hipersocket adapter config and status
IFSTAT	TCP/IP stack Interface
IPCMD	Run any IP commands
IPTRACE	Packet and OSA Traces
IPSTAT	IP Connections Status
IPMAN	Resource Manager IP Resource Active Monitoring
DVIPSTAT	DVIPA Definitions and Status
DVIPPLEX	DVIPA Sysplex distributers Information
DVIPHLTH	DVIPA Health
DVIPDDCR	Distributed DVIPA Connection Routing Informatin
DVIPCONN	DVIPA Connections
DVIPALOG	DVIPA Logging
OSAPORT	OSA Channel and Port Config and status
PING	Ping Command
SNMP	SNMP command
STACSTAT	IP Stack Status and config
TNPTSTAT	Telnet Server Config and Status
TRACERTE	Tracerte Command

NetView TCP/IP Management Summary
TEP Interface

IP Commands — **IP Network** — Ping, Tracerte, SNMP Alerting

Config and Status — **OSA-Express** — OSA Trace

Config and Status — **IP Stack** — IP Packet Trace

Config and Status — **DVIPA** — Config and Status

Connection Details Active and Inactive — **TCP/IP Connections** — Connection Details

Config and Status — **Telnet Server** — Config and Status

Performance OMEGAMON MFN — **EE HPR** — OSA IP Trace Format SNA Trace (NLDM)