



Top 10 Tips for z/OS Network Performance Monitoring with OMEGAMON

Session 11899

Tivoli. software

Dean Butler
butlerde@us.ibm.com



Agenda

- Best Practices in Monitoring
- Top 10 tips
- Scenarios

Preface

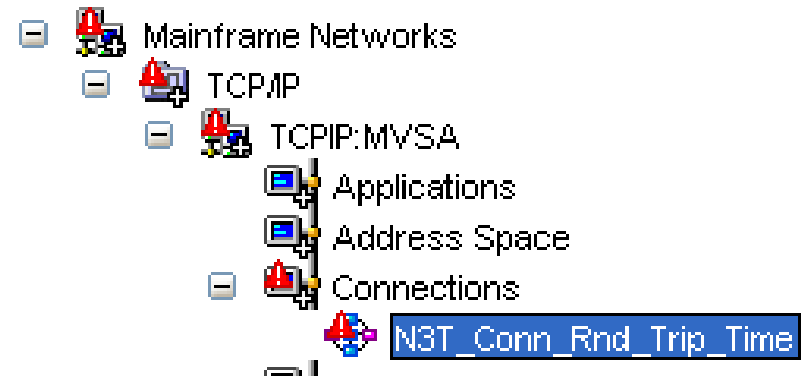
- This presentation highlights best practices from customers who use OMEGAMON XE for Mainframe Network to monitor their z/OS Networking environment
- Features custom Navigator view and workspaces created for customers with customers
 - Available on IBM Service Management Library:
<http://www.ibm.com/software/ismlibrary?NavCode=1TW10OM1K>
 - OMEGAMON Dashboard Edition (DE) is required
 - YouTube: <http://www.youtube.com/watch?v=jVjonG6Zfrw>

Best Practices in Monitoring

- **Proactive** performance and availability monitoring of z/OS, network, applications
- Monitor and collect key performance and availability metrics across entire enterprise (System z and distributed)
- Proactive & predictive alerts (generate events)
- Automated actions on events (issue command or send e-mail notification)
- Enhanced trouble shooting with:
 - Side-by-side real-time and historical data provides rich context for problem identification
 - Historical locking to “stay” in the problem while navigating
- Dynamic thresholding enables thresholds to be customized per resource, date, day of week, etc

Situations

Identify potential problems, generate event, automate actions (e.g. command or e-mail)



View Thresholds

Highlight metrics in a table you are viewing

Response Time	Origin Node	System ID
15.19	TCP/IP: MVSA	MVSA
5.67	TCP/IP: MVSA	MVSA
Response Time GE 5.00		

Create a baseline

- Identify “normal” network profiles for your applications, interfaces, and TCP/IP stacks
- Analogous to blood pressure monitoring
 - At rest = after IPL or early in morning
 - Busiest = most active time of day
 - Quiet time = end of business day
- Start with:

Which application is having a problem?

Collection Time	Application Name	Connection Count	Active Connections	Accepted Connections	Connection Rate	Active Connection High Water Mark	Time stamp for Active Connections High Water Mark
11/1/2010 9:44:55 AM	APP12345	4005	563	15108	3021	1270	10/29/2010 10:29
11/20XX 11:29:40 AM	XYW12345	3024	233	13304	2660	315	11/16/2010 15:49

Performance over time – historical data is important

- Connection Rate
- Concurrent connections
- High water mark
- Byte rate for each

Collection Time	Application Name	Connection Count	Active Connections	Accepted Connections	Connection Rate	Active Connection High Water Mark	Time stamp for Active Connections High Water Mark
11/1/2010 8:44	XXXXXXXXXX	1017	999	129	25	1270	10/29/2010 10:29
11/1/2010 8:59	XXXXXXXXXX	1041	1023	103	20	1270	10/29/2010 10:29
11/1/2010 9:14	XXXXXXXXXX	1068	1050	102	20	1270	10/29/2010 10:29
11/1/2010 9:29	XXXXXXXXXX	1115	1098	108	21	1270	10/29/2010 10:29
11/1/2010 9:44	XXXXXXXXXX	4005	563	15108	3021	1270	10/29/2010 10:29

Create a front end to the Physical Navigator

– Example from one customer

- At-a-glance view of LPAR or TCP/IP status
- Navigate quickly to workspaces

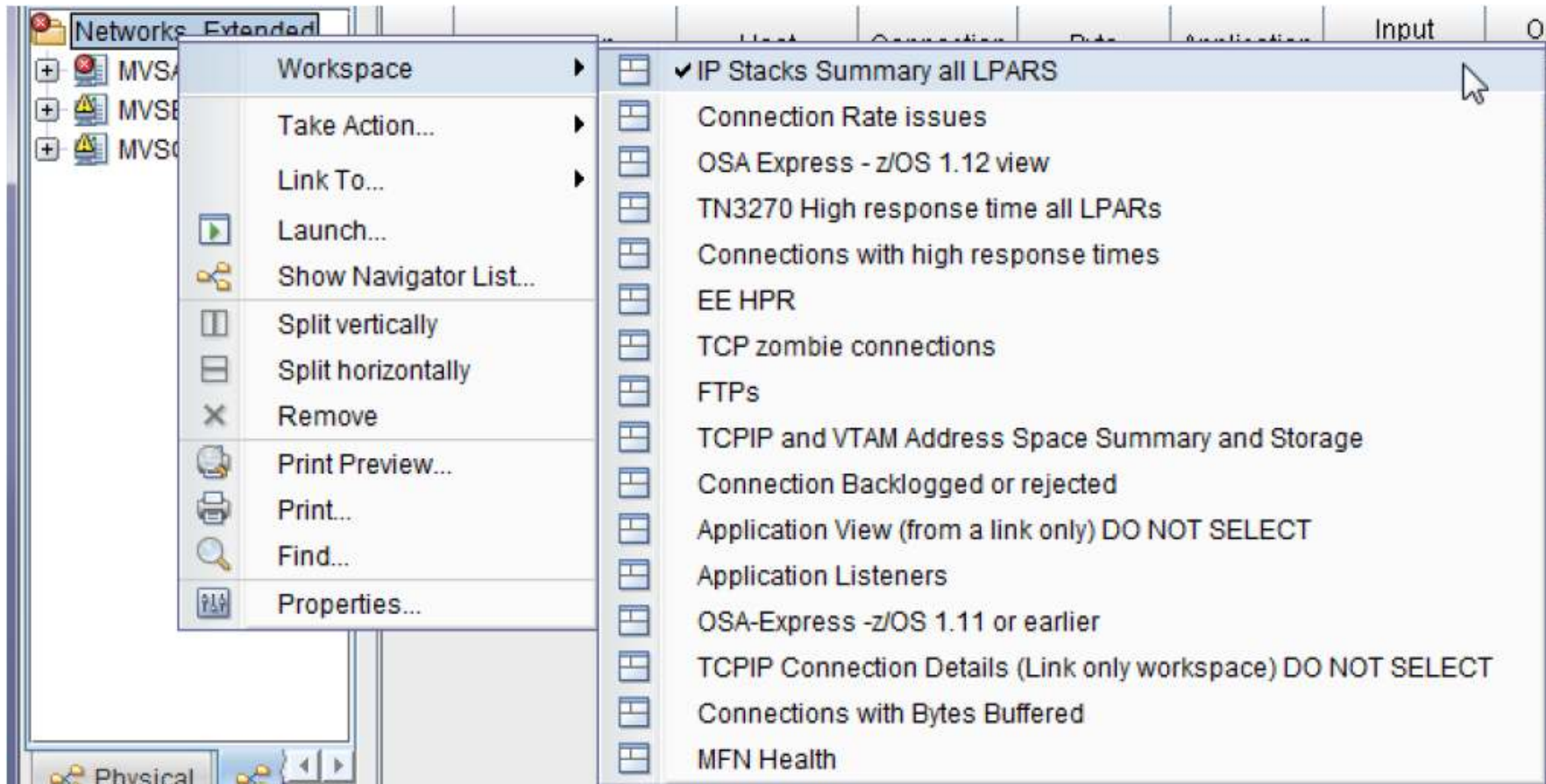
The screenshot displays the Physical Navigator application window. The main pane shows a row of ten green circular nodes representing network components. A context menu is open over the nodes, listing several options:

- TCPIP Address Space
- TCPIP Application Workspace
- TCPIP Connection Workspace
- VTAM Address Space
- VTAM Buffer Summary
- VTAM CSM storage
- VTAM EE Links
- VTAM HPR Links
- Link Wizard...
- Link Anchor...

The interface also includes a 'Situation Event Con' panel on the left with a table for monitoring events, and a 'Notes' panel at the bottom. The right side of the window shows a sidebar with various workspace options.

Add a logical Navigator view

- Download and import Network Extended views and workspaces

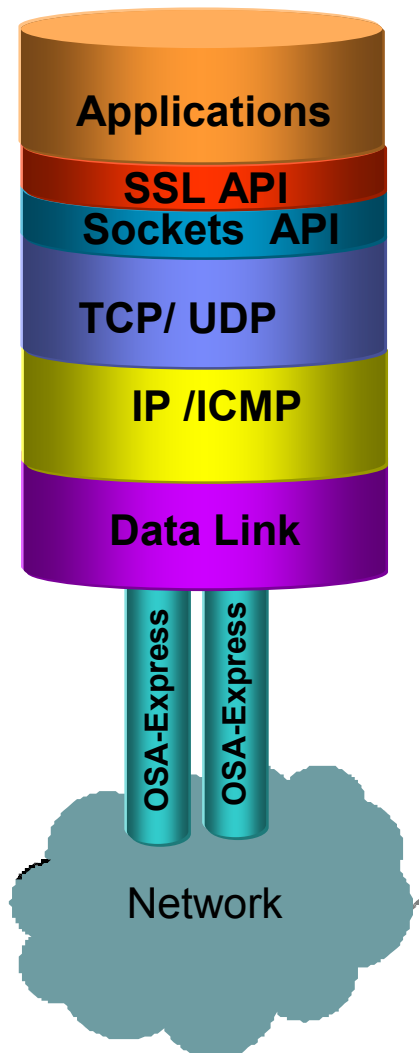


Enable historical data collection

- Choose a set of tables that meet business needs
 - Initially to establish baseline
 - Diagnose intermittent problems
 - Periodically re-assess baseline and business needs
- Add other tables to historical collection when debugging specific problems
- Short term (24 hours) vs. long term (data warehouse)

VTAM Buffer Pools				
VTAM Buffer Pool Extents				
VTAM Buffer Usage by Category				
VTAM Buffer Usage by Address Space				
CSM Storage				
EE Connections				
EE Connections Details				
FTP Sessions	Started	15 minutes	TEMA	Off
TCPIP FTP	Started	15 minutes	TEMA	Off
HPR RTP Connections				
IPSec Status				
VTAM Summary Statistics	Started	15 minutes	TEMA	Off
TCPIP Applications	Started	15 minutes	TEMA	Off
TCPIP Address Space				
OSA-Express Channels	Started	15 minutes	TEMA	Off
TCP Listener				
TCPIP Connections				
TCPIP Details	Startec	5 minutes	TEMA	Off
TCPIP Devices				
TCPIP Gateways				
OSA-Express3 Ports Control	Started	15 minutes	TEMA	Off
OSA-Express3 Ports Errors	Started	15 minutes	TEMA	Off
OSA-Express3 Ports Summary	Started	15 minutes	TEMA	Off
OSA-Express3 Ports Throughput	Started	15 minutes	TEMA	Off
Interfaces	Started	15 minutes	TEMA	Off
OSA-Express LPARS				
TN3270 Server Sess Avail				
OSA-Express Ports				
TCPIP Memory Statistics				
TCPIP Stack Layer	Started	15 minutes	TEMA	Off
OSA 10 Gigabit Ports Control				
OSA 10 Gigabit Ports Errors				
OSA 10 Gigabit Ports Summary				
OSA 10 Gigabit Ports Throughput				
UDP Connections				
VTAM Address Space	Started	15 minutes	TEMA	Off
VTAM SIO				

TCP/IP Key Metrics



Interfaces key metrics

- Status– Is the interface up or down?
- Discards
 - Inbound– indicates possible problem w/ interface, adjacent node, or network
 - Outbound– indicates possible problem w/ interface, IP stack, or application
- Throughput-- uneven distribution across defined interfaces indicates possible problems with path to gateway or lack of network availability

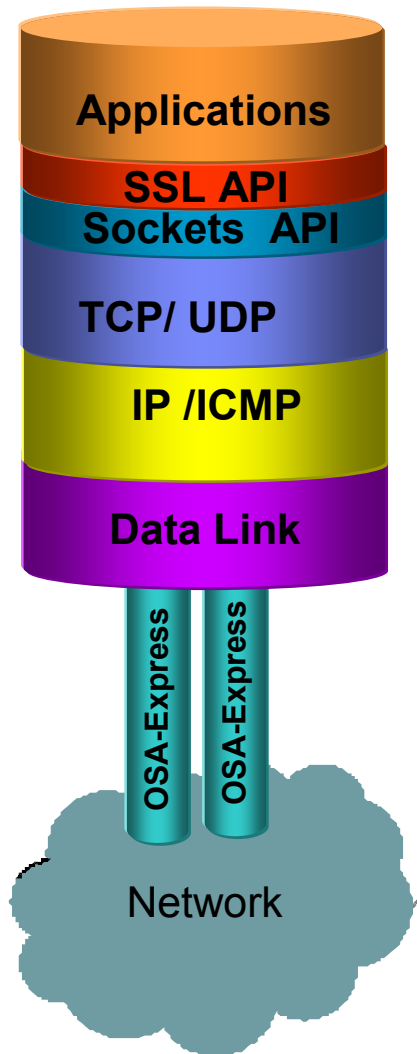
IP key metrics

- Discards
 - Inbound– checksum errors can be caused by problems w/ local interface or problem at adjacent node; security definition problems; routing errors
 - Outbound– security definition problems; routing errors
- Throughput
 - Significant drop for extended time can indicate network problem
 - Significant increase for extended time can indicate application error.
- Fragmentation/Reassembly: frequent fragmentation/reassembly can indicate an application problem or an error in a recent network configuration change

UDP key metrics

- Discards– checksum errors or no port
- Throughput

TCP/IP Key Metrics (cont)

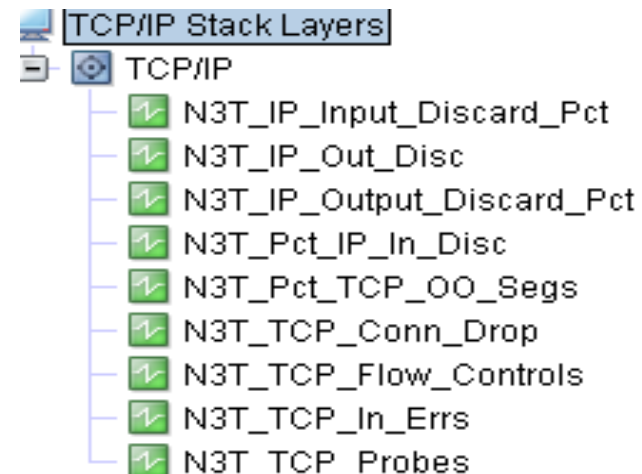
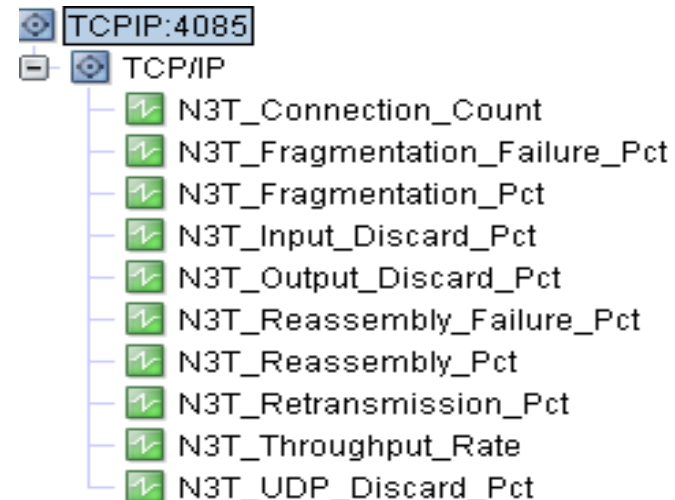
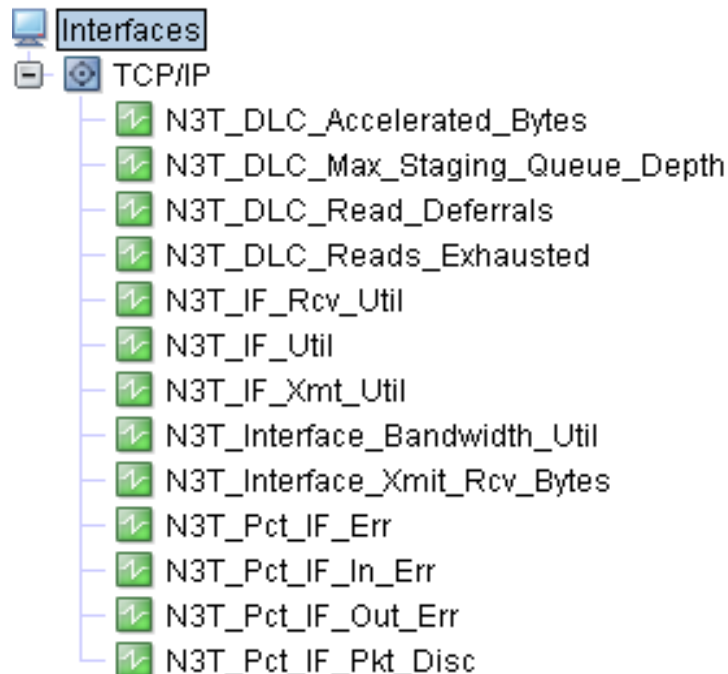


■ TCP key metrics

- Session count– large change from typical value for a significant amount of time can indicate a problem w/ application, OS, or network
- Connections dropped– large number during one or more consecutive intervals can indicate problems w/ application, OS, or network
- Retransmits-- ACKs for data sent not being received
 - Is data being sent successfully and arriving at partner node?
 - Is partner generating ACKs and successfully sending them?
- Duplicate ACKs– Data being sent is not being received by partner
 - Need to figure out whether data is being sent successfully, if so, then where is it being dropped?
- Segment errors received – checksum errors indicate problem w/partner endpoint
- Window probes– large numbers can indicate problem w/remote application
 - Partner has closed window (sent a 0 window) and no data can be sent
 - Window probe requests window be opened so data can be sent
 - If window probe threshold is reached connection is dropped

Monitor key metrics automatically using situations

- Analyze historical data to determine the appropriate situation thresholds for your enterprise





Top 10 Tips

Tivoli. software

OSA Express and Interfaces

The screenshot displays the Tivoli software interface for OSA Express. At the top, a network diagram titled "OSA Interface Topology -- Interface Names and System IDs" shows a central MVSA node connected to MVSB and MVSC nodes, which are in turn connected to several OSA Express interfaces: OSX3400P, OSX3200P, EZ6OSM02, EZ6OSM01, and OSAFBC0L. Below the diagram are three tables:

System ID	Interface Name	Interface Type	Device or Datapath Status	Interface Status	Total Outbound Packets Discarded for No Storage	IP Address Version	Total Inbound Packets Discarded in Error
MVSB	OSAFBC0L	OSA QDIO ethernet OSD	Active	Active	0	IPv4	4
MVSC	OSAFBC0L	OSA QDIO ethernet OSD	Active	Active	0	IPv4	4
MVSA	EZ6OSM01	OSA QDIO ethernet OSM	Active	Active	24	IPv6	32
MVSA	EZ6OSM02	OSA QDIO ethernet OSM	Active	Active	24	IPv6	32
MVSA	OSAFBC0L	OSA QDIO ethernet OSD	Active	Active	0	IPv4	2
MVSA	OSX3200P	OSA QDIO ethernet OSX	Active	Active	0	IPv4	0
MVSA	OSX3400P	OSA QDIO ethernet OSX	Active	Active	0	IPv4	0

System ID	Interface Name	Interface Type	Interface Status	QDIO Accelerator	Frame Invalidation Support	Queue Priority	Q
MVSA	OSX3400P	OSA Q...	Active	No	Yes	4	4
MVSA	OSX3400P	OSA Q...	Active	No	Yes	3	3
MVSA	OSX3400P	OSA Q...	Active	No	Yes	2	2
MVSA	OSX3400P	OSA Q...	Active	No	Yes	1	1
MVSA	OSX3200P	OSA Q...	Active	No	Yes	4	4
MVSA	OSX3200P	OSA Q...	Active	No	Yes	3	3
MVSA	OSX3200P	OSA Q...	Active	No	Yes	2	2

IP Address Version	Device or Datapath Status	Interface Status	Duplicate Address Count	Interface Type	Actual Inbound Performance Type	Actual MTU Value	TCP Segmentation Offload Active
IPv4	Active	Active	0	OSA QDIO ethern...	DYNAMIC	8992	No
IPv4	Active	Active	0	OSA QDIO ethern...	DYNAMIC	8992	No
IPv6	Active	Active	1	OSA QDIO ethern...	BALANCED	1500	No
IPv6	Active	Active	0	OSA QDIO ethern...	BALANCED	1500	No

System ID	Interface Name	Interface Status	QDIO Accelerator	Frame Invalidation Support	Queue Workload Name	Queue ID	Real Interr
MVSB	OSAFBC0L	Active	No	Yes	PRIMARY	1	505,
MVSC	OSAFBC0L	Active	No	Yes	PRIMARY	1	410,
MVSA	OSX3400P	Active	No	Yes	PRIMARY	1	
MVSA	OSX3400P	Active	No	Yes	PRIMARY	1	
MVSA	OSX3400P	Active	No	Yes	PRIMARY	1	4,126
MVSA	OSX3200P	Active	No	Yes	PRIMARY	1	
MVSA	OSX3200P	Active	No	Yes	PRIMARY	1	

- Interfaces**
- Device Inactive
 - High bandwidth Utilization
 - No traffic
 - QDIO is Accelerating Bytes
 - Max Staging queue depth
 - DLC Read deferrals
 - DLC Read Exhausted

- OSA Express**
- High PCI Utilization
 - Channel utilization
 - Missed packets
 - Not Stored Frames

Connection in Backlog or Rejected

Listeners with Connections in Backlog or Rejected

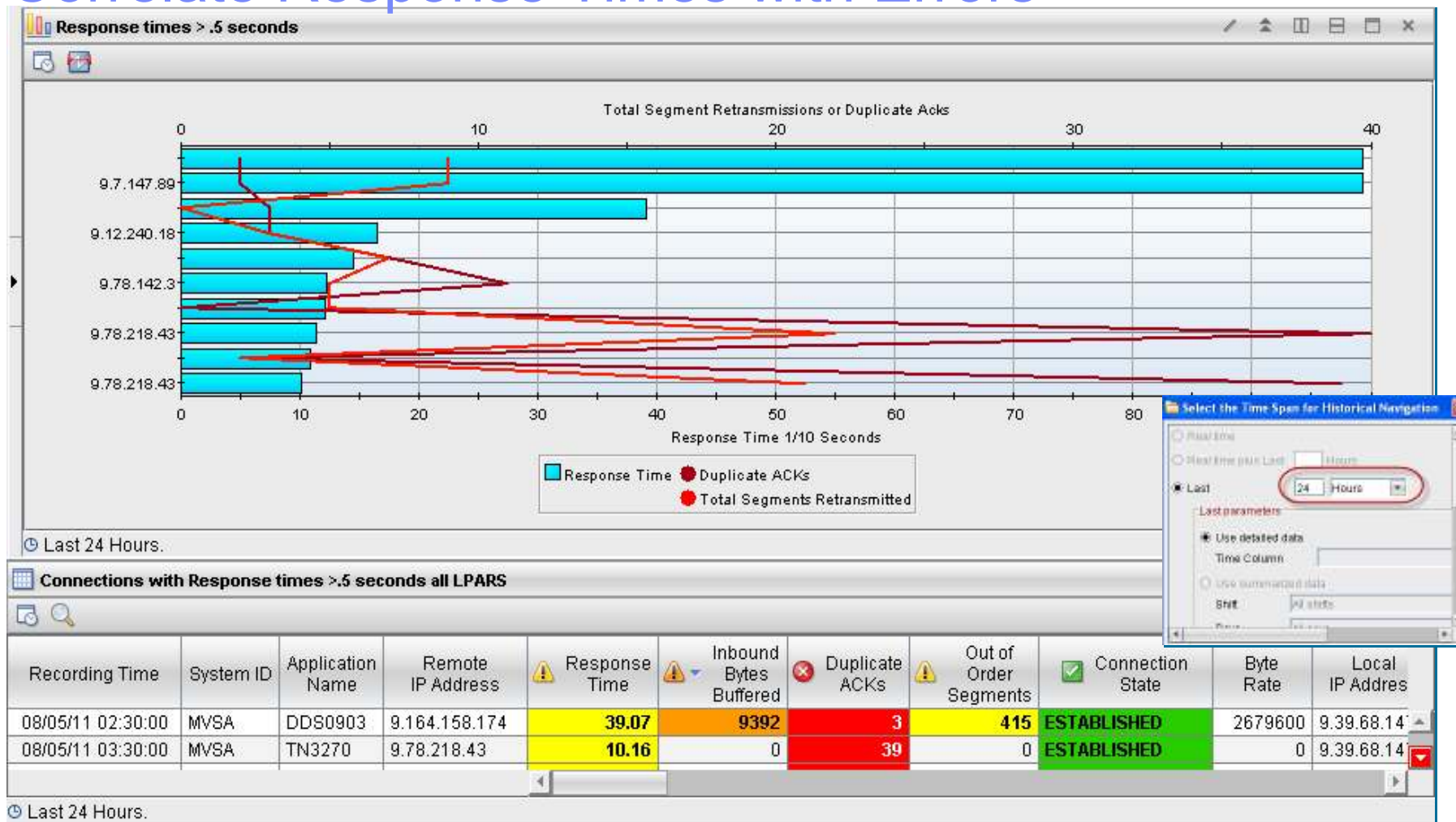
	System ID	Application Name	Local Port	⚠ Connections in Backlog	📄 Backlog Limit	Backlog Connections Rejected	⚠ Total Backlog Connections Rejected	Backlog Connections Rejected Time Stamp
🔗	MVSB	PORTMAP1	111	0	2	0	6	08/18/11 14:54:40
🔗	MVSB	DB2SDIST	5446	5	10	0	0	
🔗	MVSC	PORTMAP1	111	0	2	0	6	08/18/11 14:11:03
🔗	MVSA	CXEGDSST	1920	0	10	0	7	08/20/11 10:05:35
🔗	MVSA	PORTMAP1	111	0	2	0	6	08/18/11 14:35:27
🔗	MVSA	CICPV32	5120	0	1	0	0	08/18/11 14:57:12

Maximum connection requests Queued

Connections Queued Exceeded Backlog Limit

- Increase Backlog Limit (TCPIP profile or in Application)
- Stagger automatic logons, if possible.

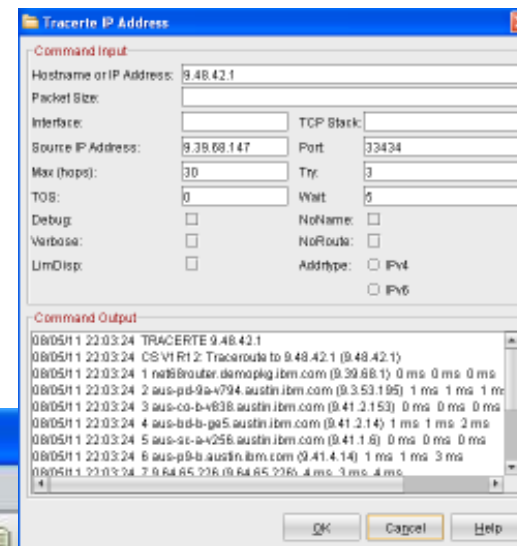
Correlate Response Times with Errors



- See if poor response time correlates with any errors.
- Duplicate ACKs, out of Order Segments, Segments Retransmitted
- Turn on history to see when problems are occurring

Zombie connections

- Connection that do not get dropped
- Connection with no traffic for a long time
- Connection may be hung (not established)



ie connections - XPBASE - Ernie Gilman *ADMIN MODE*

How to issue POPUP commands

Right Click anywhere on a connection and select: DROP PING TRACETE NSLOOKUP or EXPORT

TCP connections with no activity for >10 Mins - all LPARS

System ID	Application Name	Remote IP Address	Remote Port	Local IP Address	Local Port	ASID	Byte	Time Since Last	Connection	Inbound Bytes	Hex Connection
MVSA	BBOS002S	9.39.68.147	9558	9.39.68.147	134		0	11,884.23	CLOSE_WAIT	23	
MVSA	BBOS002S	9.39.68.147	9558	9.39.68.147	183		0	700.34	CLOSE_WAIT	23	
MVSA	BBOS002S	9.39.68.147	9558	9.39.68.147	183		0	700.34	CLOSE_WAIT	23	
MVSA	IBMSMV31	9.65.252.47	2546	9.39.68.147	95		0	17,322.36	ESTABLISHED	0	
MVSA	CXEGI2	9.39.68.147			135		0				
MVSA	1072	9.39.68.147			424		0				
MVSA	ADM9F07C	9.39.68.147			120		0				
MVSA	ADM9E110	9.39.68.147			423		0				

Drop Connection

Ping IP Address

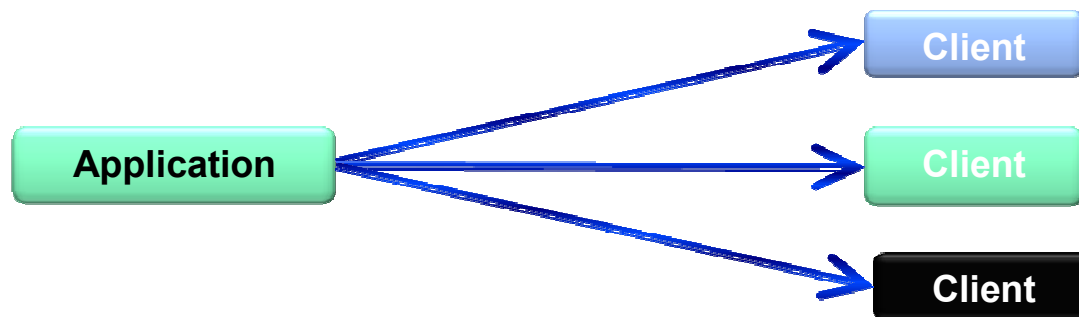
Tracerte IP Address

NSLookup IP Address

Create Application Network Filtered Views

Examples:

- Connect:Direct
- MQ
- CICS
- WebSphere



Address Space

- CPU
- Storage
- Priority

Application Listener

- Connection Rejections
- Backlog limit
- Number of Connections
- Connection Rate

TCP/IP Connections

- Response times
- Buffers queued
- Connection hangs
- Congestion
 - Reset windows
 - Retries,
 - Out of order

Monitoring Connect:Direct

- Status of the Connect:Direct Listeners (Default Ports 1363 & 1364)
- Notice we have bytes backing up for one of them
- Check the dataset response time (MSR)
- Connect:Direct address space CPU utilization with drill down to the current WLM

TCP Listener

Origin Node	Application Name	Local Port	System ID	Collection Time	ASID	Hex Connection Number	Local IP Address	Active Connections	Accepted Connections	Connection Rate	Active Connections High Water Mark	Time Stamp for Active Connections High Water Mark
TCPIP:MVSA	CDCONN	1363	MVSA	01/23/12 08:37:58	0X0033	0X2A2AF92A	9.39.68.147	1	0	0	1	01/18/12 16:41:57
TCPIP:MVSA	CDCONN	1364	MVSA	01/23/12 08:37:58	0X0033	0X2A2AF929	9.39.68.147	1	5	5	1	01/18/12 16:41:57

Active connections

System ID	Application Name	Local IP Address	Remote IP Address	Local Port	Inbound Bytes Buffered	Inbound Queued Data Time Stamp	Hex Connection Number	Byte Rate	Collection Time	Remote Port	ASID	Connection Start Time	Connection Duration
MVSA	CDCONN	9.39.68.147	9.39.68.147	1363	0		0X308BA4AD	34760	01/23/12 08:37:58	7712	0X...	01/23/12 ...	489
MVSA	CDCONN	9.39.68.147	9.39.68.147	1364	4116	01/23/12 08...	0X308DBBEB	2147483647	01/23/12 08:37:58	16481	0X...	01/23/12 ...	9

Connect Direct Datasets

Dataset with Largest Allocation	Percent Used	Highest MSR	Total Datasets
CONDIR.USER.XFER.OUT	99.75	2.1	2

Application Active TCP Connection Topology by Remote IP Address only

z/OS Address Space Utilization

Job Name	Type	SvcClass	SvcClass Period	CPU Percent	TCB Percent	SRE Percent
CDCONN	Batch	BATMED	2	90.4	72.2	18

TN3270 high response time exception view

The screenshot displays the Tivoli Performance Viewer interface. On the left is the Navigator pane showing a tree view of networks, with 'TCPIP: MVSA' selected. The main area is divided into three panes:

- TN3270 Average Response times > .5 Seconds:** A 3D bar chart showing response times in milliseconds. The y-axis lists session IDs: 9.190.179.98, 9.78.218.58, 9.78.208.175, 9.181.255.57, and 9.48.97.122. The x-axis ranges from 0 to 1,200 milliseconds. Each bar is composed of yellow (Average IP Response Time) and cyan (Average SNA Response Time) segments.
- Response times by ...:** A 3D bar chart showing response times in milliseconds. The y-axis lists the same session IDs. The x-axis ranges from 0 to 100 milliseconds. Each bar is composed of yellow, orange, and red segments, corresponding to Bucket 3, Bucket 4, and Bucket 5 respectively.
- TN3270 SESSIONS with response time > .5 seconds:** A table listing session details.

System ID	SNA Application Name	Remote IP Address	Session End	Average Total Response Time	Average IP Response Time	Average SNA Response Time	Average Transaction Count	Response Time Collection Time	Total Transactions Detected
MVSA	ISZSMGR	9.78.218...	<input checked="" type="checkbox"/>	1123	931	192	2	07/26/11 21:25:16	9
MVSA	DDCTSO...	9.78.208...	<input checked="" type="checkbox"/>	861	320	541	0	07/26/11 21:25:33	6
MVSA	DDCTSO...	9.181.25...	<input checked="" type="checkbox"/>	630	471	159	0	07/26/11 21:25:29	10

FTP sessions and transfers

FTP Transfers > 10,000 bytes - Top 10 by duration in last ftp interval

FTP Transfers - Active

Remote IP Address	Local IP Address	Local Port	User ID on Server	User ID on Server Extended	Client User ID	Role	Transmission Start
93.374	9.39.68.147	35399	NETOP2	NETOP2		Server	08/25/11 16:3

FTP session logon errors

System ID	Application Name	Login Failure Reason Description	FTP Type	Remote IP Address	Remote Port
MVSA	FTPD2	Password_not_valid	Server	9.39.66.103	446
MVSA	FTPD8	Password_not_valid	Server	9.39.66.103	344
MVSA	FTPD2	Password_not_valid	Server	9.39.66.103	344

FTP Transfers - Completed at least 10,000 bytes 10 longest

Dataset Name	System ID	TCPIP STC Name	TCP Data Connection ID	Server Logging Session ID
NETOP2.MUSIC.MP3	MVSA	TCPIP	0X097408A7	FTPD106226
NETOP2.MUSIC.MP3	MVSA	TCPIP	0X0971E6F5	FTPD106221
NETOP2.MUSIC.MP3	MVSA	TCPIP	0X09704554	FTPD106215
NETOP2.MUSIC.MP3	MVSA	TCPIP	0X0970241E	FTPD106215

FTP Transfers - Completed in error

Last Reply to Client	Last Reply to Client Description	Transf Dur
226	Closing_data_connection_-_requested_file_action_successful	
226	Closing_data_connection_-_requested_file_action_successful	
451	Requested_action_aborted_-_local_error_in_processing	
451	Requested_action_aborted_-_local_error_in_processing	

Hub Time: Thu, 08/25/2011 04:37 PM | Server Available | FTPs - XPBASE - Ernie Gilman *ADMIN MODE*

EE and HPR

HPR all LPARS

Recording Time	System ID	Remote CP Name	Sessions	ARB Mode	Lock RTP Narr
08/05/11 21:00:00	MVSA	USIBMNR.NDCMVSB	11	Yellow	CNRC
08/05/11 18:00:00	MVSA	USIBMNR.NDCMVSB	11	Yellow	CNRC
08/05/11 19:00:00	MVSA	USIBMNR.NDCMVSB	11	Red	CNRC
08/05/11 18:00:00	MVSA	USIBMNR.NDCMVSC	6	Red	CNRC
08/05/11 20:00:00	MVSA	USIBMNR.NDCMVSB	11	Red	CNRC
08/05/11 19:00:00	MVSA	USIBMNR.NDCMVSC	2	Green	CNRC
08/05/11 19:00:00	MVSA	USIBMNR.NDCMVSB	1	Green	CNRC
08/05/11 19:00:00	MVSA	USIBMNR.NDCMVSB	1	Green	CNRC
08/05/11 20:00:00	MVSA	USIBMNR.NDCMVSC	6	Green	CNRC
08/05/11 20:00:00	MVSA	USIBMNR.NDCMVSC	2	Green	CNRC

Last 4 Hours.

HPR Topology

Total: 4 Selected: 0 Last refreshed: 08/06/11

Enterprise Extender all LPARS

Origin Node	System ID	PU Name	Local IP Address	Remote IP Address	RTP Pipes	Sessions	Packets Retransmitted	Percent of Packets Retransmitted	Packet Retransmission Rate	Transmit Byte Rate	Receive Byte Rate	Bytes Sent	Bytes Received
VTAM: MVSA	MVSA	EX000012	9.39.68.12	9.65.189.66	1	2	0	0	0	33	33	33	33

TCP/IP and VTAM address spaces and storage

TCPIP Address Space all LPARS

System ID	Host IP Address	zOS Release	CPU Percentage	Paging Rate	CSA Usage Below 16MB	CSA Percent Below 16MB	Total CSA Usage	Total CSA Percentage	Connection Count	Byte Rate	Application Count
MVSB	9.39.68.146	zOS_1.12	0	0	136	0	26032	0	53	67999	15
MVSC	9.39.68.145	zOS_1.12	0	0	136	0	26032	0	73	118353	15
MVSA	9.39.68.147	zOS_1.12	0	0	136	0	34392	0	587	1299346	121

TCPIP Memory Statistics all LPARS

System ID	IP Address	ECSA Storage In Use	ECSA Storage Free	Percent ECSA Storage In Use	Authorized Private Storage In Use	Authorized Private Storage Free	Percent Authorized Private Storage In Use	64bit Common Storage In Use	64bit Common Storage Free
MVSB	9.39.68.146	3,071,680	0	100	8,917,608	9,456	100	151,120	897,...
MVSC	9.39.68.145	3,070,848	0	100	9,040,392	9,808	100	157,504	891,...
MVSA	9.39.68.147	6,361,080	61,608	99	11,197,544	24,208	100	333,568	715,...

VTAM Address Space all LPARS

System ID	CPU Percentage	Paging Rate	CSA Below	CSA Percent	CSA	CSA Percentage	DASD SIO Per Sec	NCP SIO Per Sec	CTC SIO Per Sec	Local SNA SIO Per Sec	Local Non-SNA SIO Per Sec	Other SIO Per Sec	SIO Rate Pct of System
MVSC	0				9228	2	0	0	0	0	0	0	0
MVSA	0	0	84541	2	10213686	3	0	0	0	0	0	0	0

CSM Storage Statistics all LPARS

System ID	Percent ECSA In Use Storage	Percent ECSA Allocated Storage	Storage In Use Across ECSA Pools	Storage Free Across ECSA Pools	Storage Allocated Across ECSA Pools	Maximum ECSA Storage Allowed	Storage In Use Across DSP Pools	Storage Free Across DSP Pools	Storage Allocated Across DSP Pools	Storage In Use Across Pools
MVSC	0	2	248	1800	2383	122880	5208	1616	6824	5456
MVSA	1	3	812	2340	4160	122880	23008	5648	28656	23820

OMEGAMON XE for Mainframe Networks Agent Health

Displays status information about the agents running on your z/OS LPARs.

Display this view after installing OMEGAMON XE for Mainframe Networks to ensure that the monitoring agent is running, configured properly and connected to TEMS/TEPS.

Check the agent health view if data is not being displayed. Verify agent configuration settings, network connection, etc.

The screenshot displays the MFN Health - XPBASE - Ernie Gilman *ADMIN MODE* interface. It features three main data tables:

- MFN Agent Status - All LPARS:** A table with columns for System ID, Origin Node, TCP Collection Start Time, TCP Collection Interval, TCP Collector SNMP Parameter Dataset Name, PAGENT Daemon Started, IKE Daemon Started, SNA Collection Started, SNA Collection Start Time, SNA Collection Interval, Virtual IO Unit Name, and Sysplex Name. It lists agents MVSB, MVSC, and MVSA.
- MFN SNA Collector Status - All LPARS:** A table with columns for Origin Node, Agent VTAM Major Node Name, Agent VTAM Major Node Status, Agent VTAM Application Name, Agent VTAM Application Status, PMI Exit Name, PMI Exit Status, SNA NMI Enabled, EE And HPR Collection, ALL HPR Collection, CSM Buffer Reporting Collection, Buffer Pool And VTAM Environment Collection, and Sysplex Name. It lists agents for MVSB, MVSC, and MVSA.
- MFN TCP Collector Status - All LPARS:** A table with columns for Origin Node, Agent name, SNMP Agent Port, SNMP Version, SMF Service Enabled, IPv4 Security Enabled, IPv6 Security Enabled, Connections And Applications Collection, IP Security Collection, OSA Statistics Collection, Stack Layer Statistics Collection, Interface Statistics Collection, Data Link Control Statistics Collection, Routing Table Collection, Routing Table Collection Frequency, and TN3270 Server Collection. It lists agents for MVSB, MVSC, and MVSA.

The status bars at the bottom indicate: Hub Time: Sun, 08/21/2011 02:42 PM, Server Available, and MFN Health - XPBASE - Ernie Gilman *ADMIN MODE*.



Scenarios

Tivoli. software

Scenario A: Scheduled logons and “silent” failures

The setting:

A mainframe network systems programmer was building a baseline for network performance of his LPARs and applications. A very high number of rejected connections were being reported by OMEGAMON XE for Mainframe Networks just after 10 pm each evening. At first, the systems programmer thought he had found a problem with the monitoring software.

Scheduled logons and “silent” failures

1. Johann, the network systems programmer, enabled a situation that e-mails him when backlog connections are rejected.

	System ID	Application Name	Local Port	Connections in Backlog	Backlog Limit	Backlog Connections Rejected	Total Backlog Connections Rejected	Backlog Connections Rejected Time Stamp
	MVSB	PORTMAP1	111	0	2	0	6	08/18/11 14:54:40
	MVSB	DB2SDIST	5446	5	10	0	0	
	MVSC	PORTMAP1	111	0	2	0	6	08/18/11 14:11:03
	MVSA	CXEGDSST	1920	0	10	0	7	08/20/11 10:05:35
	MVSA	PORTMAP1	111	0	2	0	6	08/18/11 14:35:27
	MVSA	CXEGDSST	5446	0	10	0	7	08/18/11 14:57:12

2. The e-mails confirmed that thousands of connection requests were being rejected before the FTP server was able to accept.

BacklogConnsRejected - The number of rejected backlog connections for FTPD1 on SYSXX is **6,842**: 11/16/09 22:07EST.

BacklogConnsRejected - The number of rejected backlog connections for FTPD1 on SYSXX is **8,045**: 11/17/09 22:06EST.

Scheduled logons and “silent” failures ...

3. The backlog limit for the FTP server is 50, which is reasonable for expected activity

Active Connections	Accepted Connections	Connection Rate	Active Connections High Water Mark	Time Stamp for Active Connections High Water Mark	Idle Time Since Last Accept	Server Up Time	Connections in Backlog	Backlog Connections Rejected	Backlog Connections Rejected Time Stamp	Backlog Limit
0	1	0	1	15:11:41	0:01	871.02	0	0	01:05:00	50

4. After looking at a packet trace on the listener port and consulting with a project manager, Johann determined that an application timer on 10000+ workstations triggered an FTP logon at 10 pm. The timer was adjusted to prevent the bursts.

```

Session B - [24 x 80]
File Edit View Communication Actions Window Help
-----
CNMKWIND OUTPUT FROM FMTPACKT FULL TCPNAME=TCPIP2 ASCII RAD LINE 177 OF 2392
BNH773I NUMBER OF PACKETS: 66 , MISSED BUFFERS: 0 , TCPNAME: TCPIP2
-----
6 TVT2002 PACKET 00000004 14:59:50.235842 Packet Trace
To Interface : TCPIPLINK Device: CTC Full=112
Tod Clock : 2005/02/02 14:59:50.235842
Sequence # : 0 Flags: Pkt Out
IpHeader: Version : 4 Header Length: 20
Tos : 00 QOS: Routine Normal Service
Packet Length : 112 ID Number: 2880
Fragment : Offset: 0
TTL : 64 Protocol: TCP CheckSum: 09E5 F
FFF
Source : 9.42.45.131
Destination : 9.42.8.77

TCP
Source Port : 21 (ftp) Destination Port: 1732 ()
Sequence Number : 677336339 Ack Number: 2213976836
Header Length : 32 Flags: Ack Psh
Window Size : 32768 CheckSum: EFFF FFFF Urgent Data Pointer:
0000
BNH183I CURRENT SCROLL VALUE IS 1
CMD=>
MA b 24/009
Connected to remote server/host tivvm2.raleigh.ibm.com using port 23
ustpl7a 2B13/02/510 on ustpl7a

```

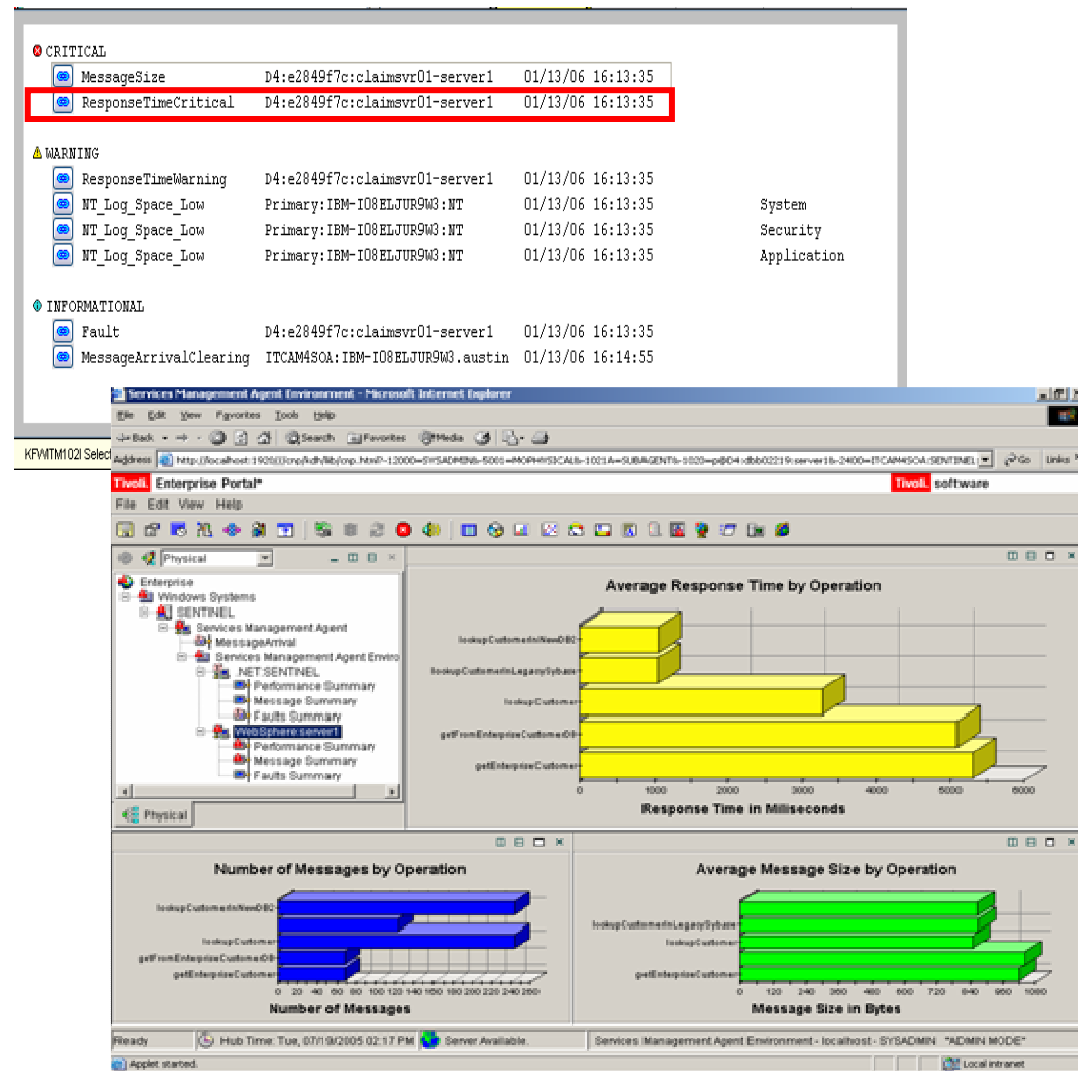
Scenario B: Slow response time in web service

The setting:

A company recently deployed a set of web services that replaced a very high profile application. The operations team monitors the performance closely. When performance degrades, its time to investigate...

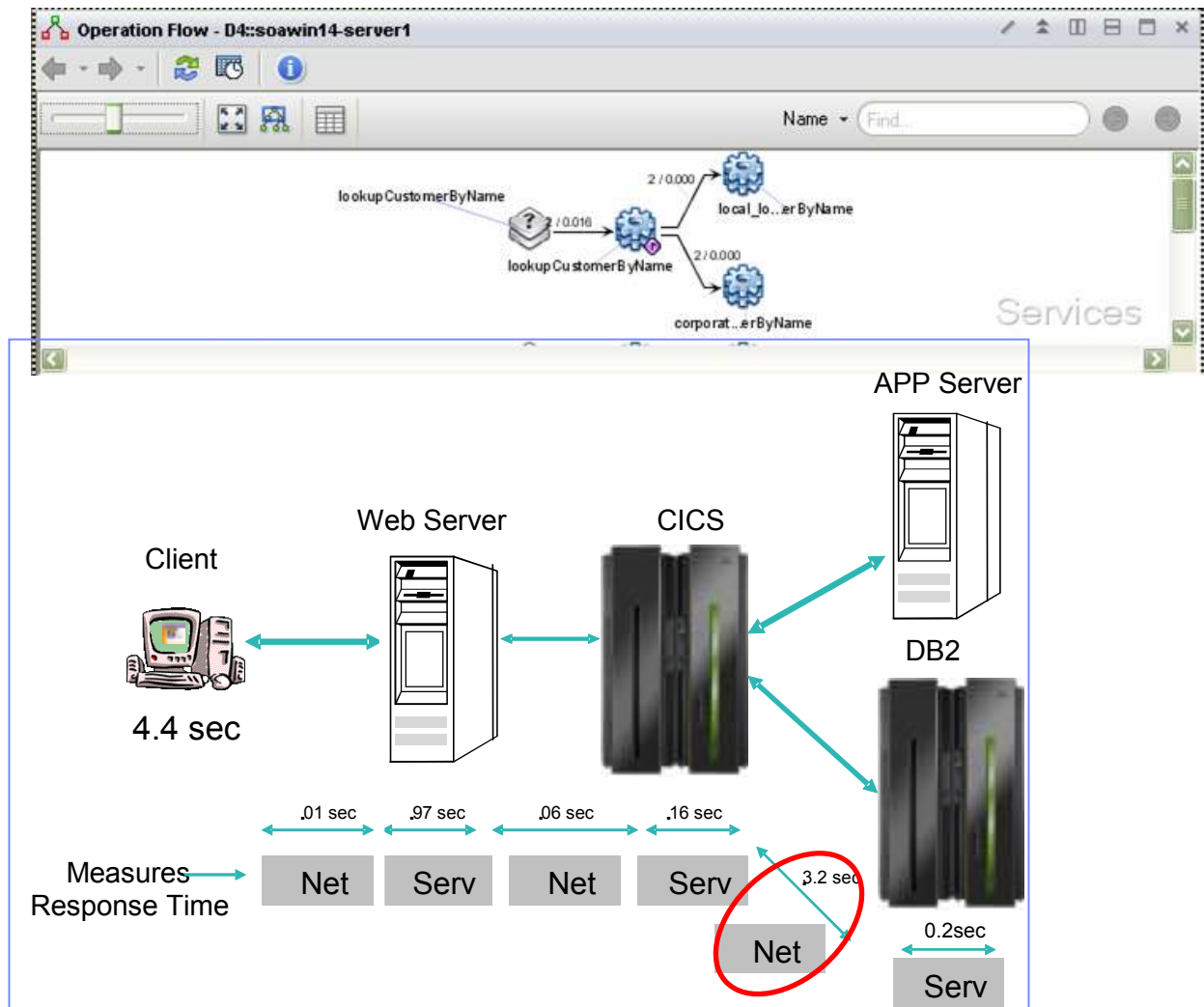
Slow response time in web service ...

1. An alert identifies a response time problem. Annette, an operator, determines that slow response times are being recorded for the new web services.
2. Annette checks the number of requests and the message size and determines this is a normal volume of traffic. Annette passes the issue to Johann, a SME.



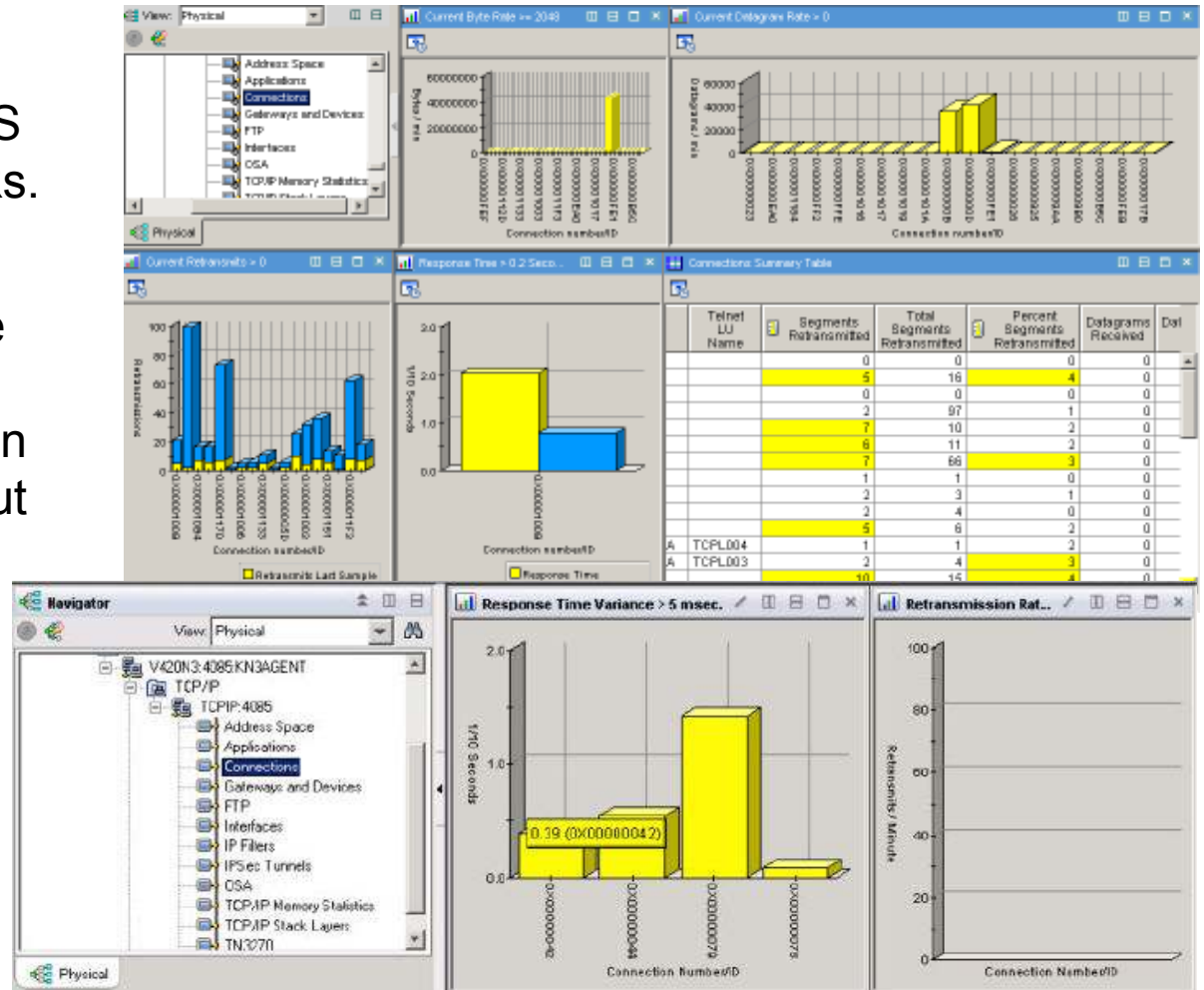
Slow response time in web service ...

3. Johann begins by looking closer at the web services. Identifies flows and response time for each step.
4. Problem appears to be with the network between the CICS and DB2 servers. These two LPARs are connected by a data center network.



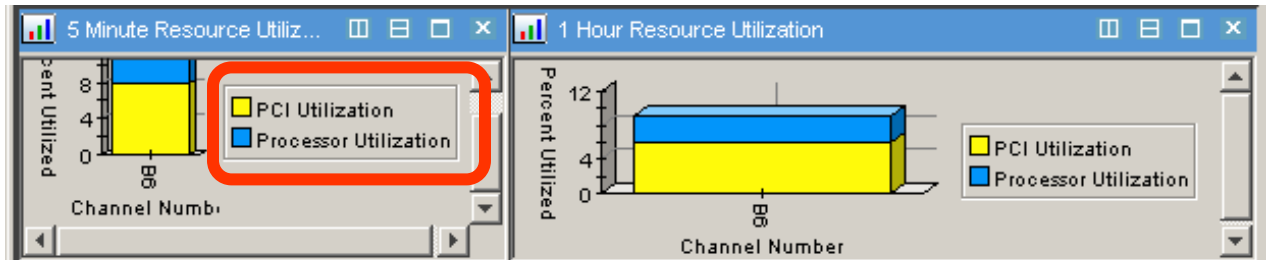
Slow response time in web service ...

5. Johann views metrics for connections between CICS and DB2 on the two LPARs.
6. Johann notices there have been retransmits and out-of-order segments between CICS and DB2 servers. But what is the root cause?



Slow response time in web service ...

7. Johann checks the OSA cards and discovers the OSA on the DB2 server has high PCI and processor utilization.



8. Further checks reveal contention on OSA with other LPARs in the CEC is causing the performance issues.

Device Name	Channel Number	Channel Type	Micro Code Level	Subtype	Mode	State	Share Indicator	Port Count
OSA1	B6	OSADirectExpress	0X0630	97			Shared	1

Collection Time	Port Name	Link Name	Port Type	Hardware State	Disabled Status	Service Mode	Configuration Name	Configuration Speed
12/16/08 13:34:34	OSAA	TCPIPLIN	oneThousandBaseTEthernet	enabled	0X0000	NetInServiceMode	IBM Default ConfigFile	1000Base T oneThousandMbFullDuplex

Each OSA is dedicated to an LPAR, but also serves as backup OSA for a 2nd LPAR. Switch other LPAR to its primary OSA.

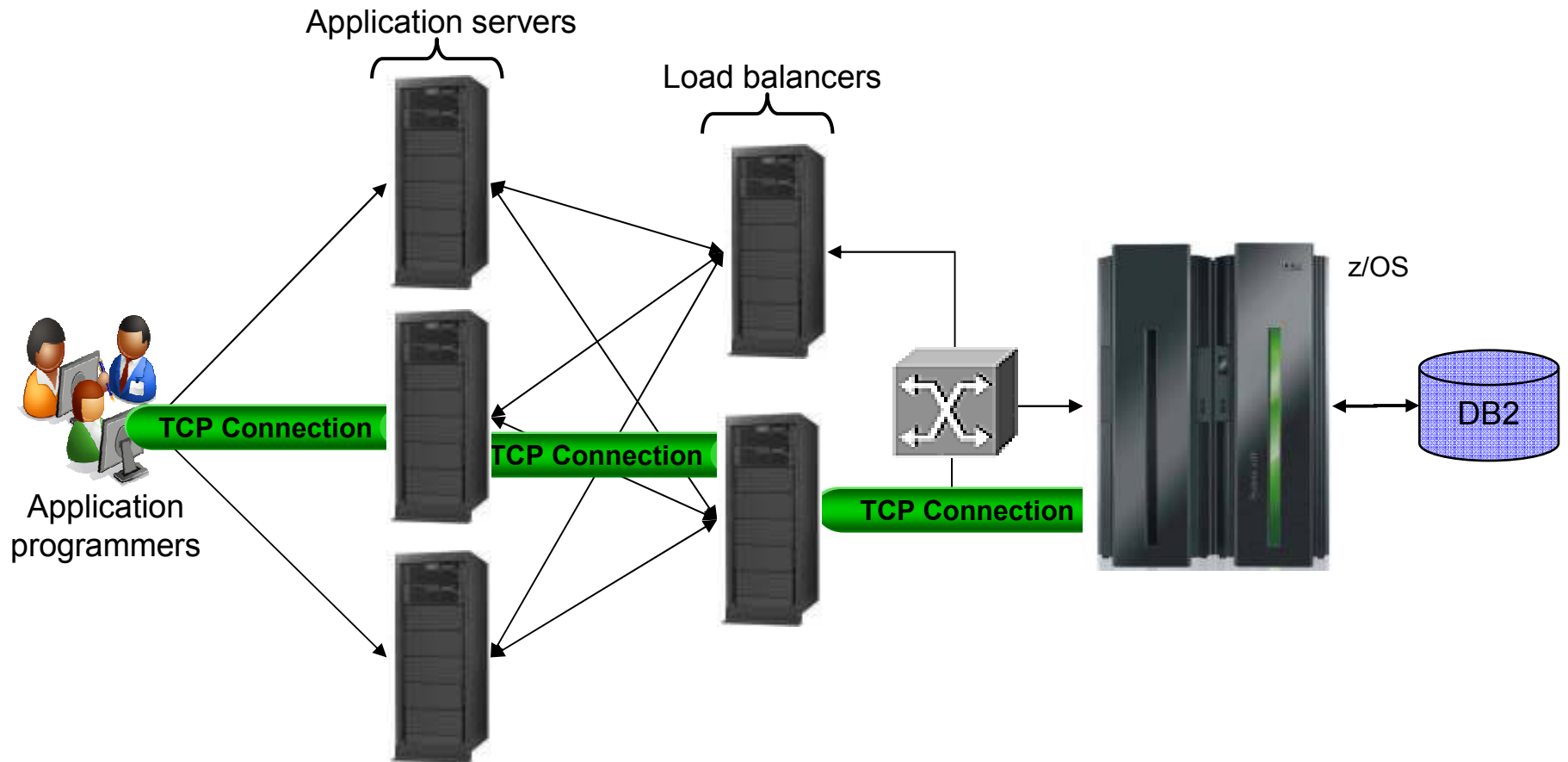
Collection Time	LPAR Name	LPAR Logical Channel Subsystem	LPAR Number	LPAR Status	Processor Utilization Per Minute	Kilobyte Rate In Per Minute	Kilobyte Rate Out Per Minute	Processor Utilization Per Five Minutes	Kilobyte Rate In Per Five Minutes	Kilobyte Rate Out Per Five Minutes	Processor Utilization Per Hour
12/16/08 13:14:27		0	1	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		1	1	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		0	2	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		1	2	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		0	3	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		1	3	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		0	4	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		1	4	unknown	0	0	0	0	0	0	0
12/16/08 13:14:27		0	5	unknown	0	0	0	0	0	0	0

Scenario C: DB2 is working, it must be the network

The setting:

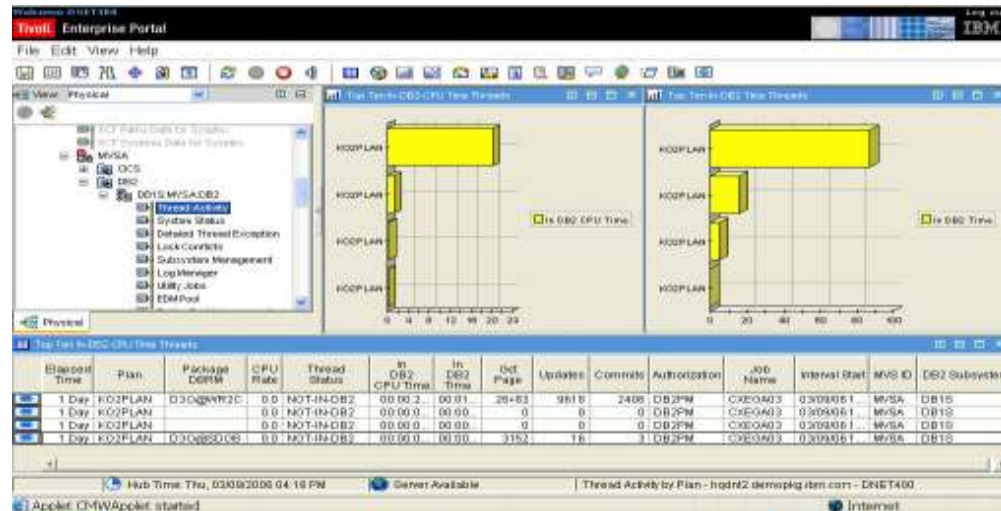
A multi-tier application framework is being used by a team of programmers to develop a Java application. The application is stored as large binary objects (BLOBs) in a DB2 on z/OS database. Each programmer retrieves, changes, and then saves a BLOB. Long delays that occur sporadically during the save are frustrating the application team.

DB2 is working, it must be the network ...



DB2 is working, it must be the network ...

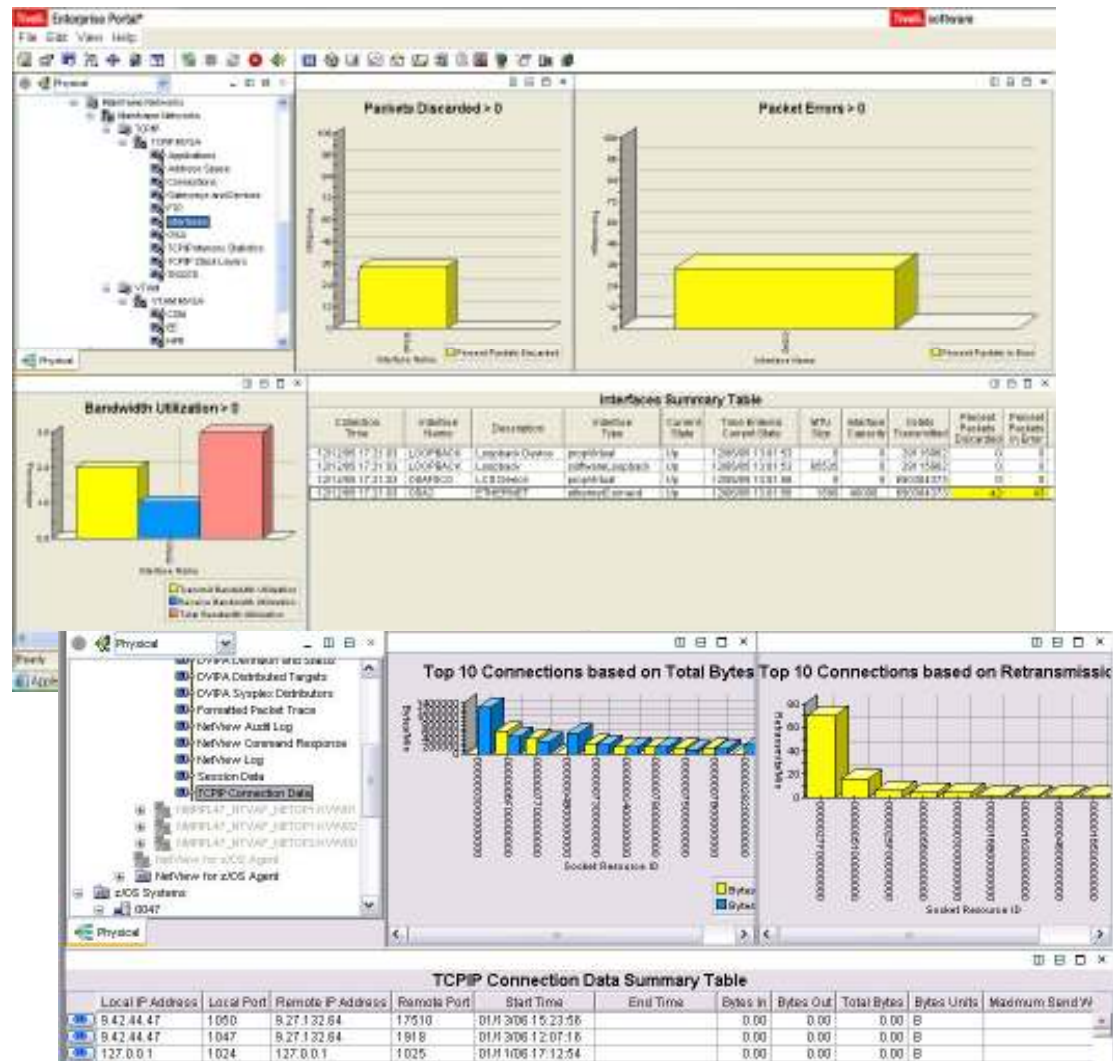
1. Facing revolt from his team, the team leader asks the DB2 systems programmer to check for performance problems.
2. The DB2 systems programmer checks thread CPU time, lock contention, and query plan, among other things. He determines that DB2 is not the cause of the slowdown.



DB2 is working, it must be the network ...

3. Expecting that the problem may be due to an underlying network problem, the team leader turns to Johann for help.

4. Johann views the DB2 application and associated connections. Large amounts of data is being transferred over the DB2 connections with no retransmits or out of order segments.

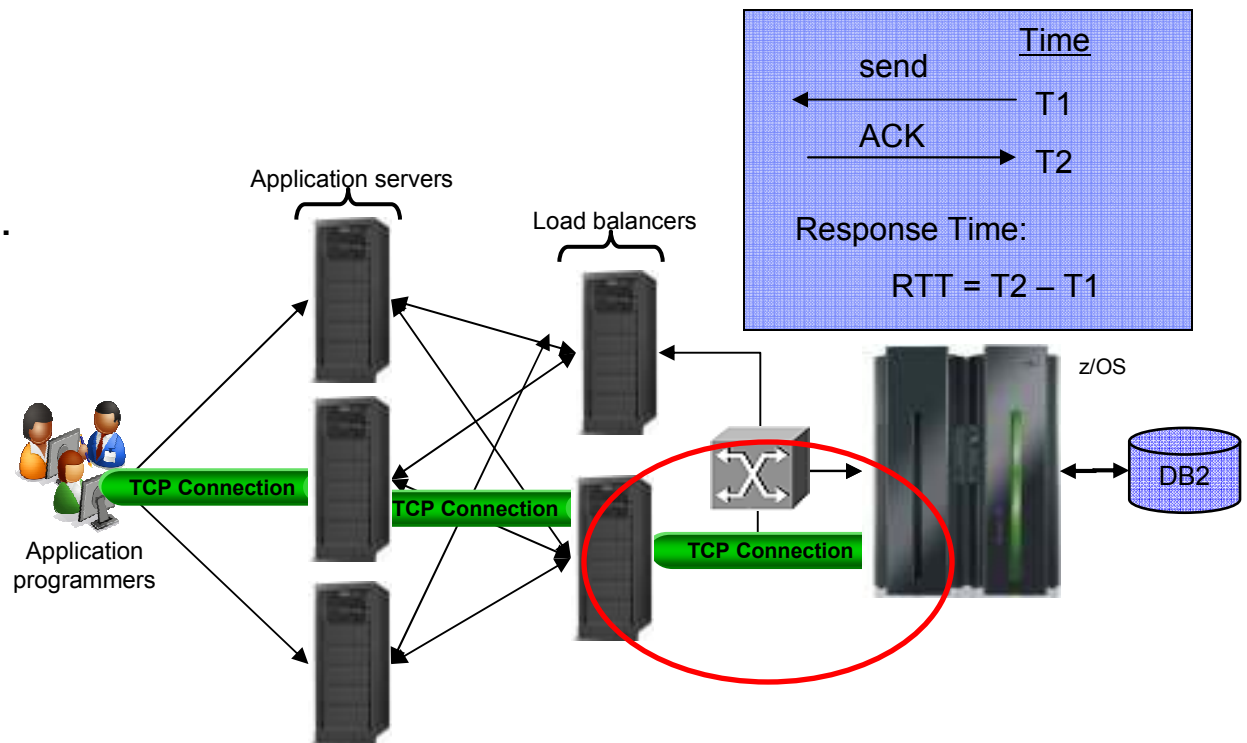


DB2 is working, it must be the network ...

5. Interesting... Response time and response time variance are higher than expected (0.5+ sec, 0.5+). Also, much more data is being sent from DB2 than received from the remote system.

Why is ACK from remote system taking so long?

6. Worked with distributed network and application server SMEs to identify and resolve.



Tivoli System z Sessions at SHARE

Monday

11:00	11207: Automating your IMSplex with System Automation for z/OS	Platinum 7
1:30	11832: What's New with Tivoli System Automation for z/OS	Elite 1
1:30	11896: Problem Solving with Consolidated Logs	Grand Salon A
3:00	11886: Improve Service Levels with Enhanced Data Analysis	Elite 1

Tuesday

9:30	11792: What's New with System z Monitoring with OMEGAMON	Elite 1
11:00	11791: Tuning Tips To Lower Costs with OMEGAMON Monitoring	Platinum 8
1:30	11900: Understanding Impact of Network on z/OS Performance	Grand Salon A

Wednesday

9:30	11835: Automated Shutdowns using either SA for z/OS or GDPS	Elite 1
1:30	11479: Predictive Analytics and IT Service Management	Grand Salon E/F
1:30	11899: Top 10 Tips for Network Perf. Monitoring w/ OMEGAMON	Platinum 9
4:30	11836: Save z/OS Software License Costs with TADz	Elite 1

Thursday

8:00	11887: Learn How To Implement Cloud on System z	Grand Salon E/F
9:30	11905: Using NetView for z/OS for Enterprise-Wide Mgmt and Auto	Grand Salon A
11:00	11909: Get up and running with NetView IP Management	Grand Salon A

Friday

38 9:30	11630: Getting Started with URM APIs for Monitoring & Discovery	Elite 1
---------	---	---------

Session 11899

Top 10 Tips for z/OS Network Performance Monitoring with OMEGAMON

