NetView for z/OS: IP Management Topics and Solutions

Session 17739

Pam McLean (pamm@us.ibm.com)
NetView for z/OS - IBM z Systems Service Management

#SHAREorg

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

Acknowledgements, Disclaimers and Trademarks

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

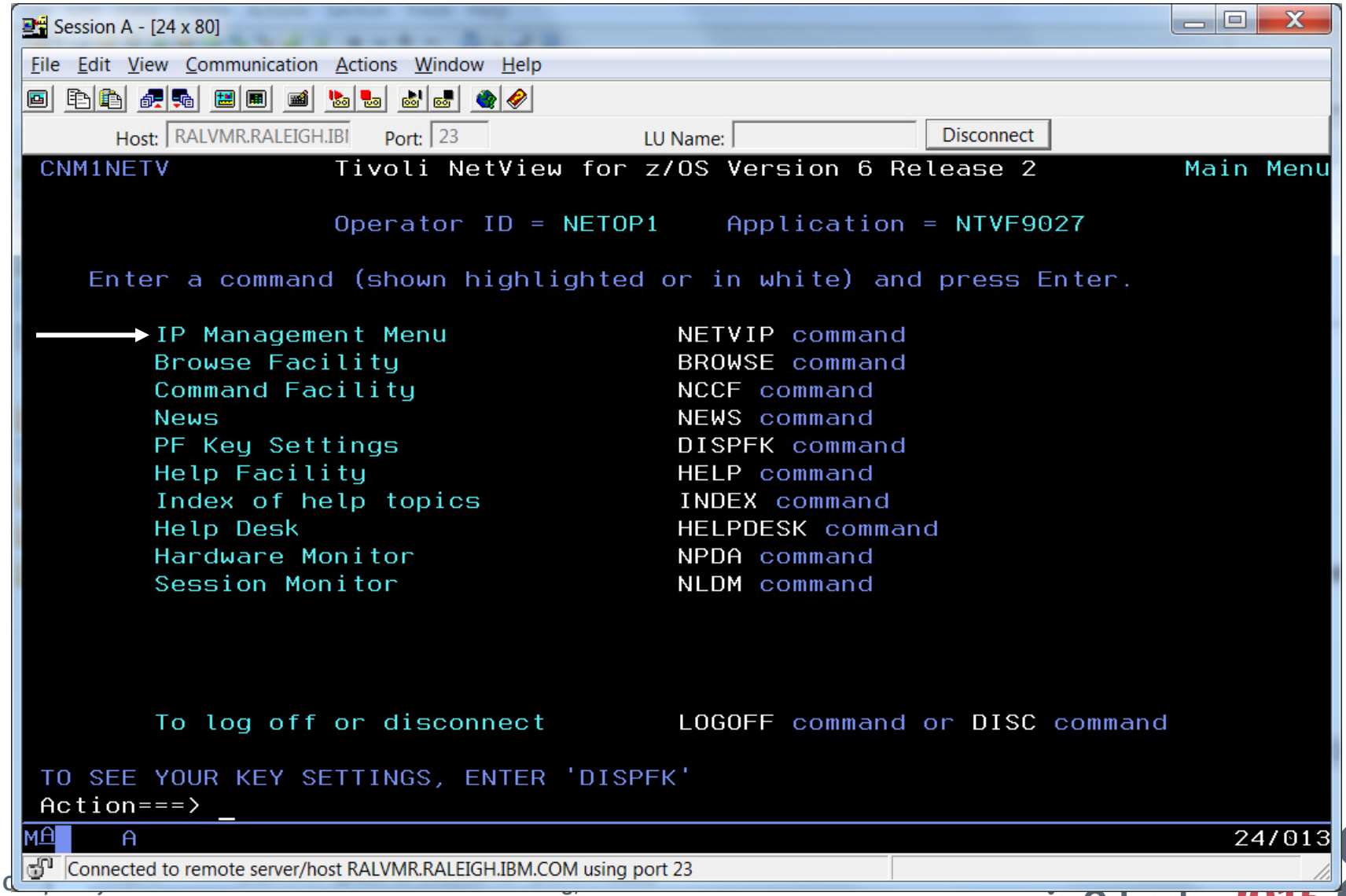
IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Agenda

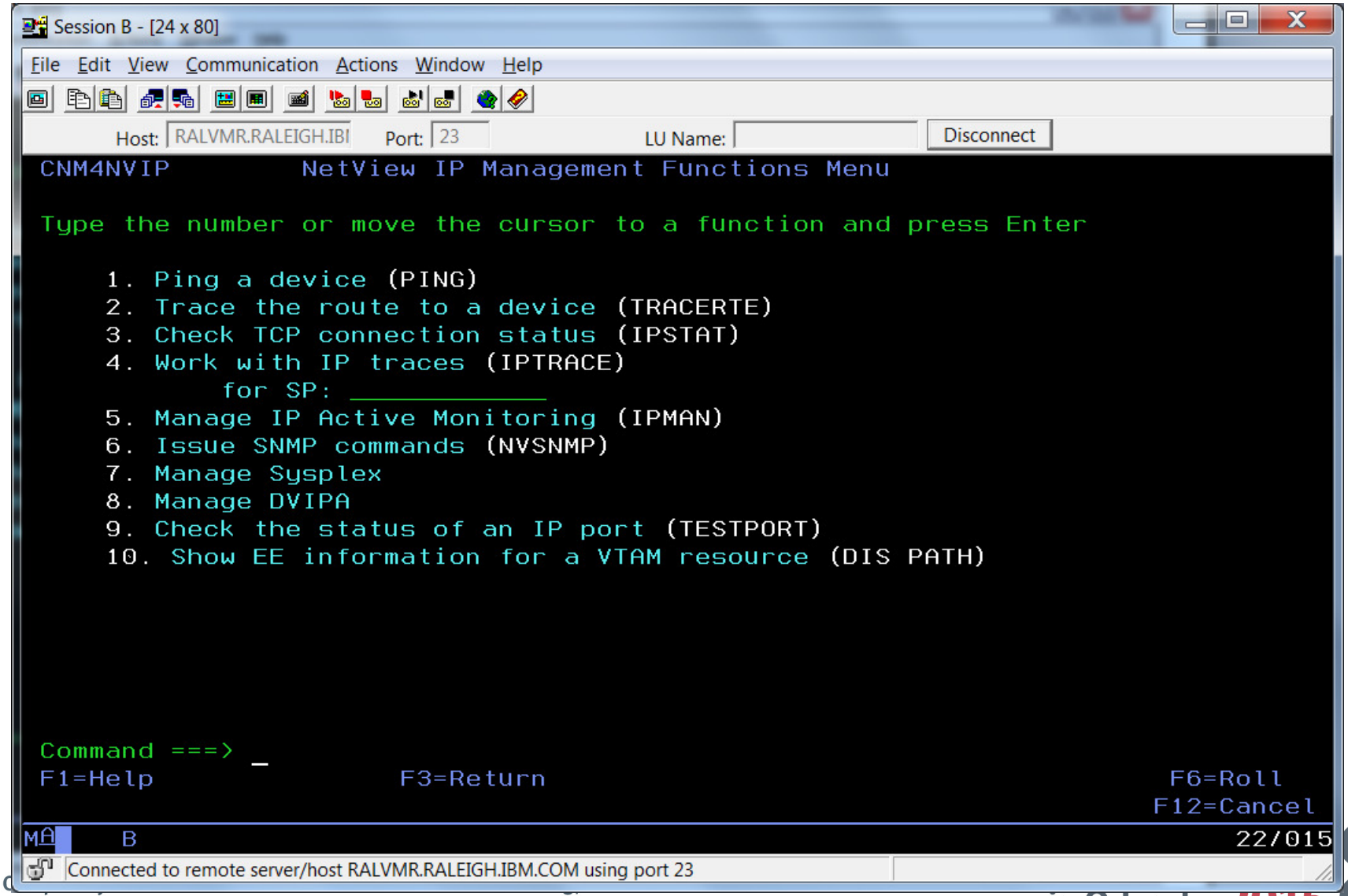
- IP Commands
- TCP Connection Management
- Intrusion Detection
- Sysplex Management
  - Discovery Manager
  - DVIPA
- Scenarios:
  - Packet Trace
  - DVIPA
    - Sysplex Distributor Favoring a System
    - Sysplex Distributor Performance
- Backup
  - Answers to questions from the session
  - Additional scenarios

IP Commands

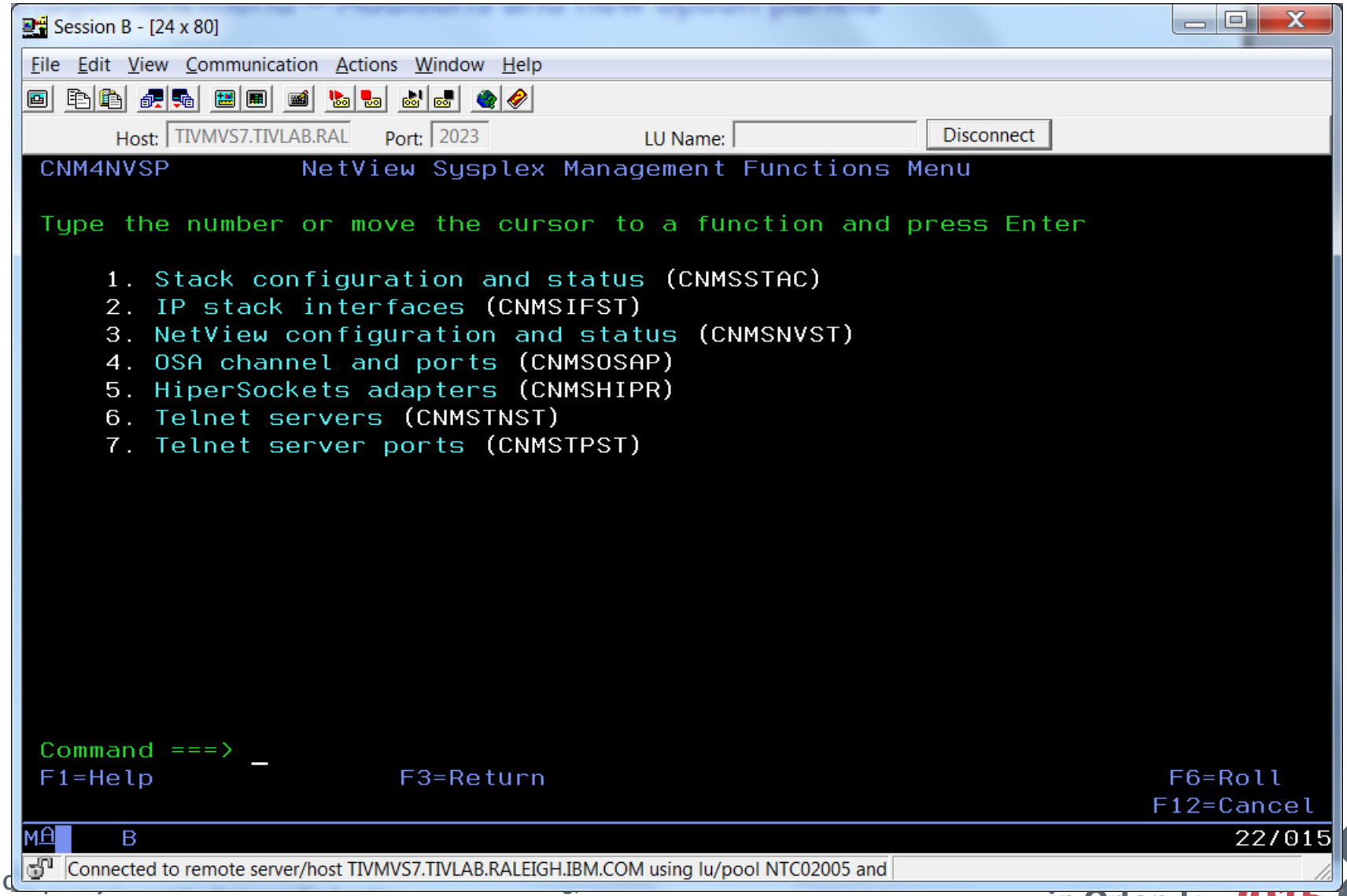
NetView Main Menu: IP Management Option



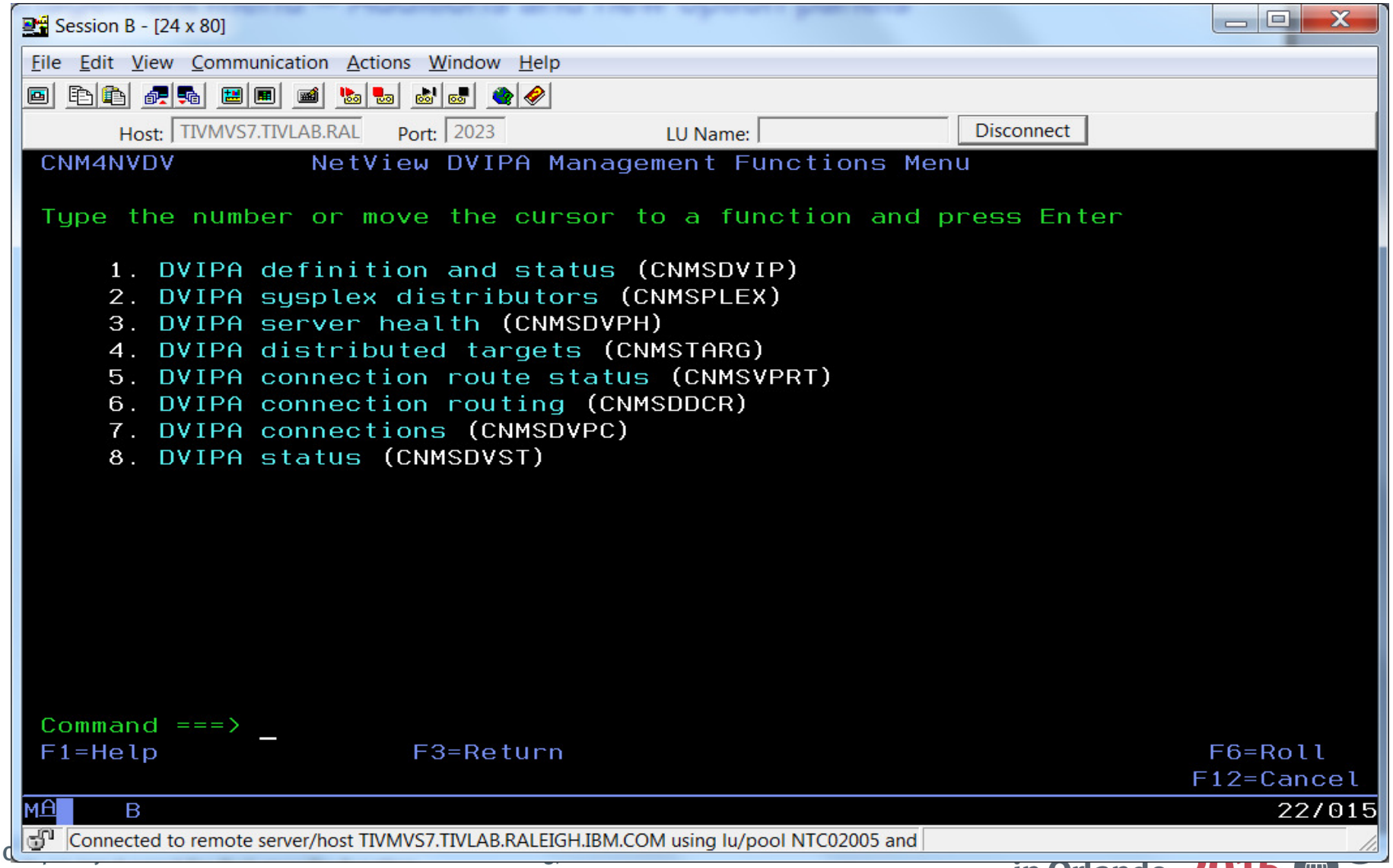
IP Management Menu



IP Management Menu: Sysplex Management



IP Management Menu: DVIPA



IP Commands

- IPLOG
- Ping
- Remote Ping
- Tracerte
- TN3270
- REXEC
- RSH
- SOCKET
- RMTCMD over IP
- Any UNIX System Services command
- IPXLATE (REXX, PL/I, C)
- EZLEMAIL (send email via SMTP)
- SNMP commands (including SNMPv3)
  - get
  - getnext
  - set
  - walk
  - trap
  - getbulk (SNMPv2c and SNMPv3)
  - bulkwalk (SNMPv2c and SNMPv3)
  - inform (SNMPv2c and SNMPv3)
  - the NVSNMP command enables panel-driven SNMP requests

TCP Connection Management

TCP/IP Connection Management

NetView for z/OS can help manage TCP/IP connections, especially when combined with OMEGAMON XE for Mainframe Networks.

- Uses z/OS Communications Server network management interface (NMI) to retrieve connection data for TCP/IP connections
- Active connection data kept in NetView (and Comm Server) storage
- Inactive connection data written to VSAM
- Data can be filtered using CNMSTYLE definitions
- NetView cross-domain capabilities enable the viewing of connection data at remote z/OS hosts
- Supports IPv4 and IPv6

Connection Data

- Active Connections
  - Local IP address and port
  - Remote IP address and port
  - TCP/IP stack name
  - Start date and time
  - Last activity date/time
  - Connection ID
  - Bytes sent/received
  - Byte rate
  - Segments retransmitted
  - Percent segments retransmitted
  - And more
- Inactive Connections
  - Local IP address and port
  - Remote IP address and port
  - TCP/IP stack name
  - Start date and time
  - End date and time
  - Bytes sent and received
  - Send window size
  - Logical unit (LU) name
  - Target application identifier (APPLID)
  - Termination code
  - And more

Issue HELP BNH772 (inactive) or BNH775 (active) for complete details.

Displaying Connection Data

Connection data can be viewed from the following places:

- NetView 3270 console
  - TCPCONN
    - Raw data
    - Unformatted
    - Intended for programmatic use
  - CNMSTCPC
    - Formatted
    - Customizable
    - Intended for human user
  - IPSTAT
    - Panel-based connection control
- Tivoli Enterprise Portal

Intrusion Detection

TCP/IP Intrusions

Enhance network security by combining NetView automation facilities with the Intrusion Detection Service (IDS) of the z/OS Communications Server.

- What is an intrusion?
  - Information gathering (scan)
    - Network and system information
    - Data locations
    - Map target of an attack
  - Eavesdropping, impersonation, or theft
    - On the network, on the host
    - Base for further attacks on others
  - Denial of Service
    - Attack on availability
- Intrusions can occur from Internet or Intranet
  - Firewall can provide some level of protection from Internet
  - Perimeter security strategy *alone* may not be enough
  - Within a firewall, systems can be vulnerable to attack or misuse, whether accidental or malicious.

TCP/IP Intrusions

- z/OS Communications Server Intrusion Detection Service (IDS) detects:
  - Scans
    - Fast
    - Slow
    - ICMP, TCP UDP
  - Attacks
    - Malformed packets
    - IP option restrictions
    - ICMP redirect restrictions
    - Outbound raw socket restrictions
    - And more …
  - Floods

Automated Actions (Intrusion Detection)

- Notify
  - NetView alert (default)
  - Message to designated NetView operators (default)
  - email to designated recipient (for example, security administrator)
    - Using INFORM policy
- Issue UNIX, z/OS, or NetView commands
  - Gather more data
  - Take action, such as close the port
- Update statistics kept on basis of probe ID
- Collect additional statistics, email to security administrators

Sysplex Management

Dynamic IP Stack Discovery (Discovery Manager)

- IP stacks are detected automatically
  - When the NetView program initializes
  - When a stack starts after the NetView program
- Supports running multiple IP stacks
- Supports IPv6
- No need to define stacks unless you need to:
  - Manage a stack on a remote system that is not part of the same sysplex

Discovery Manager – Resources Discovered

- Information collected:
  - Central processor complex (CPC)
  - Channel subsystem identifier
  - Logical partition (LPAR)
  - Sysplex
  - Coupling facility
  - z/OS image
  - TCP/IP stack
  - TCP/IP subplex
  - IP interfaces
  - NetView applications
  - Telnet servers and ports
  - Open Systems Adapter (OSA) channels and ports
  - HiperSockets adapter

- Data available in Tivoli Enterprise Portal, NMC, and 3270 commands

DVIPA Management Capabilities

- NetView provides a lot of DVIPA information for use in managing and diagnosing problems in your sysplex:
  - Sampled, real-time, and historical monitoring capabilities
  - DVIPA events
  - Distributed DVIPA statistics

- DVIPA information can be viewed at the:
  - Local NetView domain
  - Sysplex master NetView domain
    - Displays DVIPA information available from all NetView domains in the sysplex
      - DVIPA connection information is not forwarded to the sysplex master NetView for performance reasons

- DVIPA information is displayed in the:
  - Tivoli Enterprise Portal (TEP) using the NetView for z/OS Enterprise Management Agent
  - NetView 3270 console

DVIPA Monitoring

- NetView provides the following DVIPA information:
  - DVIPA Definition and StatusSysplex Distributors
  - Distributed DVIPA (DDVIPA) Targets
  - DDVIPA Server Health, including a view for:
  - DVIPA Connections
  - VIPA Routing
  - DDVIPA Connection Routing

- TEP displays sampled (updated by events) and historical data
  - Historical data collection must be enabled
  - Long term history requires Tivoli Data Warehouse.

- NetView 3270 commands and samples display real-time DVIPA information

DVIPA Events

- DVIPA Events can be used to provide a better “real time” view of DVIPA information. NetView has automation for three types of DVIPA Events:
  - Real-time DVIPA changes
    - DVIPA status change and DVIPA removed
    - DVIPA target added and removed
    - DVIPA target server started and ended
  - DVIPA Configuration Changes
  - Sysplex Autonomics messages
- When a DVIPA event is received:
  - NetView will bundle the events using configurable delays
  - Notify the master that this system needs rediscovering
    - The master NetView also has a delay to bundle the event messages
  - Send rediscovery commands to all systems in the sysplex impacted by the event

Packet Trace with NetView v6.1

- Start / stop a single (“global”) trace
- Display unformatted packets
- View formatted packets and analysis of trace records
- Save traces into NetView data sets
- Control multiple systems from a single point

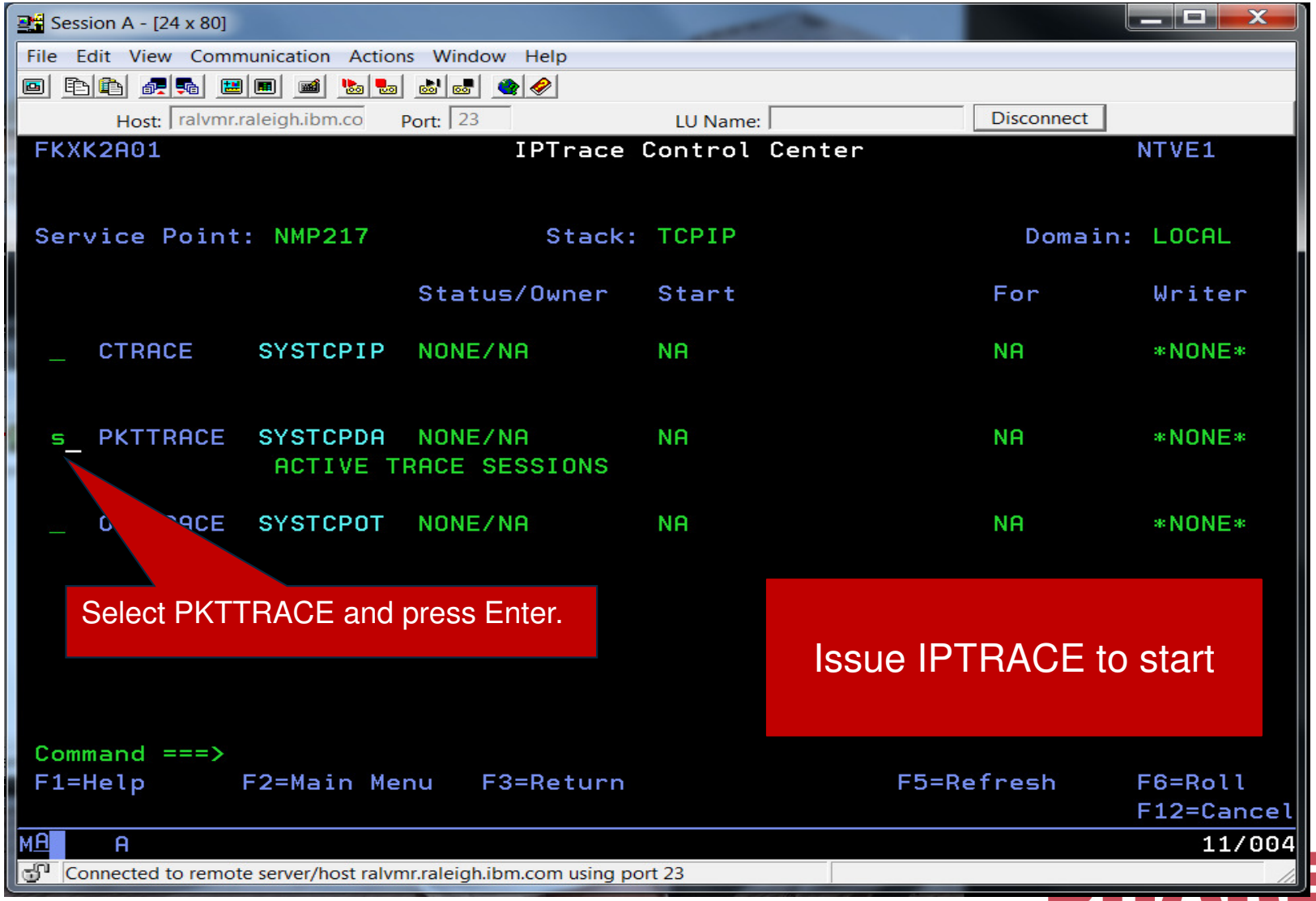
New in NetView for z/OS v6.2

- Support for multiple, concurrent packet traces (“instance” traces)
  - Multiple users can trace multiple problems from a given stack at the same time, each using different trace criteria.
  - Operators can define filters for specific issues
  - Avoids creation of unneeded trace records
  - Requires z/OS Communications Server V2.1
- Save traces in IPCS format
  - Traces can be analyzed in IPCS using the IPCS formatter tool
  - Traces can be converted to Sniffer format for use in other tools
  - Traces from different systems can be merged into a single trace
  - Traces can be sent to Comm Server Support for diagnosis
- Navigation / Filter enhancements

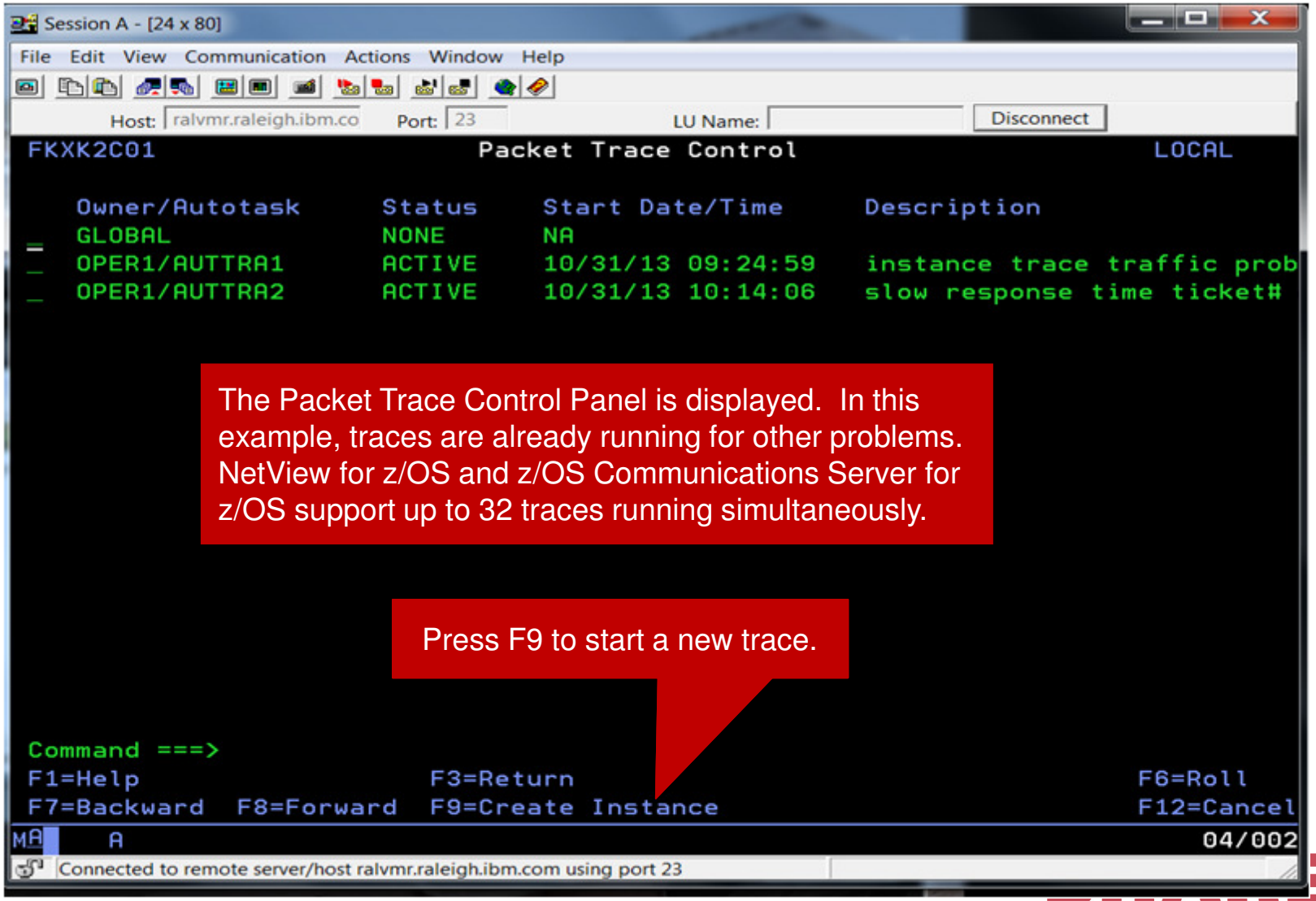
Scenario: Packet Trace Connectivity

- Scenario:
  - Users report an intermittent problem where it takes “a long time” to connect to an application. Occasionally, the connection attempt fails. They have noticed the problem occurs almost every day, at somewhat predictable times.
- Resolution Steps:
  - Use packet trace to help determine if there is a network problem.
  - Tracing the entire network should encompass the problem, but would result in a lot of packets to review.
  - By determining individual users' IP addresses, we can limit the data that has to be reviewed.
  - Multiple traces can help to compare a working connection attempt to a failing one.
  - Further analysis may be desired. The traces are saved in IPCS format, allowing them to be read by IPCS, where they can be merged or analyzed in more depth.

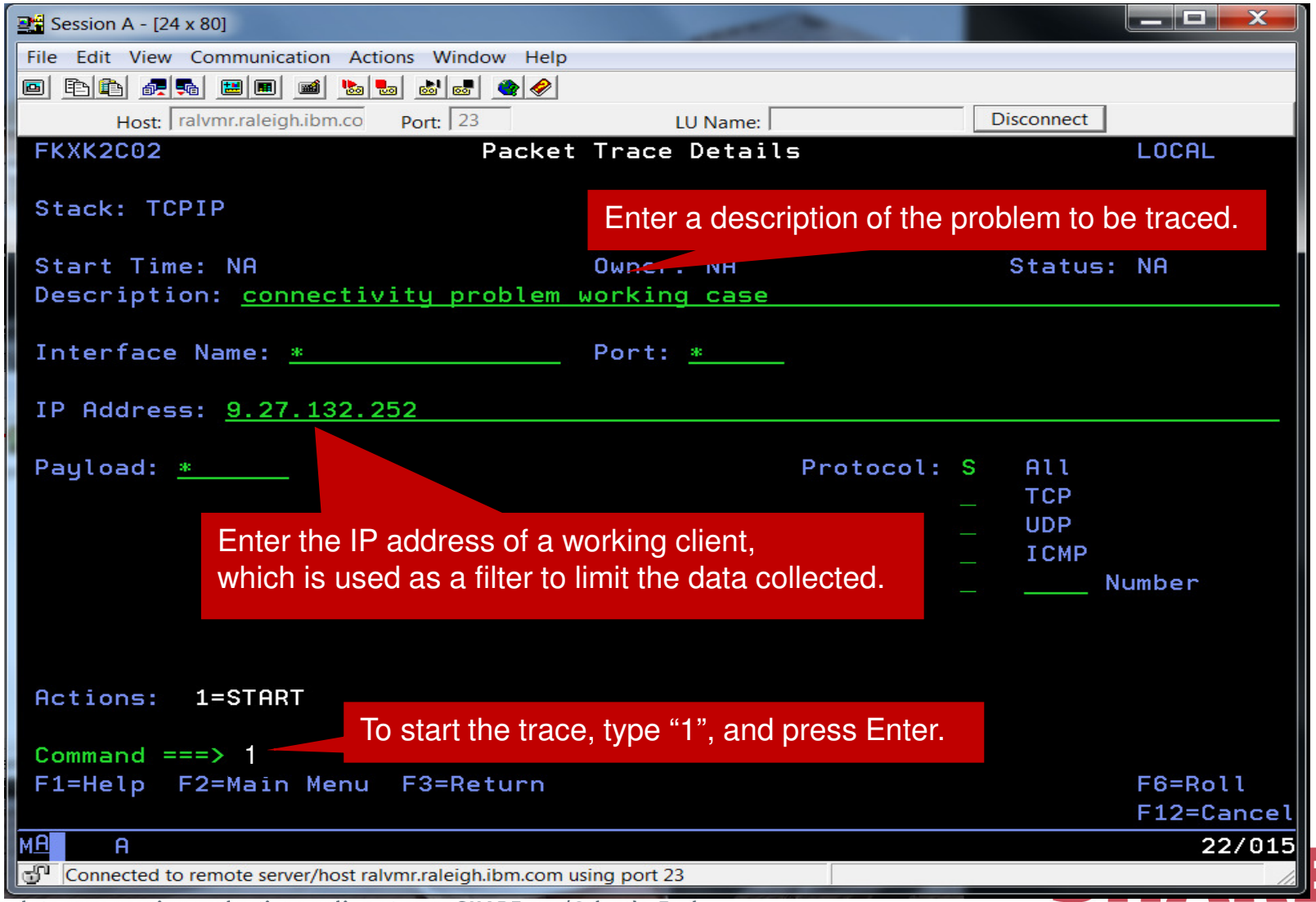
Scenario 1: Packet Trace



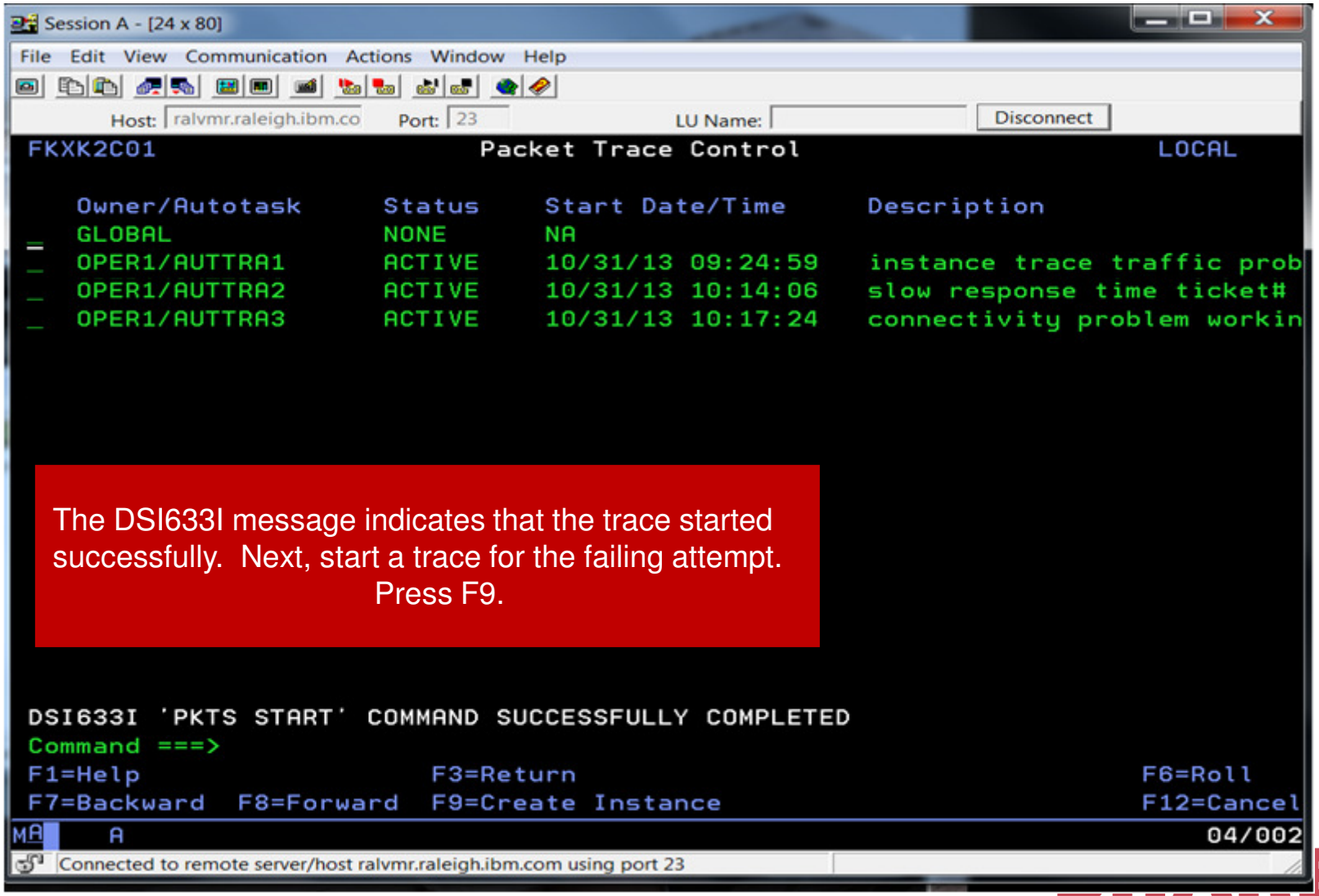
Scenario 1: Packet Trace



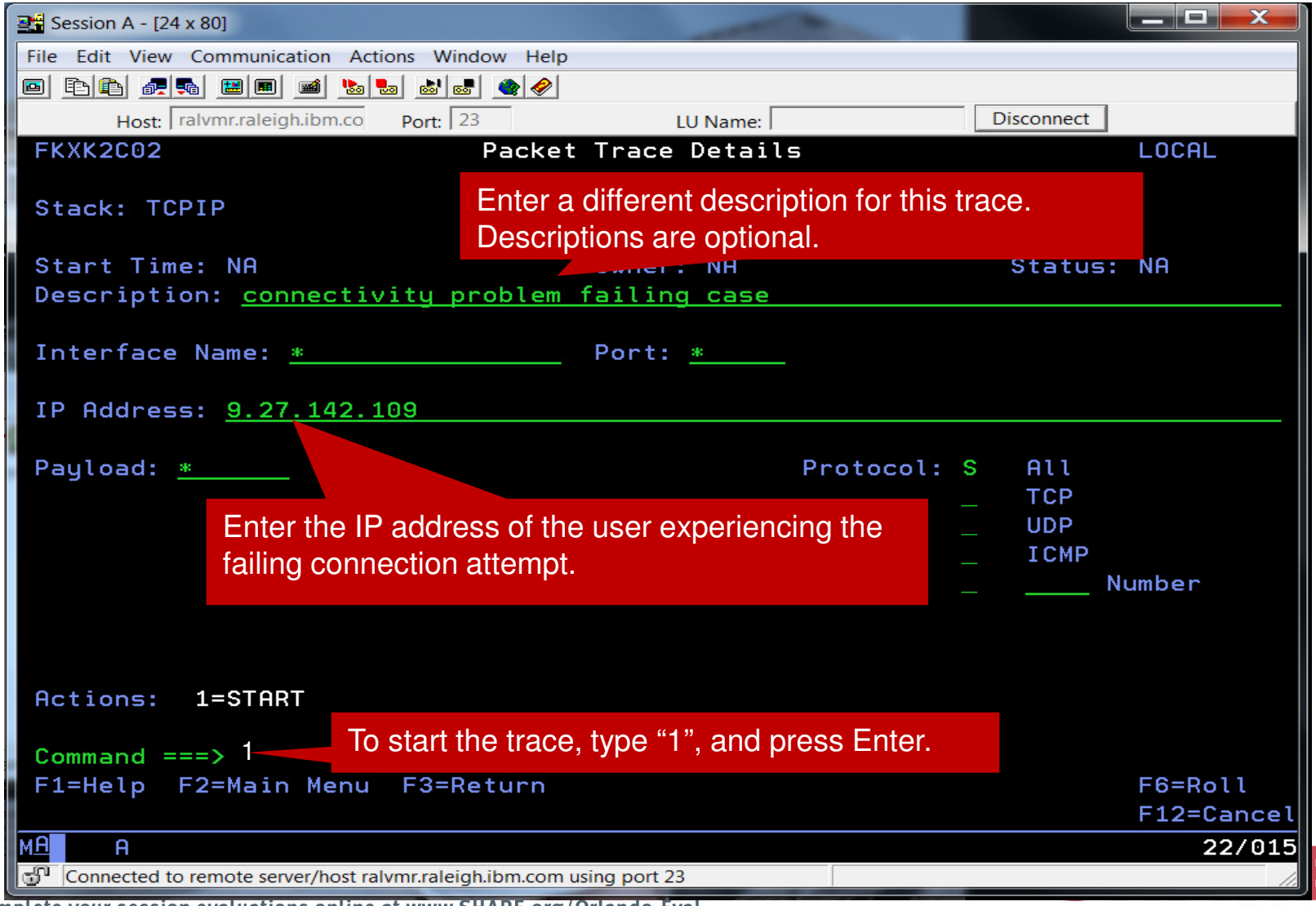
Scenario 1: Packet Trace



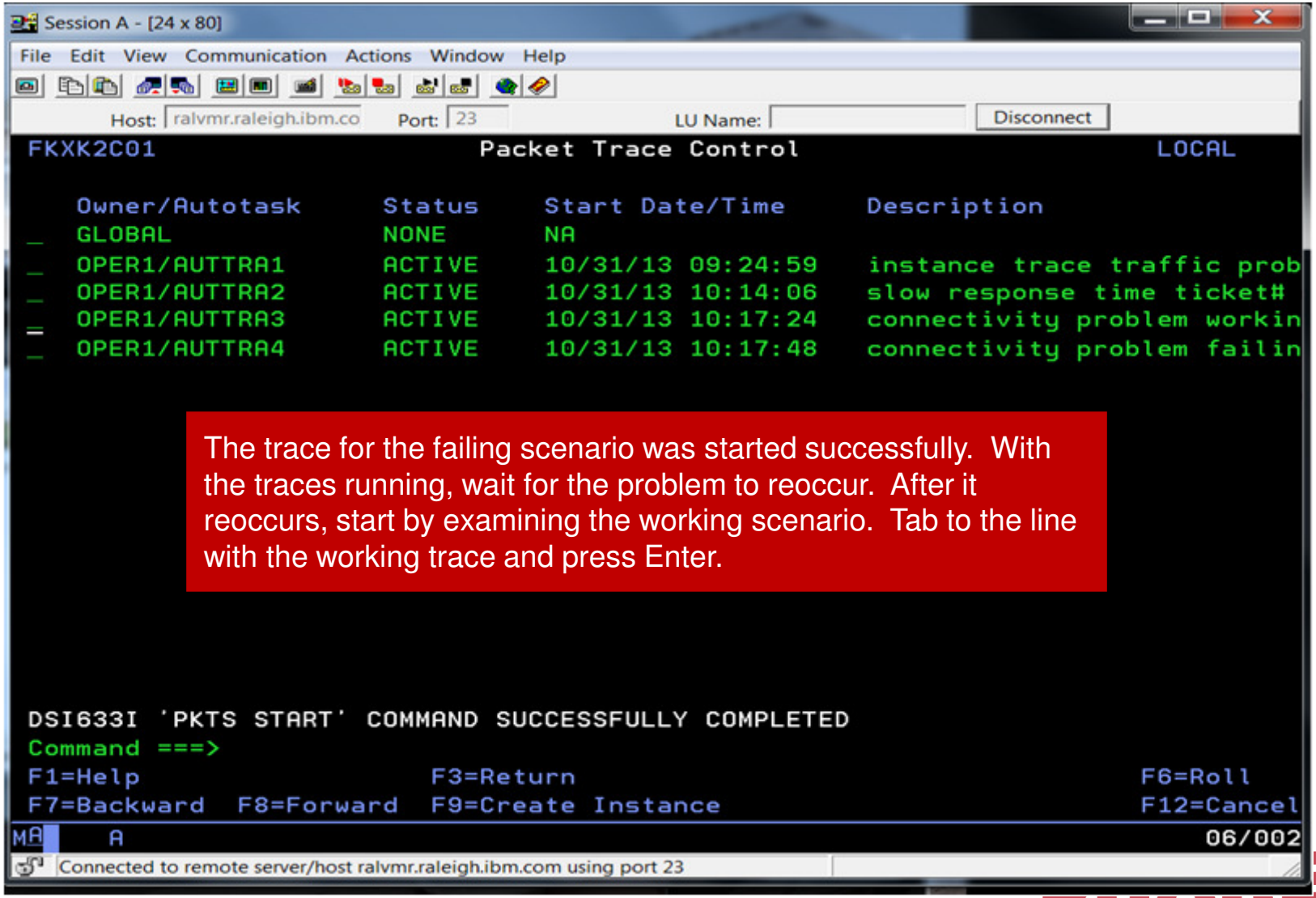
Scenario 1: Packet Trace



Scenario 1: Packet Trace

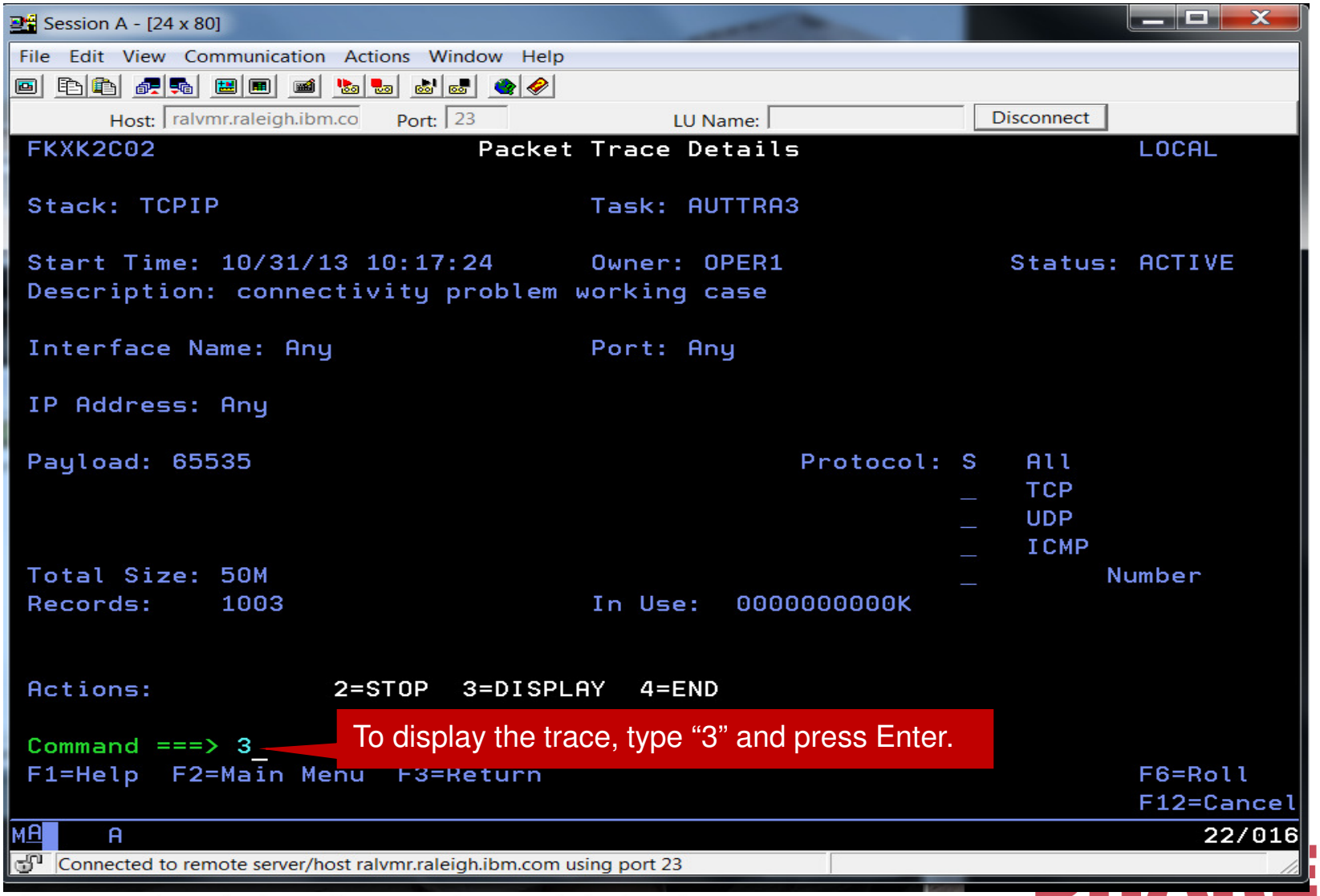


Scenario 1: Packet Trace

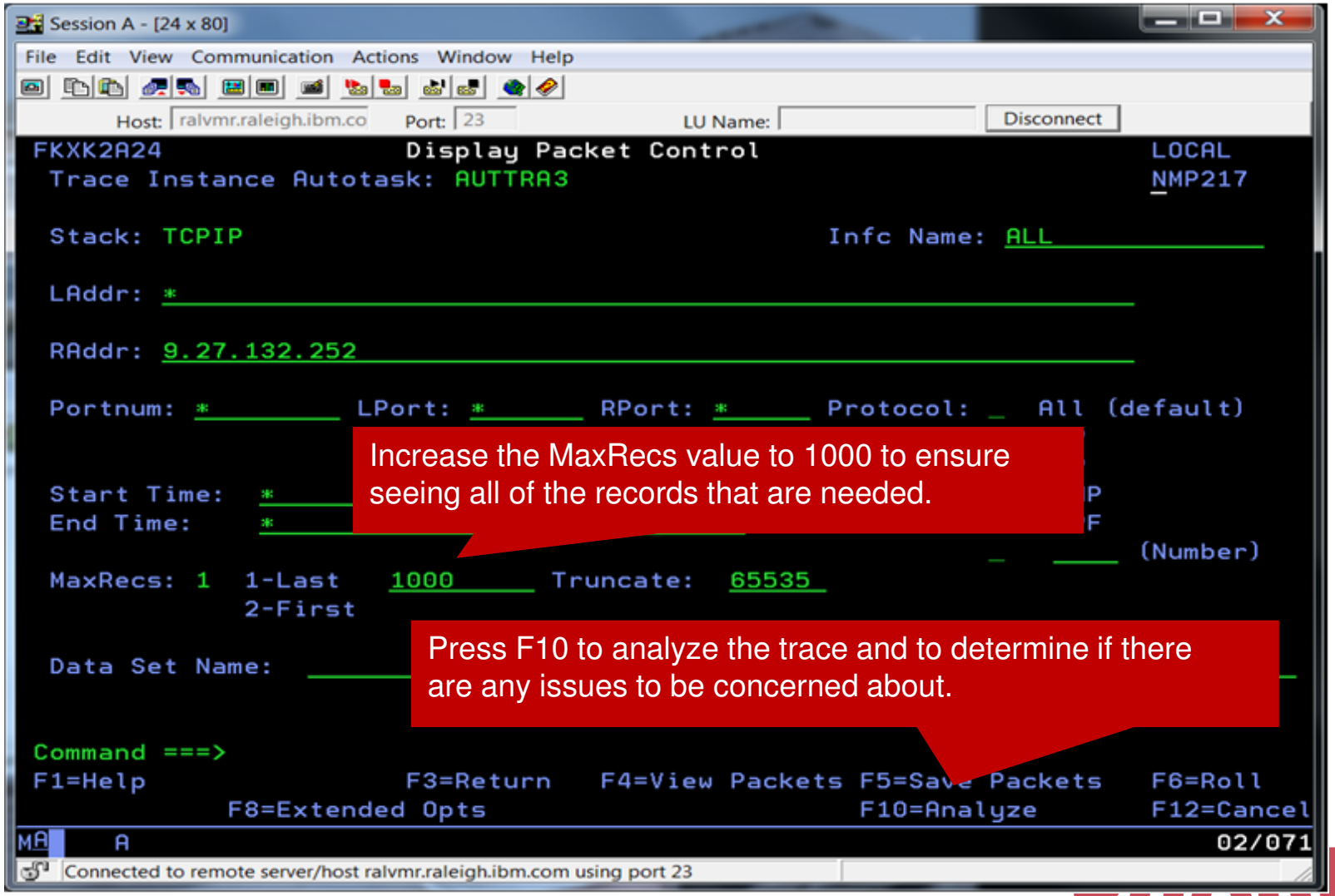


The trace for the failing scenario was started successfully. With the traces running, wait for the problem to reoccur. After it reoccurs, start by examining the working scenario. Tab to the line with the working trace and press Enter.

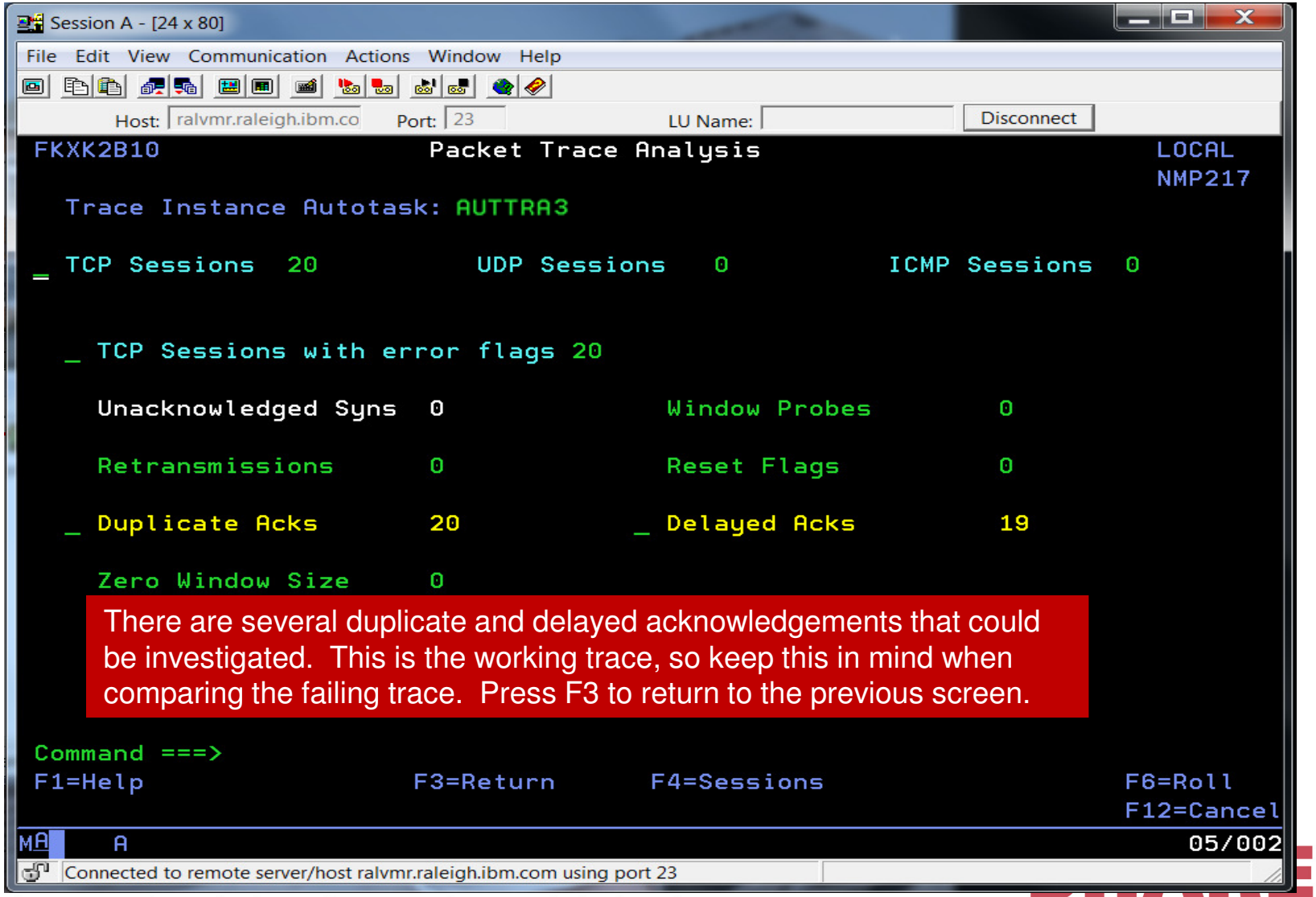
Scenario 1: Packet Trace



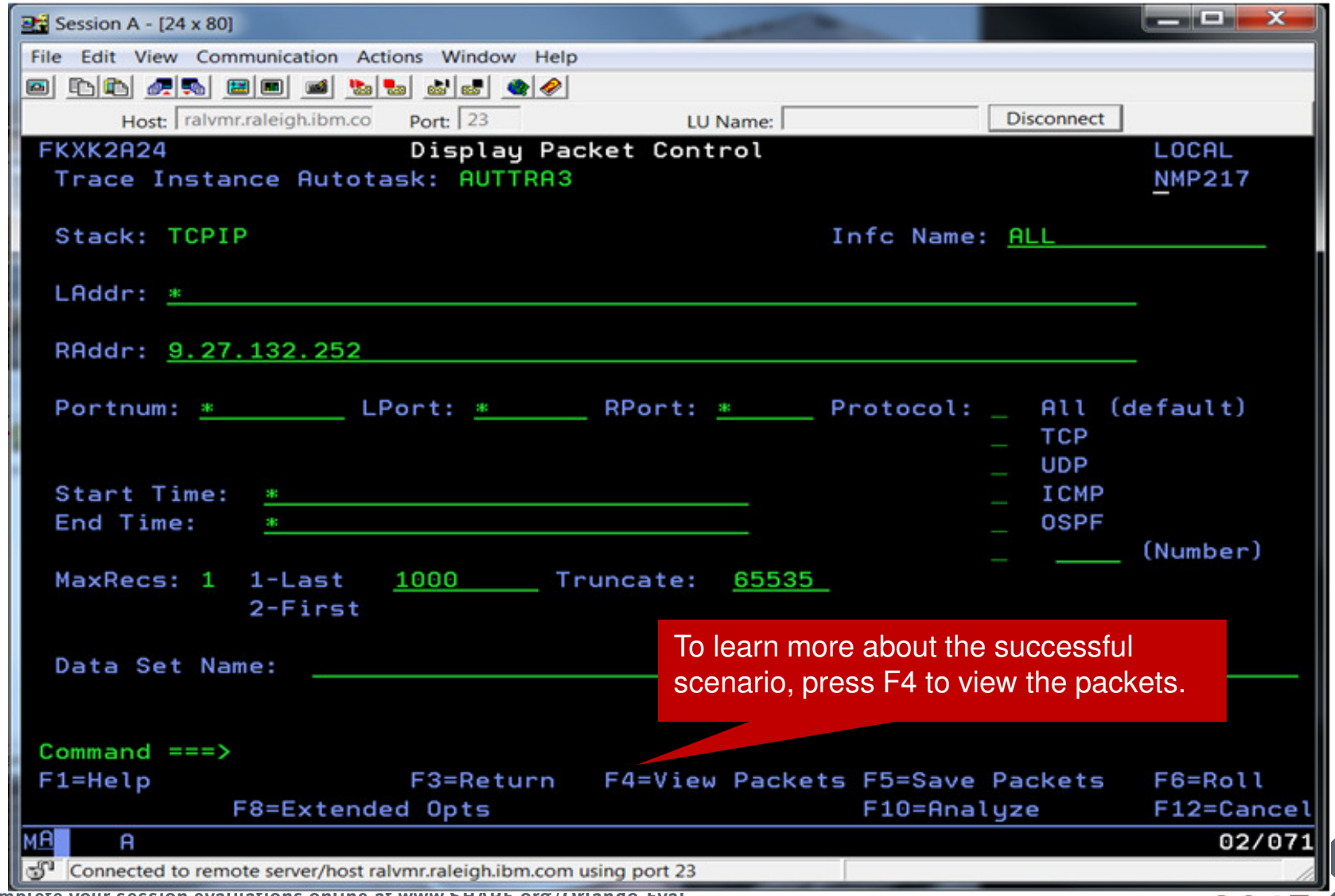
Scenario 1: Packet Trace



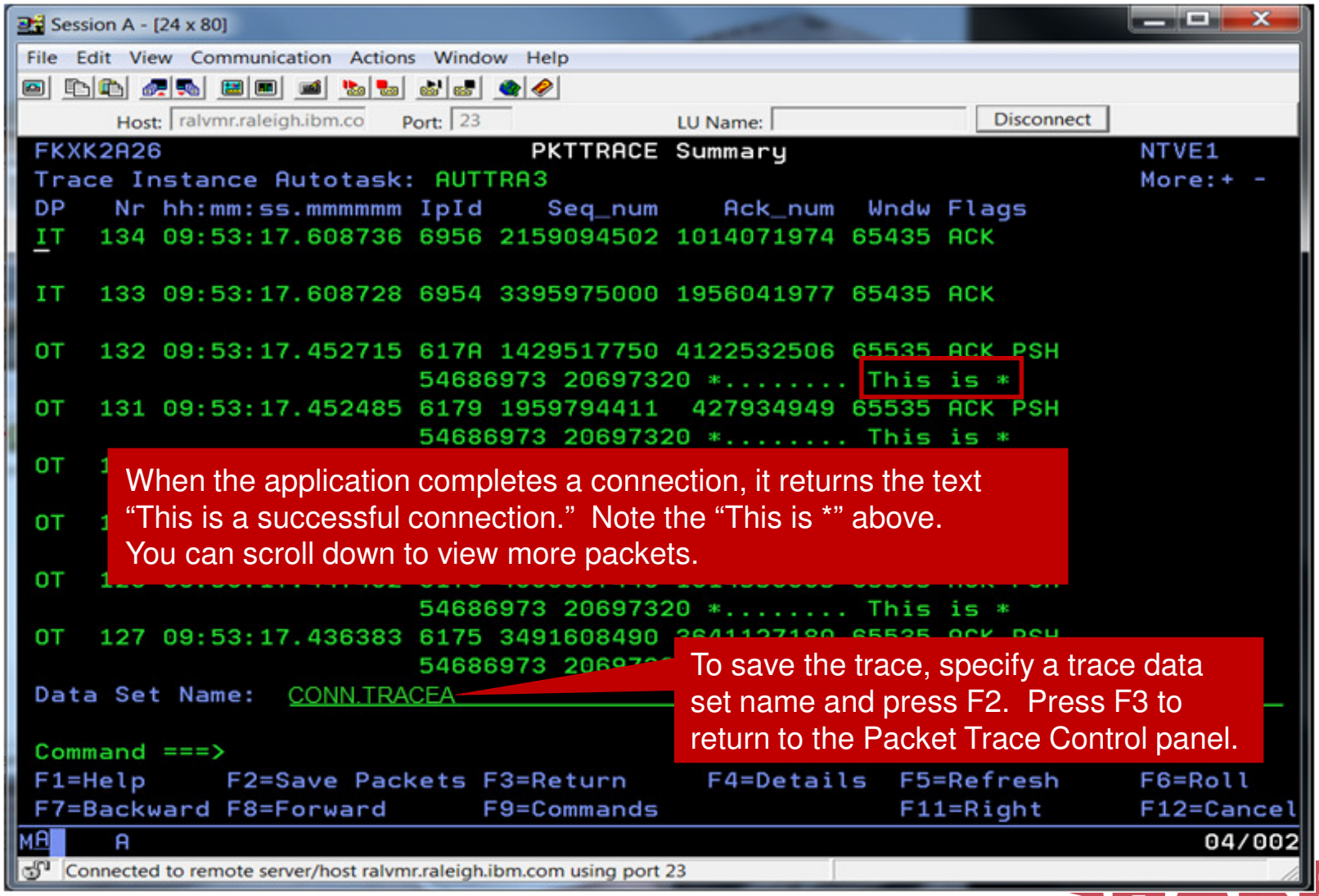
Scenario 1: Packet Trace



Scenario 1: Packet Trace



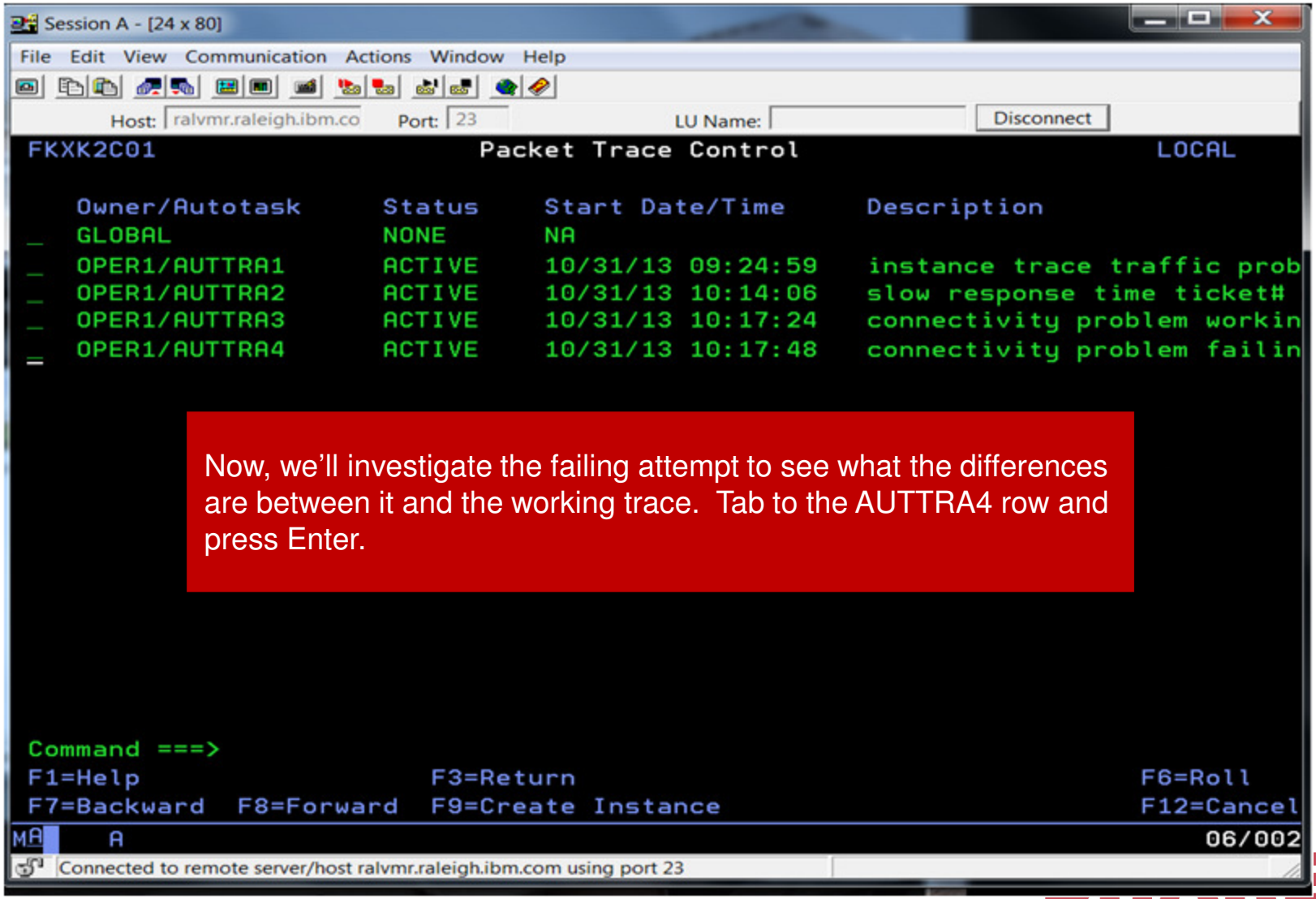
Scenario 1: Packet Trace



When the application completes a connection, it returns the text "This is a successful connection." Note the "This is *" above. You can scroll down to view more packets.

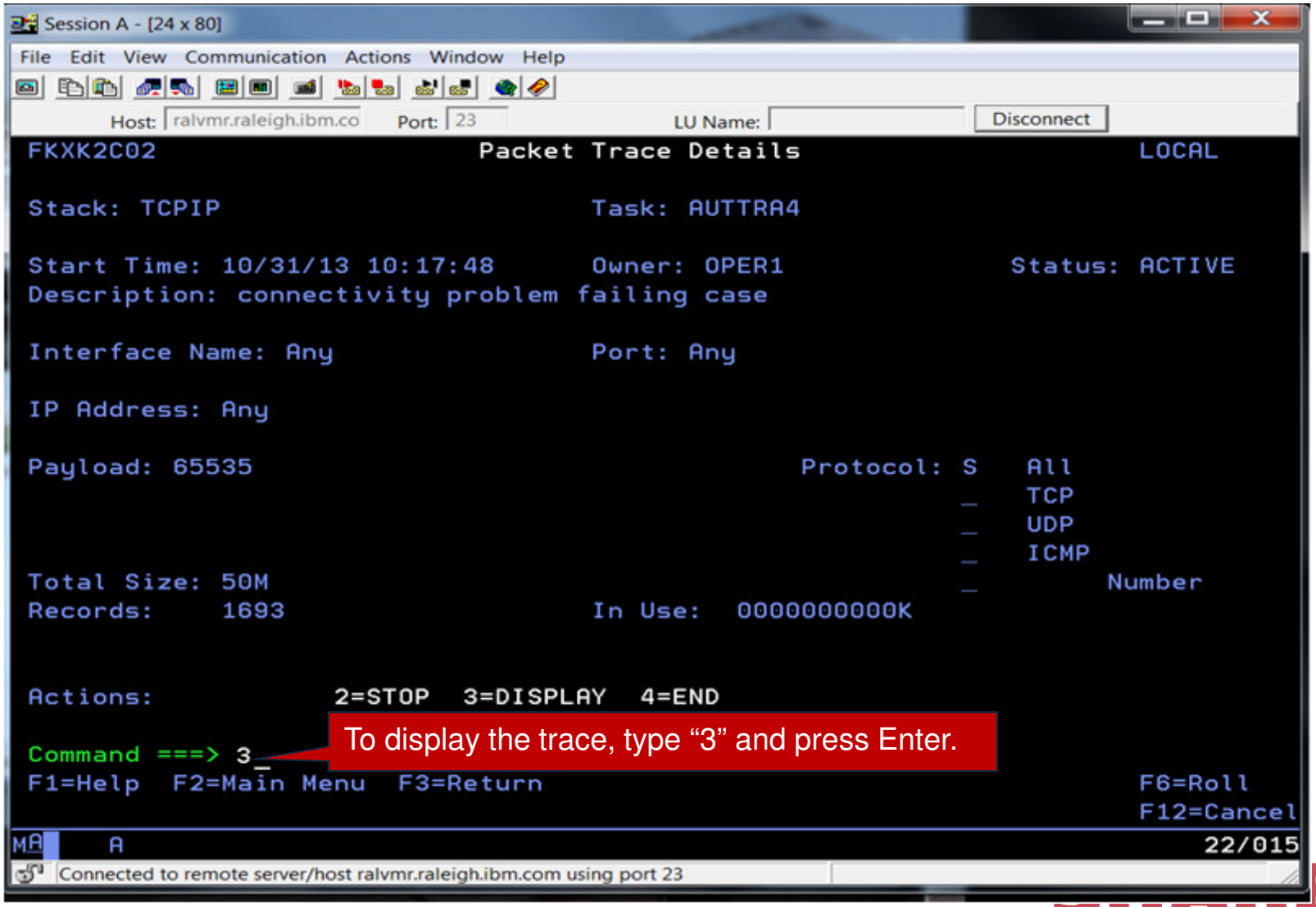
To save the trace, specify a trace data set name and press F2. Press F3 to return to the Packet Trace Control panel.

Scenario 1: Packet Trace

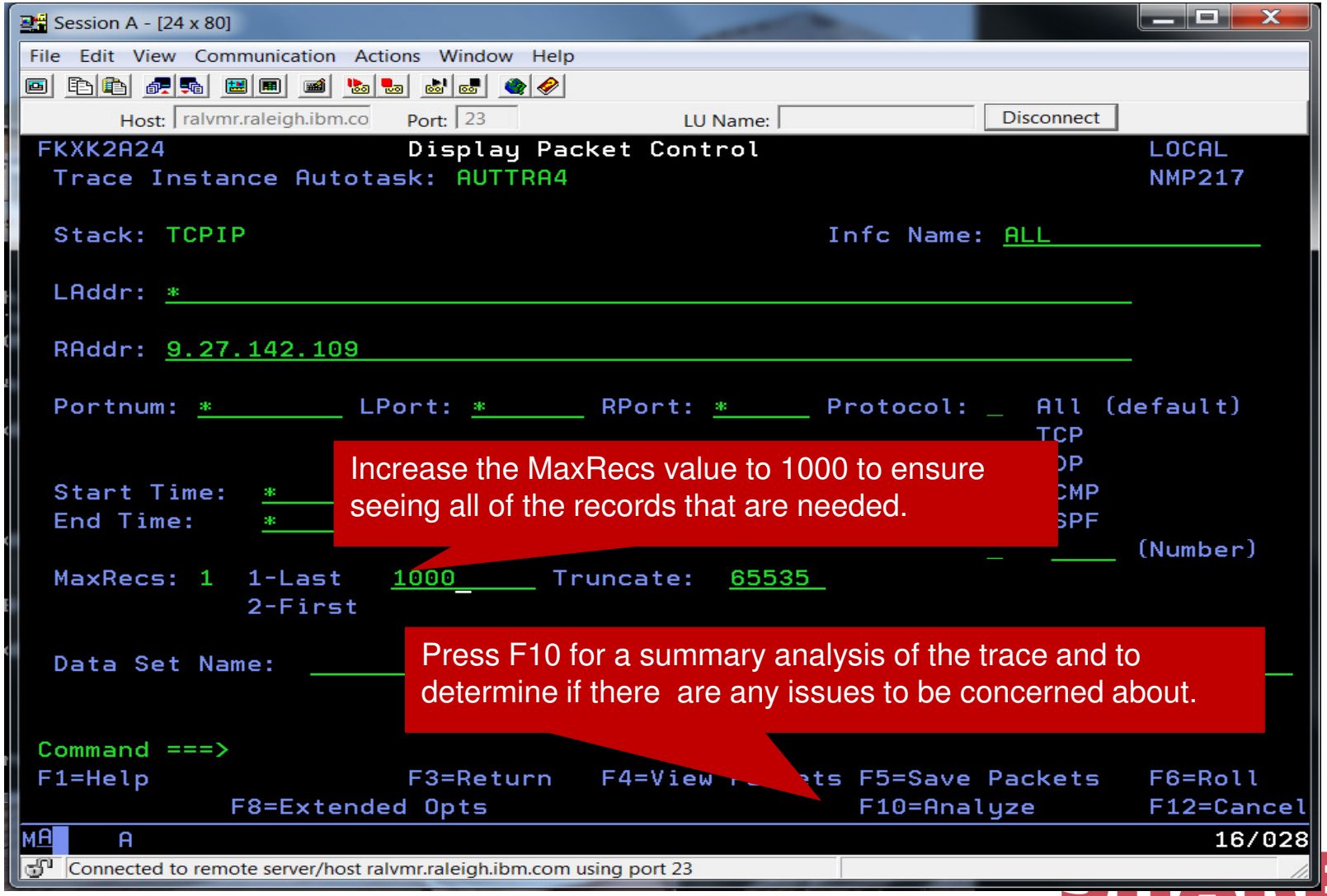


Now, we'll investigate the failing attempt to see what the differences are between it and the working trace. Tab to the AUTTRA4 row and press Enter.

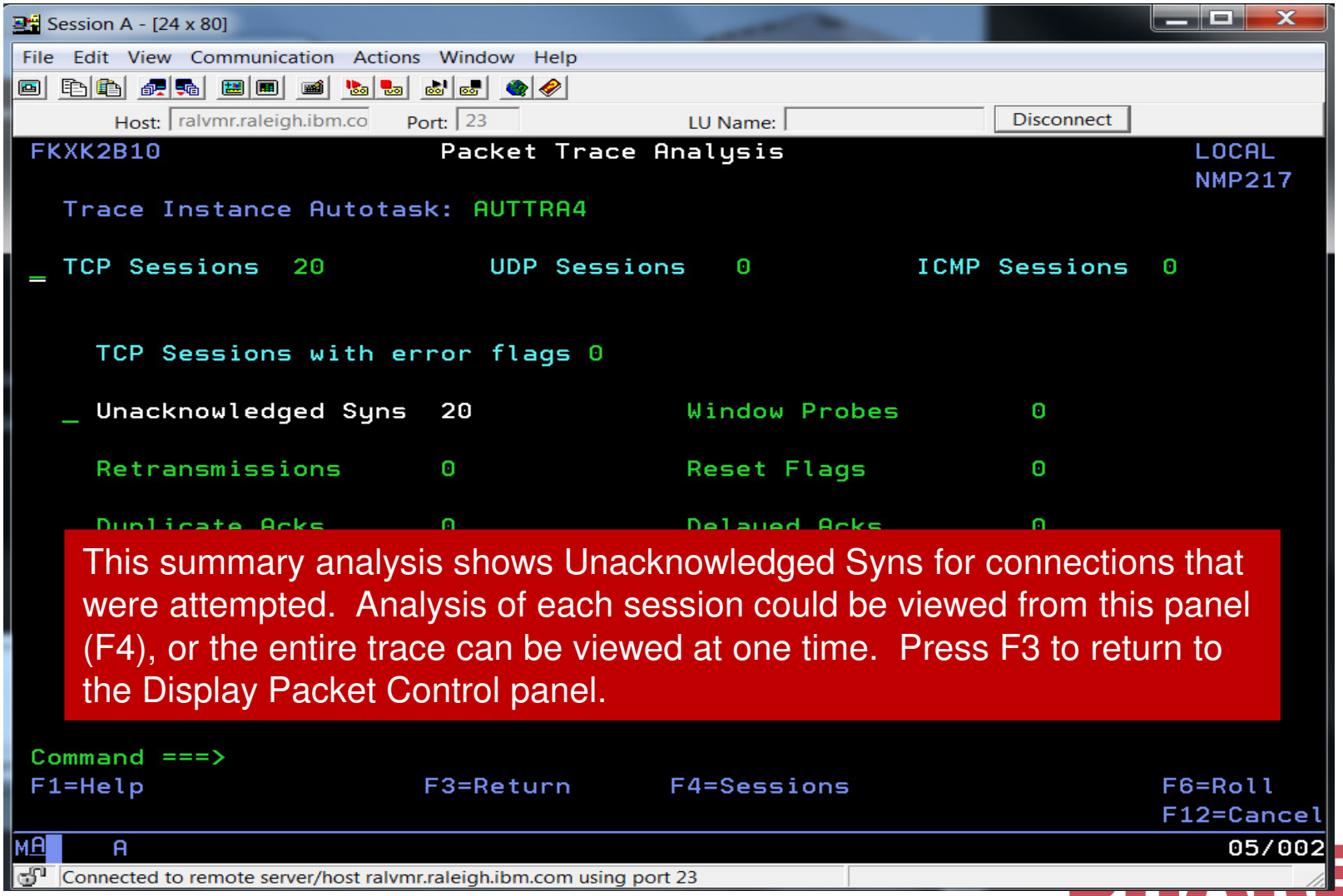
Scenario 1: Packet Trace



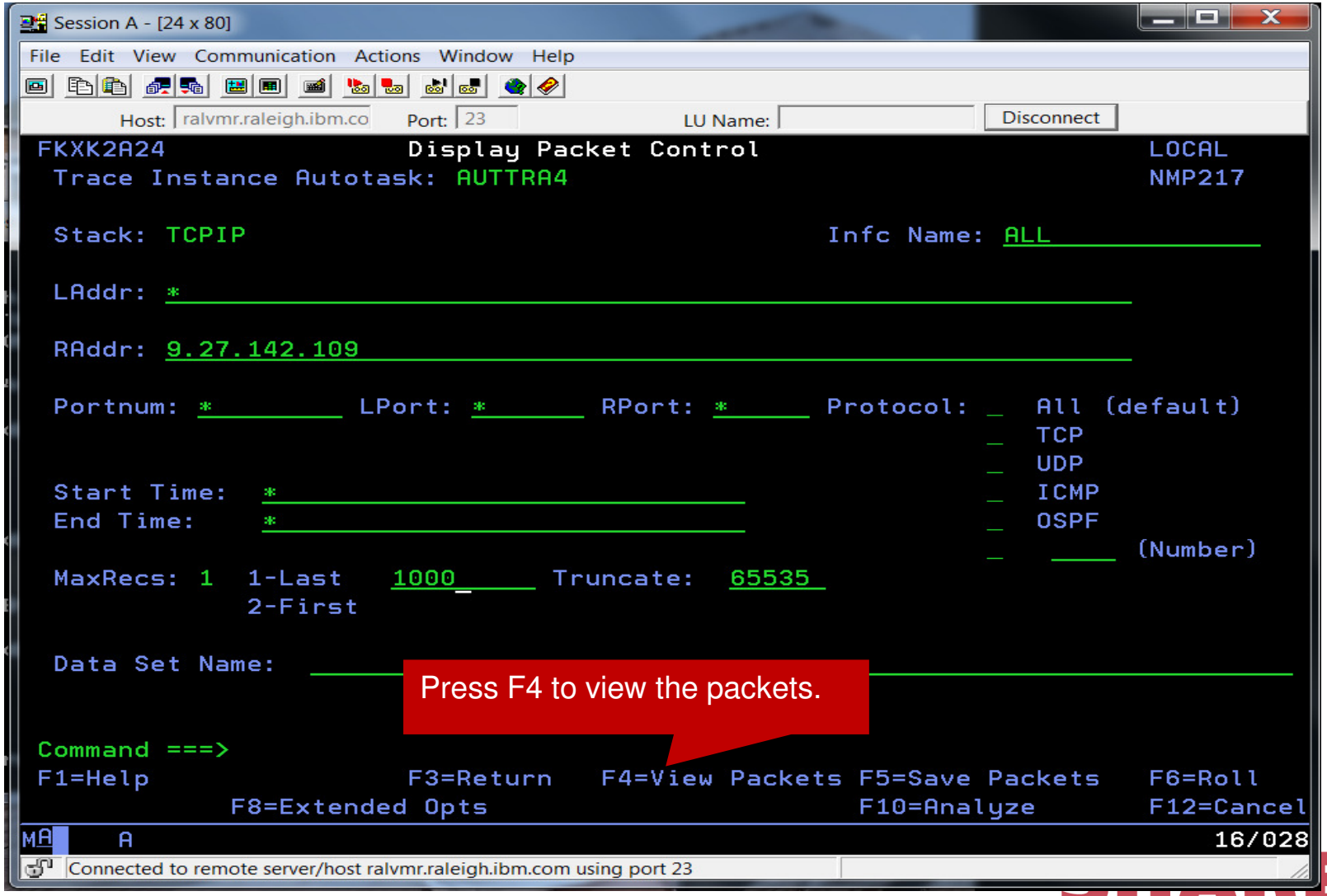
Scenario 1: Packet Trace



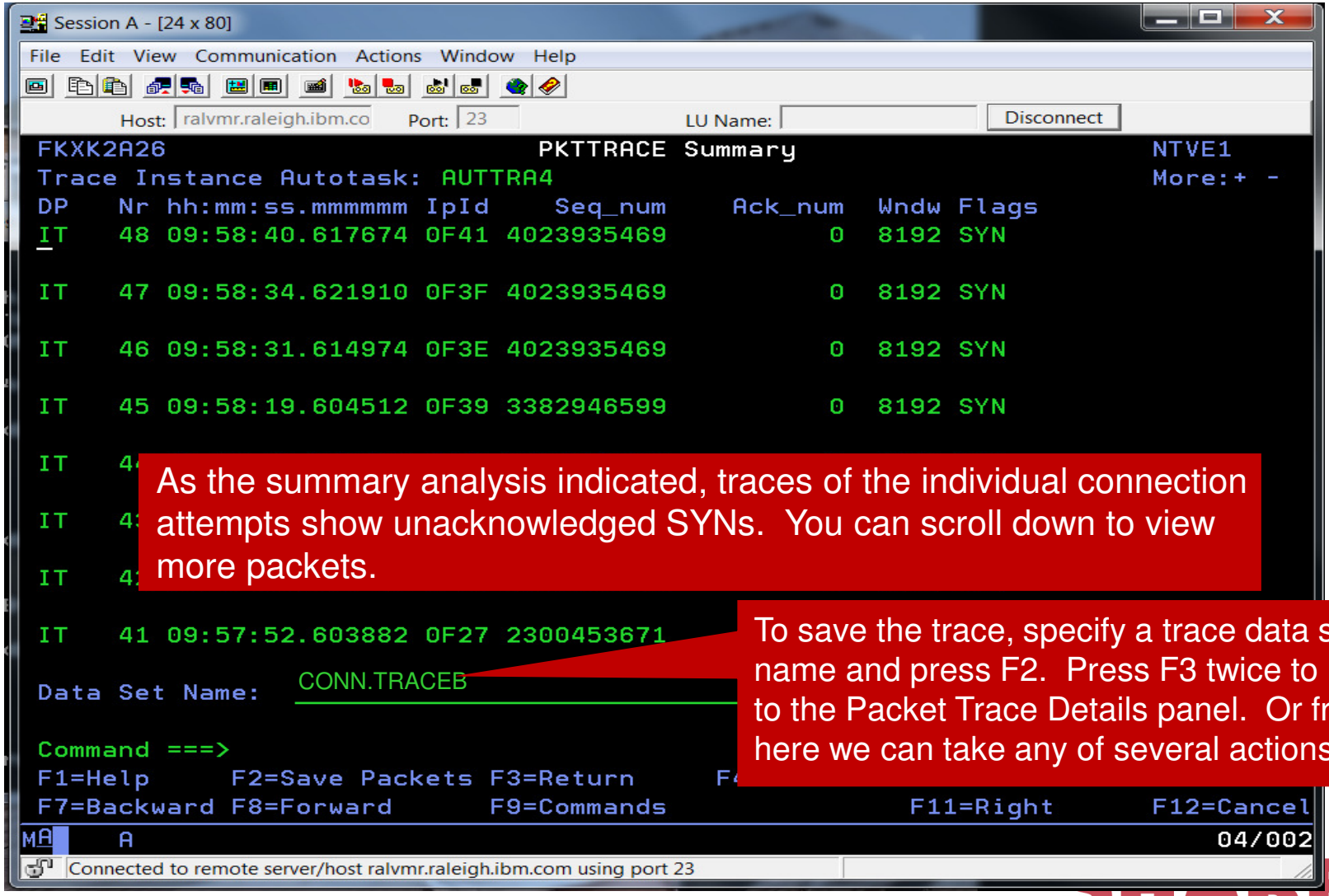
Scenario 1: Packet Trace



Scenario 1: Packet Trace



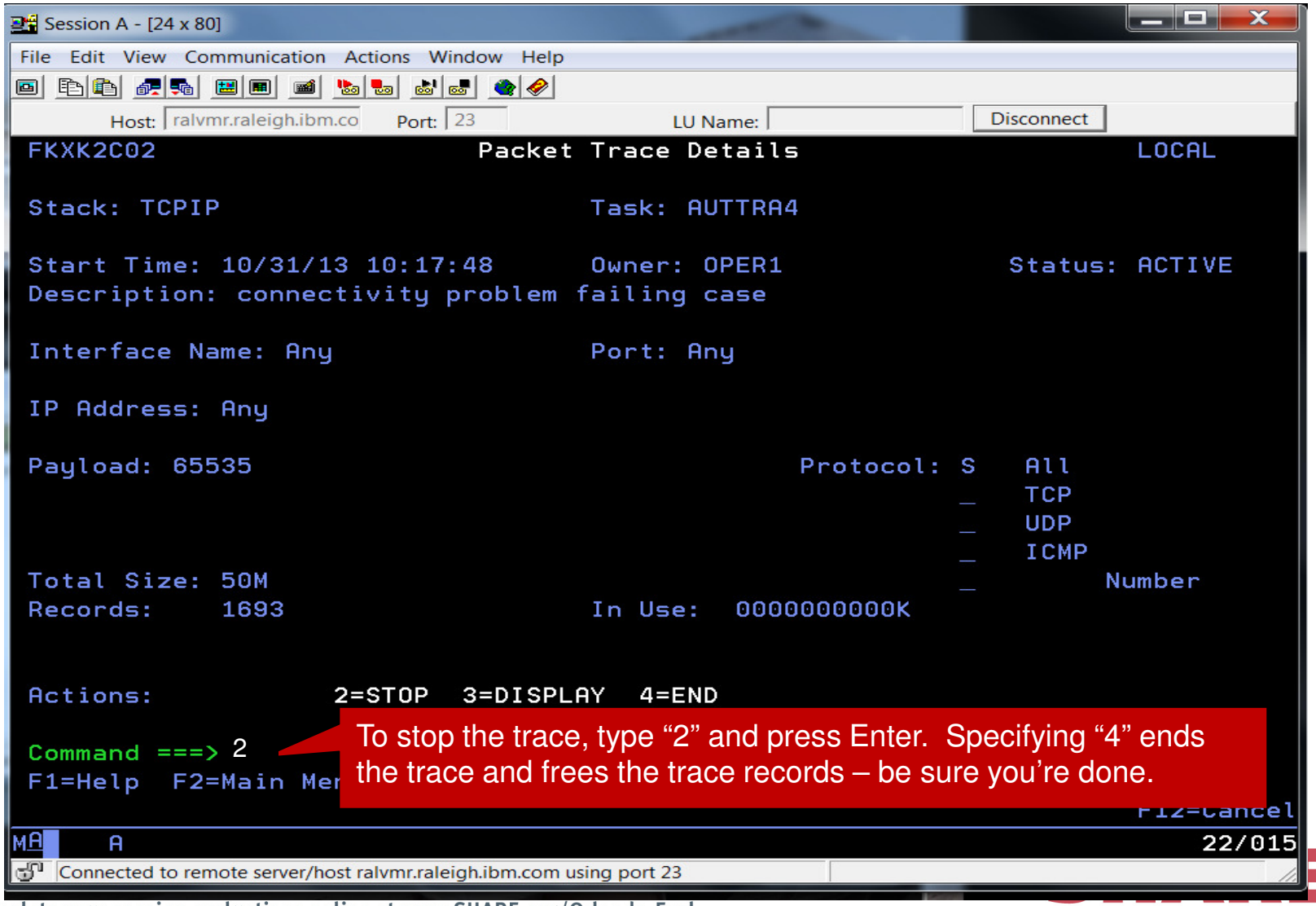
Scenario 1: Packet Trace



As the summary analysis indicated, traces of the individual connection attempts show unacknowledged SYNs. You can scroll down to view more packets.

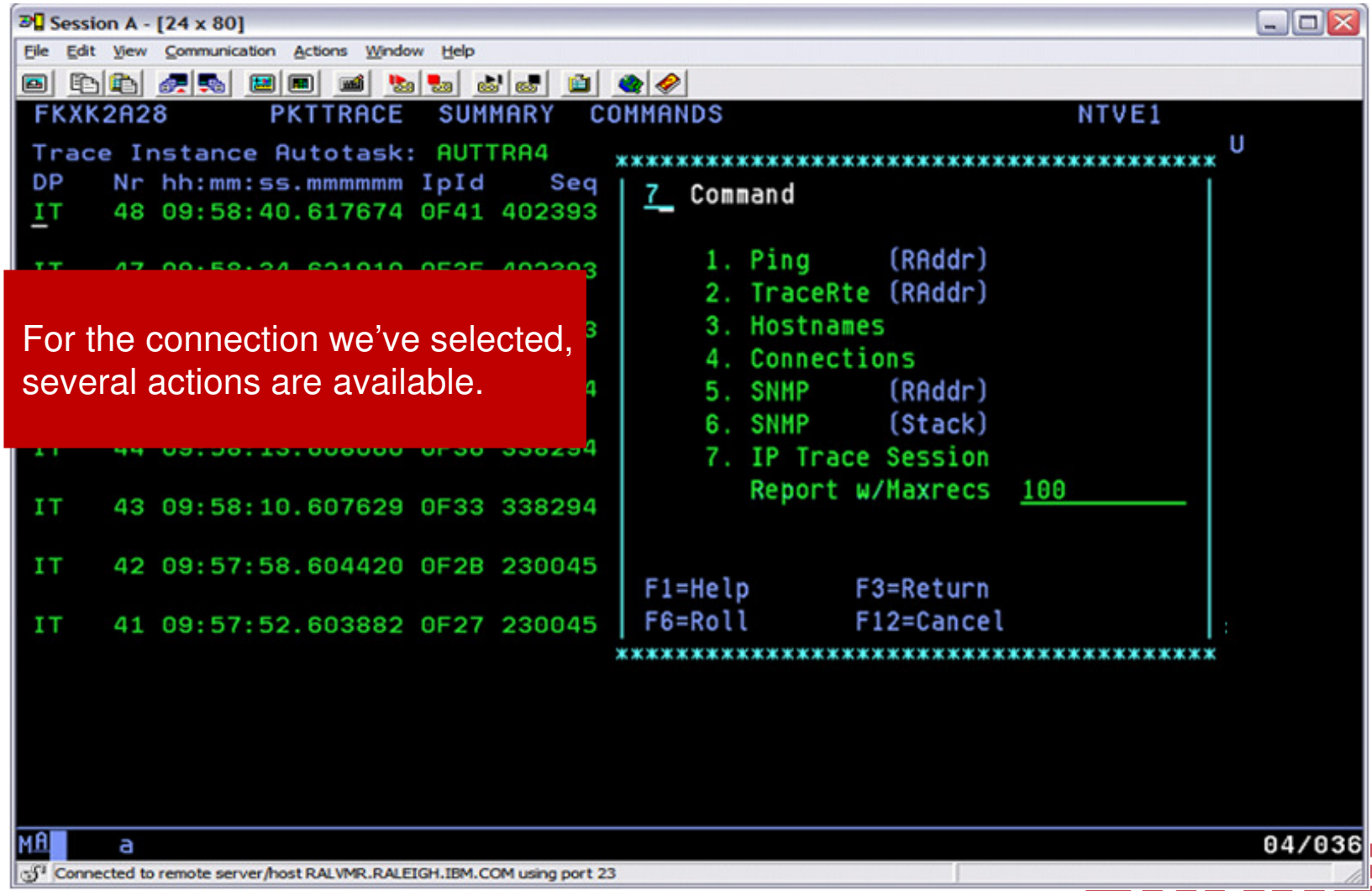
To save the trace, specify a trace data set name and press F2. Press F3 twice to return to the Packet Trace Details panel. Or from here we can take any of several actions: F9

Scenario 1: Packet Trace



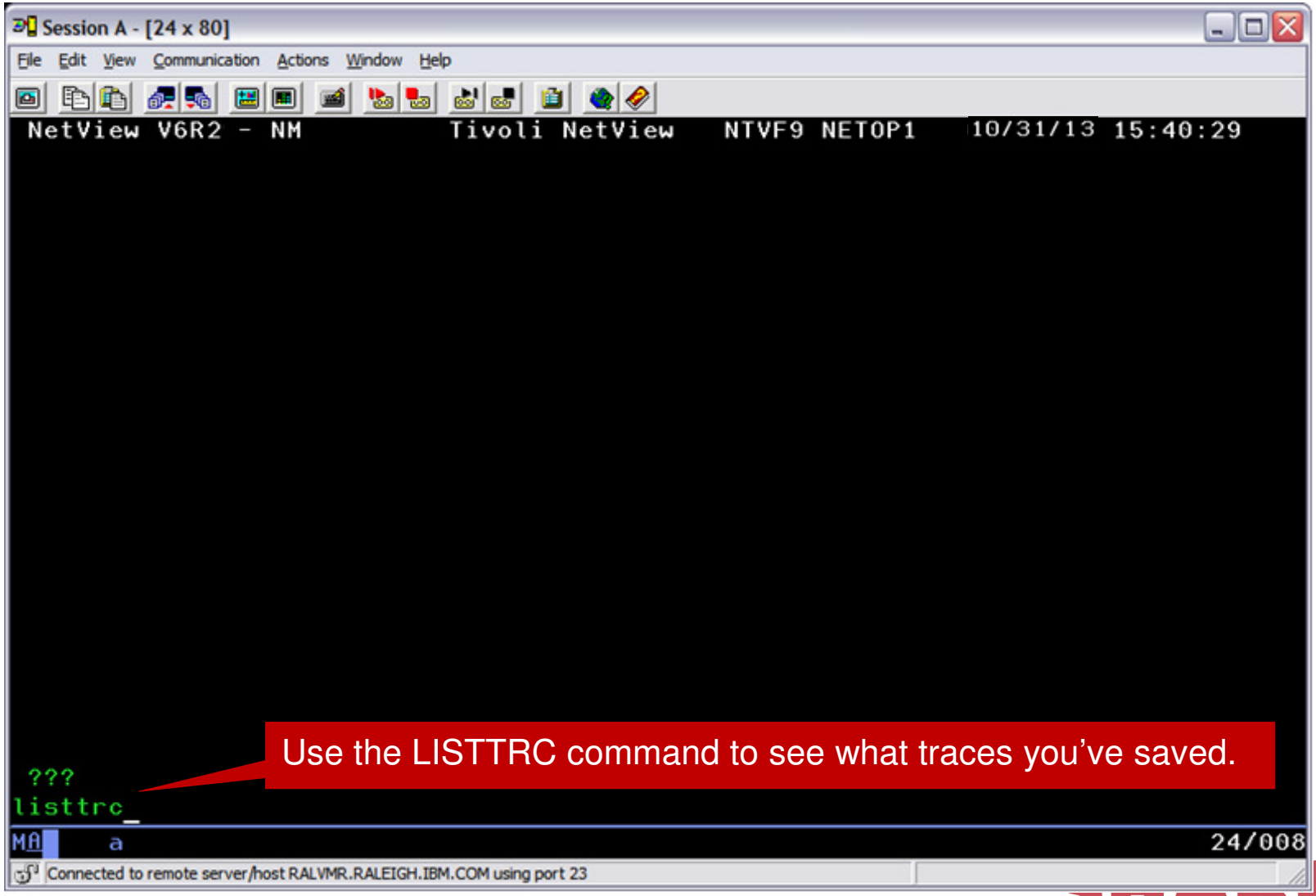
To stop the trace, type "2" and press Enter. Specifying "4" ends the trace and frees the trace records – be sure you're done.

Scenario 1: Packet Trace



For the connection we've selected, several actions are available.

Scenario 1: Packet Trace



Monitoring Sysplex Distributor – Sample Scenarios

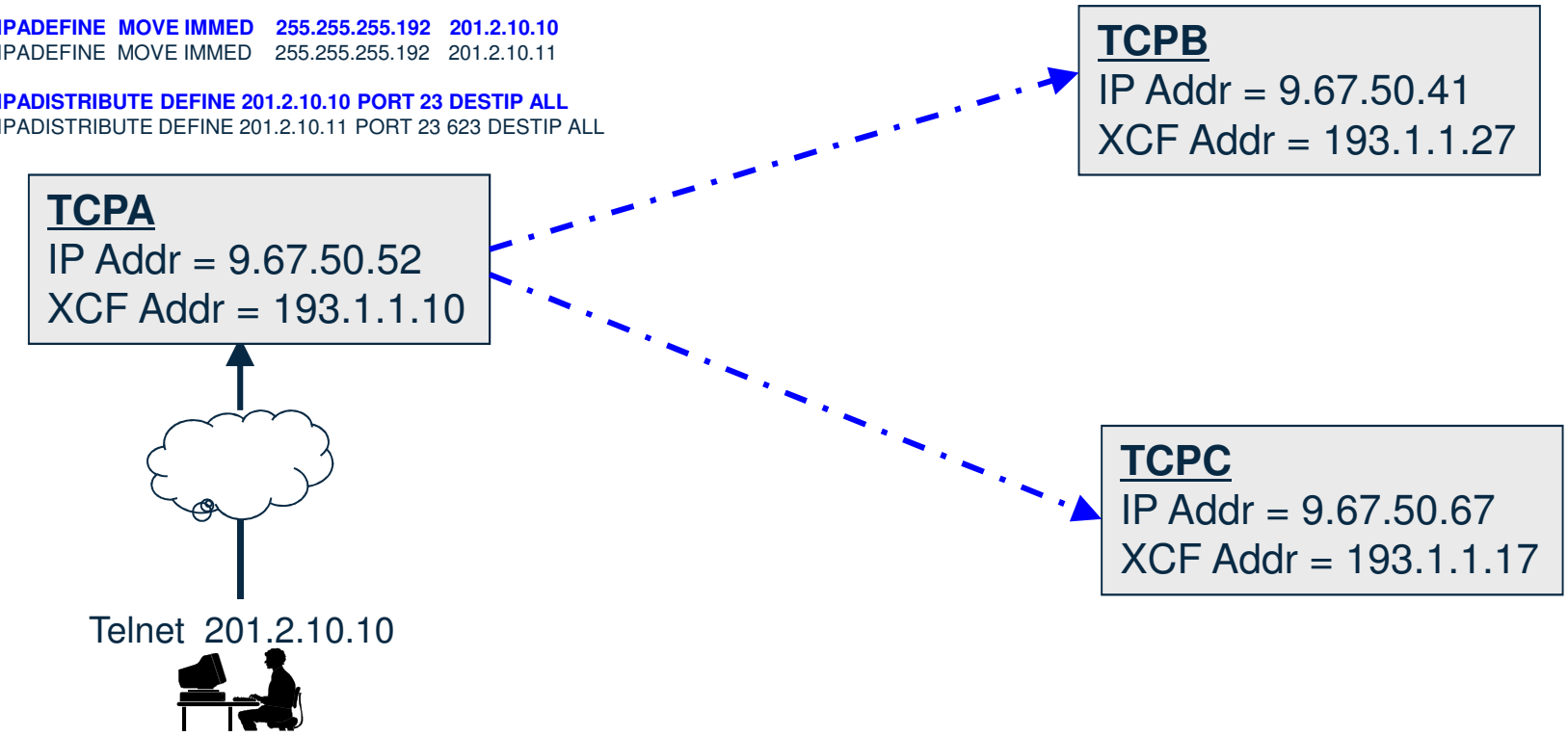
- ***Sysplex Distributor seems to be favoring one z/OS System significantly more than others for new TCP connections? Why is that?***

- Help desk is receiving calls indicating performance issues using an application that is distributed via Sysplex Distributor. You want to understand how TCP connections have been distributed for given Distributed DVIPA over the past 30 minutes.

DVIPA and DDVIPA

VIPADEFINE MOVE IMMED 255.255.255.192 201.2.10.10
VIPADEFINE MOVE IMMED 255.255.255.192 201.2.10.11

VIPADISTRIBUTE DEFINE 201.2.10.10 PORT 23 DESTIP ALL
VIPADISTRIBUTE DEFINE 201.2.10.11 PORT 23 623 DESTIP ALL



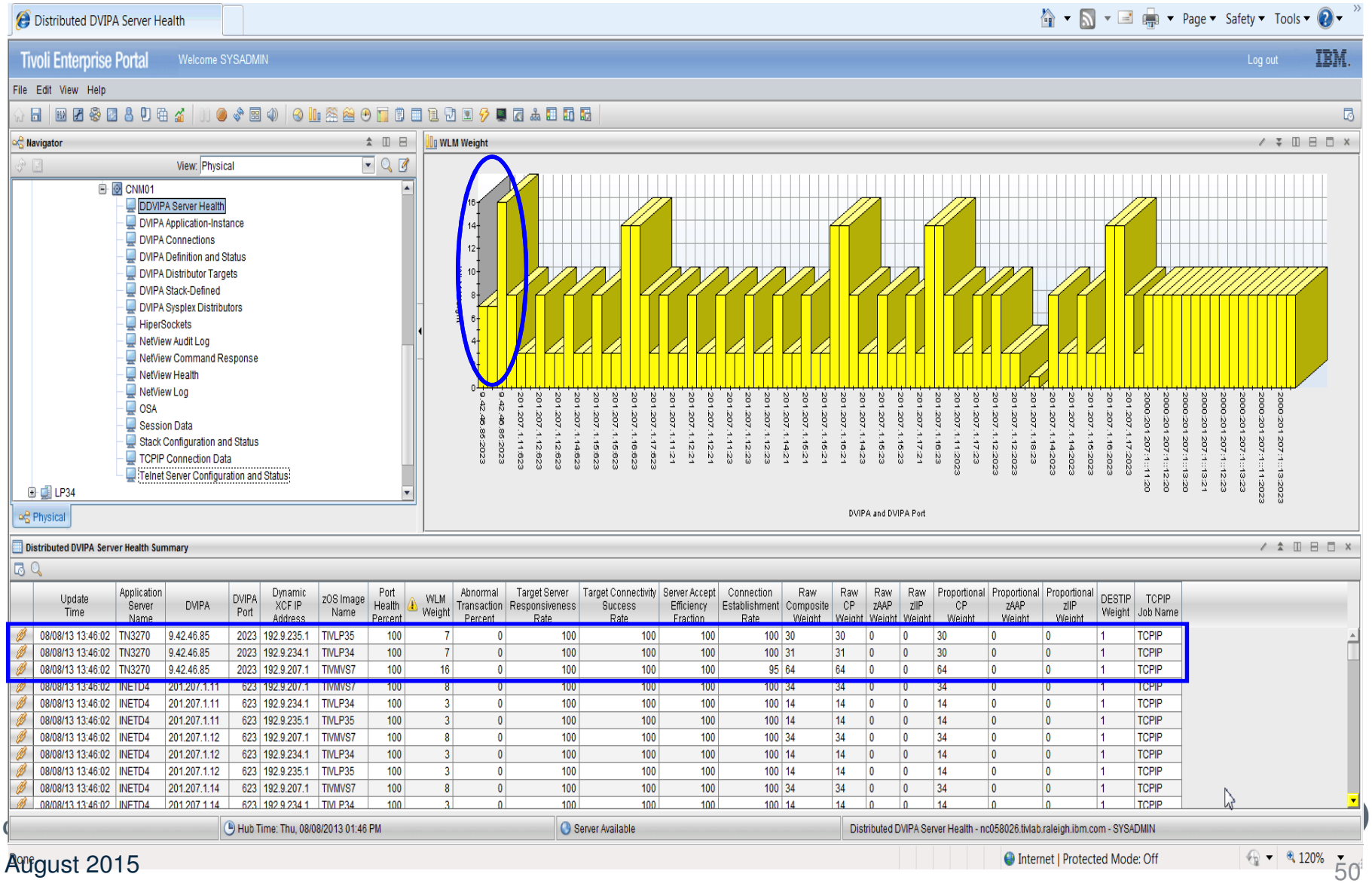
User requests a session with IP address of 201.2.10.10.

The request will come into stack TCPA as the active owner of the DVIPA based on the **VIPADEFINE** statement. The session will be distributed (routed) to any of TCPA, TCPC or TCPC, based on the **VIPADISTRIBUTE** statement.

Scenario 2: Sysplex Distributor Favoring a System

- The NetView DDVIPA Server Health workspace displays the WLM weight for DDVIPA targets. WLM weight is a key metric for DDVIPA connection distribution.
- Scenario information:
  - DVIPA 9.42.46.85 on port 2023

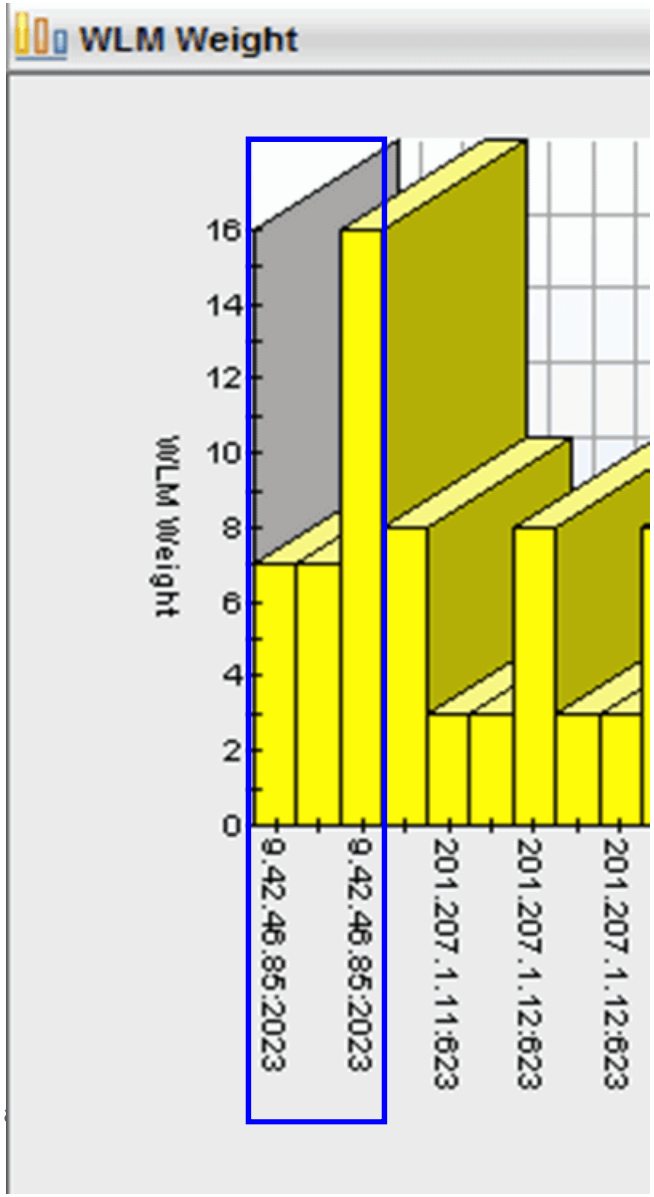
Scenario 2: WLM Weight and DDVIPA Server Health



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	Raw zIIP Weight	Proportional CP Weight	Proportional zAAP Weight	Proportional zIIP Weight	DESTIP Weight	TCPIP Job Name
08/08/13 13:46:02	TN3270	9.42.46.85	2023	192.9.235.1	TIVLP35	100	7	0	100	100	100	100	30	30	0	0	30	0	0	1	TCPIP
08/08/13 13:46:02	TN3270	9.42.46.85	2023	192.9.234.1	TIVLP34	100	7	0	100	100	100	100	31	31	0	0	30	0	0	1	TCPIP
08/08/13 13:46:02	TN3270	9.42.46.85	2023	192.9.207.1	TIVMVS7	100	16	0	100	100	100	95	64	64	0	0	64	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.11	623	192.9.207.1	TIVMVS7	100	8	0	100	100	100	100	34	34	0	0	34	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.11	623	192.9.234.1	TIVLP34	100	3	0	100	100	100	100	14	14	0	0	14	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.11	623	192.9.235.1	TIVLP35	100	3	0	100	100	100	100	14	14	0	0	14	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.12	623	192.9.207.1	TIVMVS7	100	8	0	100	100	100	100	34	34	0	0	34	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.12	623	192.9.234.1	TIVLP34	100	3	0	100	100	100	100	14	14	0	0	14	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.12	623	192.9.235.1	TIVLP35	100	3	0	100	100	100	100	14	14	0	0	14	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.14	623	192.9.207.1	TIVMVS7	100	8	0	100	100	100	100	34	34	0	0	34	0	0	1	TCPIP
08/08/13 13:46:02	INETD4	201.207.1.14	623	192.9.234.1	TIVLP34	100	3	0	100	100	100	100	14	14	0	0	14	0	0	1	TCPIP

Scenario 2: WLM Weight Bar Chart

First 3 bars show WLM weight for DVIPA 9.42.45.84 and Port 2023.



Scenario 2: WLM Weight and DDVIPA Server Health

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
TN3270	9.42.46.85	2023	192.9.235.1	TIVLP35	100	7	0	100	100
TN3270	9.42.46.85	2023	192.9.234.1	TIVLP34	100	7	0	100	100
TN3270	9.42.46.85	2023	192.9.207.1	TIVMVS7	100	16	0	100	100

Server Accept Efficiency Fraction	Connection Establishment Rate	Raw Composite Weight	Raw CP Weight	Raw zAAP Weight	Raw zIIP Weight	Proportional CP Weight
100	100	30	30	0	0	30
100	100	31	31	0	0	30
100	95	64	64	0	0	64

WLM Weight for TIVMVS7 (z13) is > double that of TIVLP34 (z10) and TIVLP35 (z10).

Monitoring Sysplex Distributor – Sample Scenarios

- Sysplex Distributor seems to be favoring one z/OS System significantly more than others for new TCP connections? Why is that?

- ***Help desk is receiving calls indicating performance issues using an application that is distributed via Sysplex Distributor. You want to understand how TCP connections have been distributed for given Distributed DVIPA over the past 30 minutes.***

Scenario 3: Application Performance Issues

- Distributed DVIPA Statistics will show you how your DDVIPA connections have been distributed for the application with performance issues for DDVIPA 197.11.211.1 on port 52002.

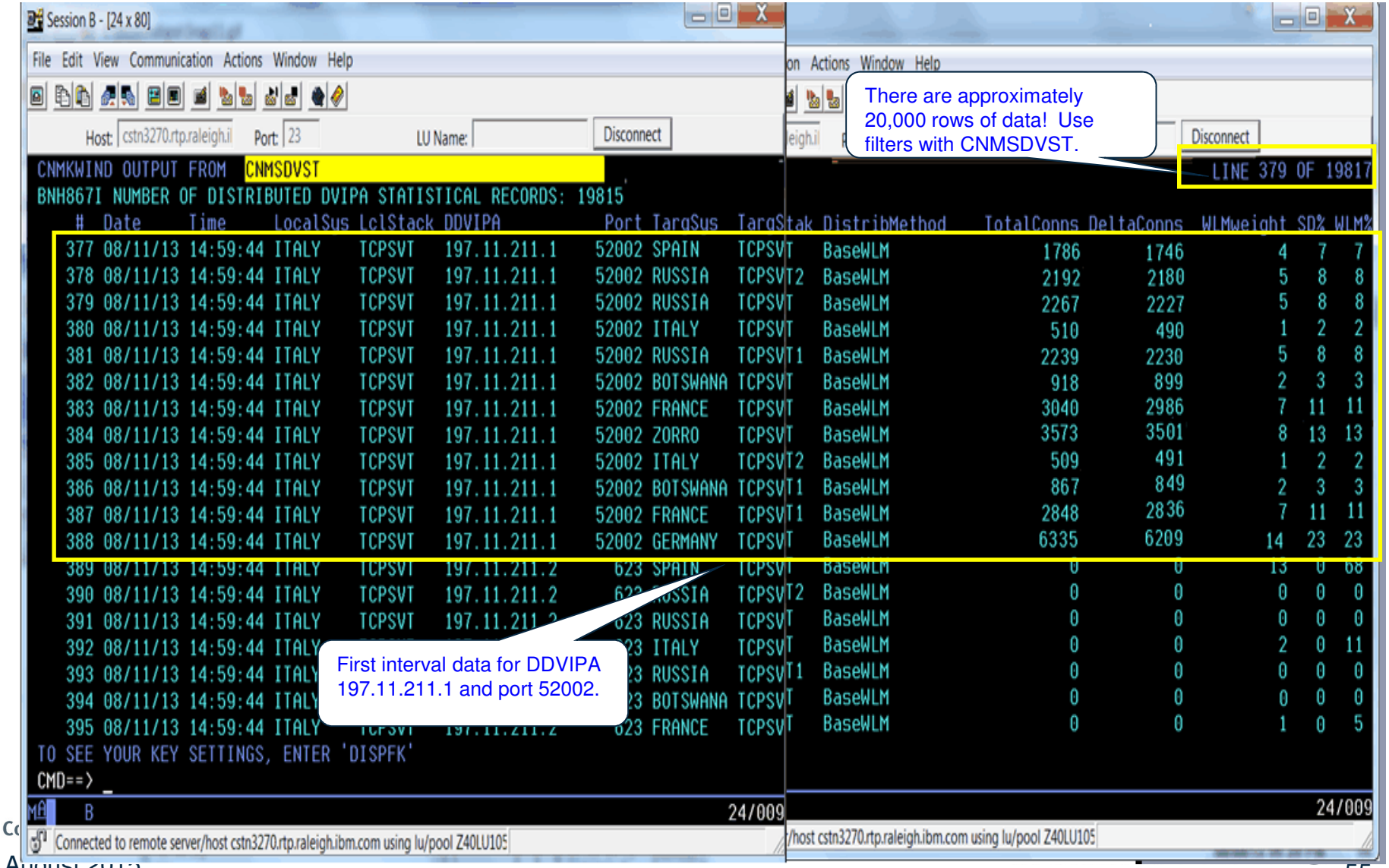
- Scenario information
  - Your DDVIPA sampling interval is 5 minutes (DVIPA.DVTAD tower)
  - DDVIPA Statistics is enabled and started across all systems in your sysplex
    - If not started, start it dynamically with the **DVIPALOG** command and filters, as desired
  - Once the next sampling interval passes, issue NetView sample command: **CNMSDVST**

    or

    wait for 30 minutes and issue:

    CNMSDVST DVIPA=197.11.211.1 PORT=52002 and scroll through the output.

Scenario 3: CNMSDVST output

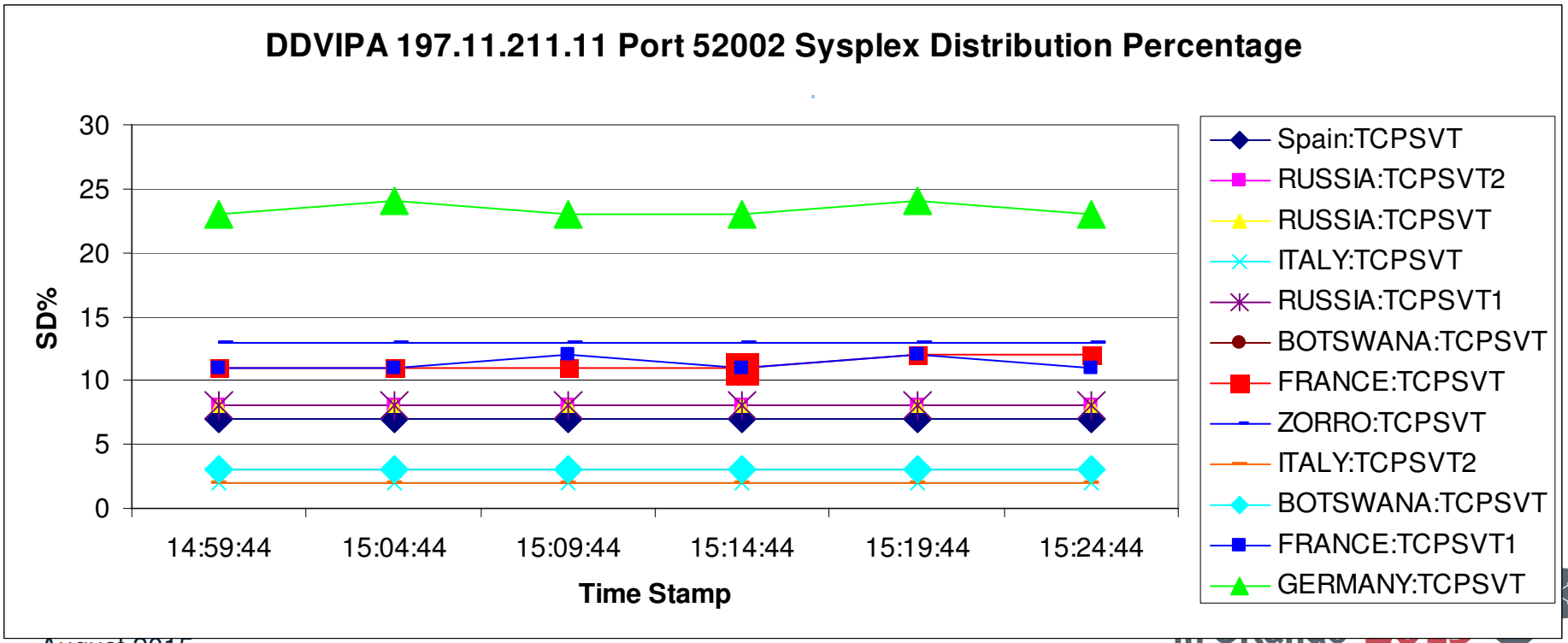


Scenario 3: DDVIPA Sysplex Distribution Percentage

Using the data from DDVIPA Statistics, you can track DDVIPA connection distribution. The graph below maps the Sysplex Distributor Connection Information provided by DDVIPA Statistics over 30 minutes.

- NetView for z/OS does not provide this function.

For our scenario, the connections are being distributed consistently across all target stacks. However, there is a wide disparity in the number of connections per stack.



Summary

- NetView for z/OS provides:
  - An extensive set of tools for managing complex networks and systems from a single point of control
  - Advanced automation facilities for network events
  - A set of user interfaces to meet your needs and management functions that work with other products to provide a complete picture of your networks and systems

Backup

Questions and Answers

Questions and Answers

- TCP Connections
  - **Q**: What needs to be enabled for this function?
  - **A**: TCPIPCOLLECT tower and TOWER.TCPIPCOLLECT = TCPCONN subtower
    - Enabled by default

Questions and Answers cont.

- Intrusion Detection (IDS)
  - Q: What does NetView do differently than z/OS MF related to this function?
  - A: Confirmed with z/OS Communications Server team that their IDS policy can be configured using the z/OS MF Configuration Assistant. There is no monitoring/automation done by z/OS MF. NetView provides automation support.
    - To enable NetView Intrusion Detection Automation Services, configure the following CNMSTYLE user statements:

      TOWER = AON

      TOWER.AON = TCP

      TOWER.AON.TCP = IDS

Questions and Answers cont.

- Packet Trace (including scenario)
  - **Q1**: What was the root cause of the problem with the “unacknowledged SYNs”?
  - **A1**: The application at the specified IP address had a limited number of connections it could accept, and that limit had been reached.
  - **Q2**: What’s the maximum size of a concurrent trace instance (used in the scenario)? Where is the trace information stored? Does the stored trace data wrap?
  - **A2**: Each concurrent trace instance is backed by a data space.
    - The default size is 50M – min is 16M - max is 2047M
    - The default is to wrap (specify a negative amount to not wrap, such as: -50M)
    - To change the size and wrap specification, see the STORAGE keyword with the PKTS command or the CNMSTYLE statement:

      PKTS.STORAGE.&CNMTCPN = 50M
    - Note: If you plan to save one or more traces, ensure that you have adequate space to do this. NetView dynamically allocates a data set to save the trace data.
  - **Q3**: Is an “external writer” required?
  - **A3**: No.
  - **Q4**: What needs to be enabled for this function?
  - **A4**: TCPIPCOLLECT tower and TOWER.TCPIPCOLLECT = PKTS subtower (both enabled by default) in CNMSTYLE user member

Questions and Answers cont.

- Discovery Manager
  - **Q1**: What needs to be enabled for this function?
  - **A1**: DISCOVERY tower and any subtowers in CNMSTYLE user member:

    TOWER.DISCOVERY = INTERFACES TELNET

    TOWER.DISCOVERY.INTERFACES = OSA HIPERSOCKETS
  - **Q2:** How can I get this data programmatically without issuing commands that write lots of information to the TCPIP job log?
  - **A2:** Use the following NetView commands (samples are in parentheses) and issue OVERRIDE SLOGCMDR=NO command for pertinent autotasks to not log MVS command output to SYSLOG :
    - **STACSTAT (CNMSTAC): Configuration and status information about TCP/IP stacks**
    - **IFSTAT (CNMSIFST): TCP/IP stack interfaces**
    - **TELNSTAT (CNMSTNST): Configuration and status information about Telnet servers**
    - **TNPTSTAT (CNMSTPST): Configuration and status information about Telnet server ports**
    - **NVSTAT (CNMSNVST): Configuration and status information about the NetView domains**
    - **OSAPORT (CNMSOSAP): OSA channel and port information**
    - **HIPERSOC (CNMSHIPR): View HiperSockets adapter information**

Questions and Answers cont.

- DVIPA
  - **Q1**: What needs to be enabled for this function?
  - **A1**: DVIPA tower and any subtowers in CNMSTYLE user member:
    TOWER.DVIPA = DVTAD DVCONN DVROUT
  - **Q2:** How can I get this data programmatically without issuing commands that write lots of information to the TCPIP job log?
  - **A2:** Use the following NetView commands (samples are in parentheses) and issue OVERRIDE SLOGCMDR=NO command for pertinent autotasks to not log MVS command output to SYSLOG :
    - **DVIPSTAT (CNMSDVIP): Definition and status information about DVIPAs**
    - **DVIPPLEX (CNMSPLEX): Information about DVIPA sysplex distributors**
    - **DVIPCONN (CNMSDVPC): DVIPA connections**
    - **DVIPTARG (CNMSTARG): DVIPA distributed targets**
    - **DVIPHLTH (CNMSDVPH): Distributed DVIPA server health information**
    - **DVIPDDCR (CNMSDDCR): Distributed DVIPA connection routing information**
    - **VIPAROUT (CNMSVPRT): Status information about VIPA routes**

Questions and Answers cont.

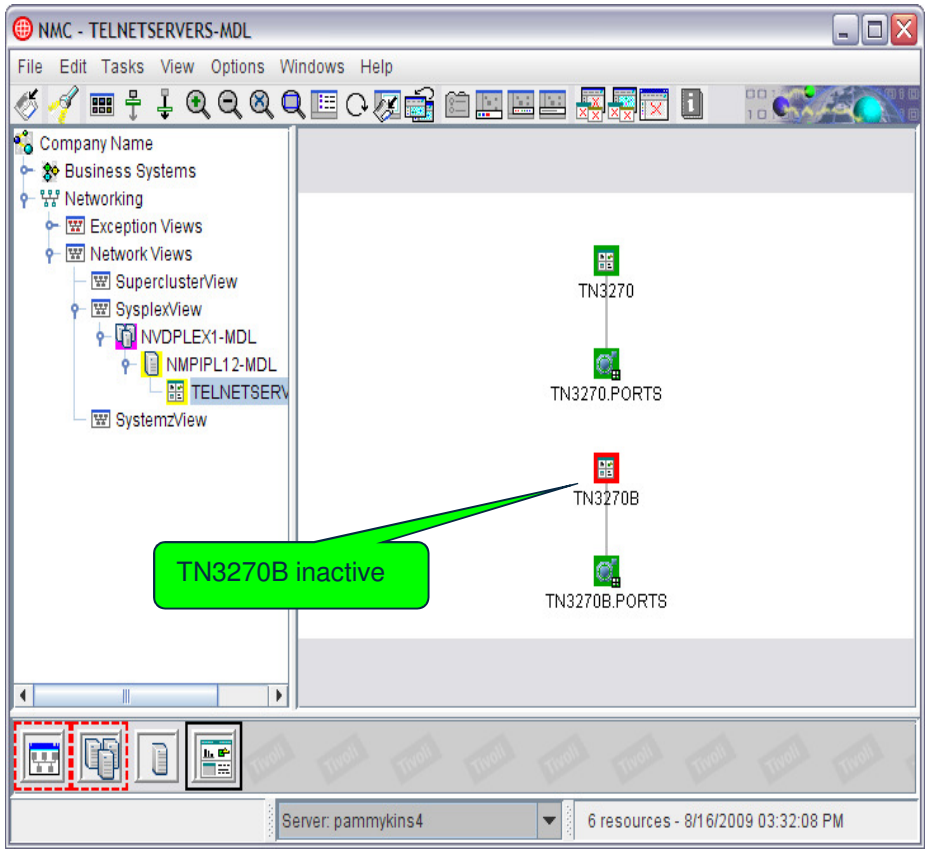
- DVIPA Q&A cont.
  - **Q3**: Are there additional metrics to help with DDVIPA problems?
  - **A3**: Yes.
    - See the NetView DDVIPA Servers workspace (TEP) or the output of the DVIPHLTH (sample CNMSDVPH) command (message BNH814I)
    - Also see Scenario 6 in this section.
      - The root cause for this scenario is that the server's ability to accept connections is very low.

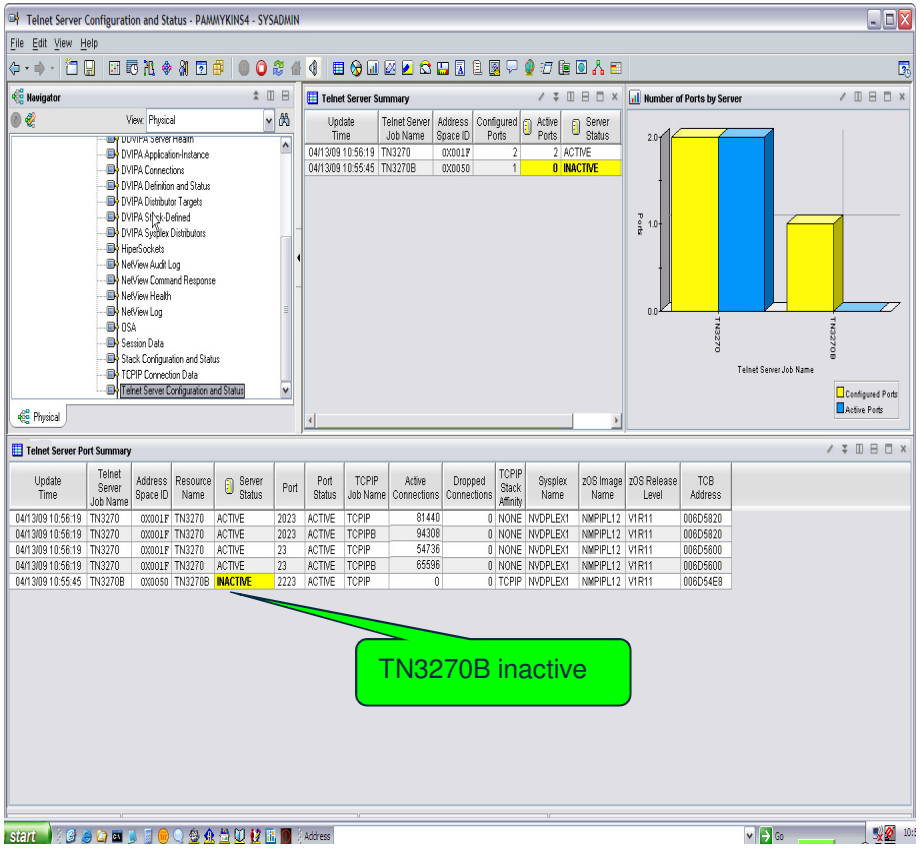
Additional Scenarios

Scenario 4: Diagnosing Telnet Server Outage

- A user reports that they can no longer establish Telnet connections to Telnet server TN3270B
- The operator looks at the Telnet Server Configuration and Status workspace and notices that TN3270B is inactive
- The operator restarts the server and monitors that connections are once again being established

Scenario 4: Telnet Server Inactive

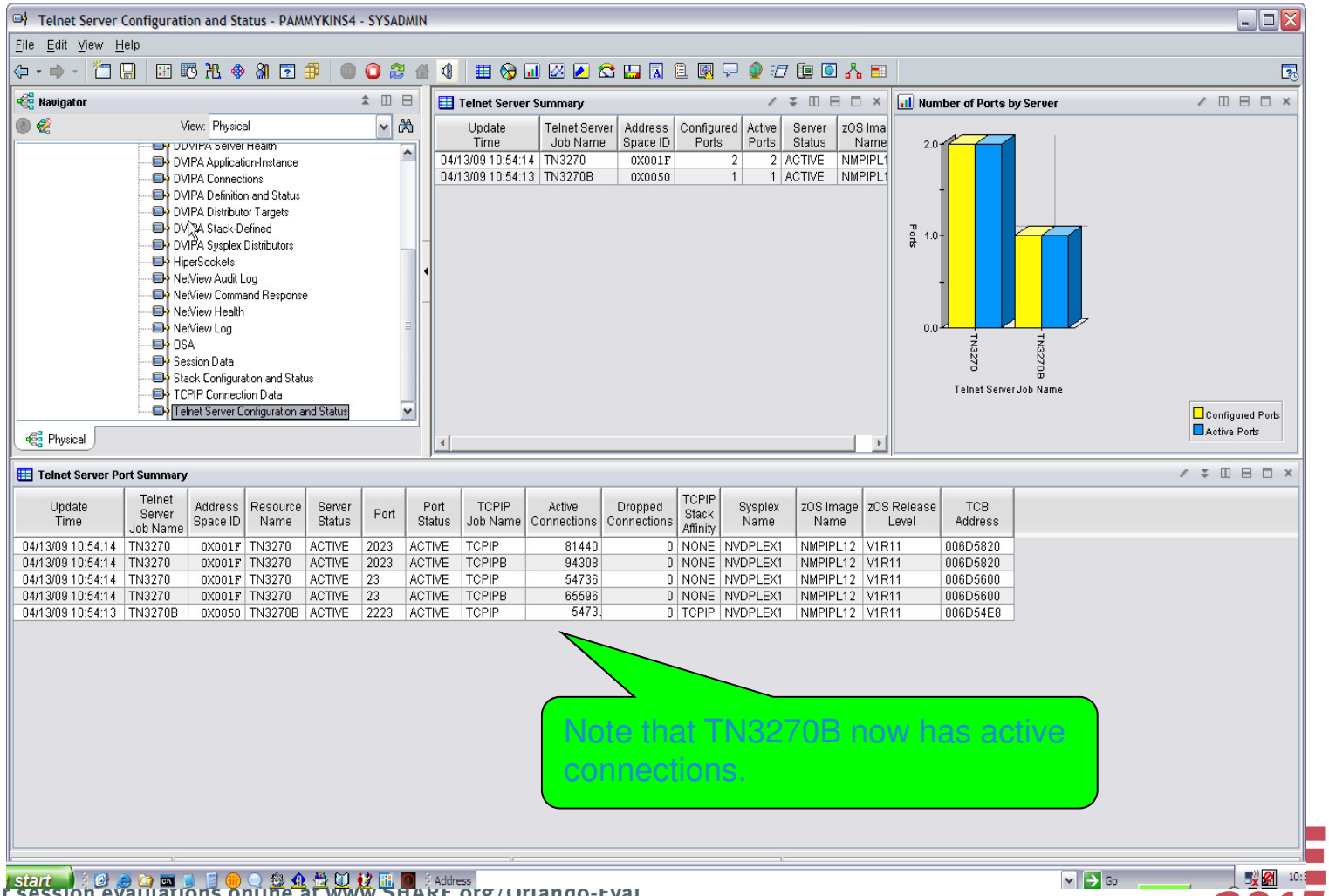





```
CNMKWIND OUTPUT FROM CNMSTNST                          LINE 0 OF 3
*------------------------------ Top of Data ------------------------------*
BNH496I NUMBER OF TELNET SERVERS: 1
 #   Telnet Server ASID Status   Config-ports Active-ports System-name
1    TN3270        001E ACTIVE   2            2            NMPIPL12
*---------------------------- Bottom of Data -----------------------------*
```

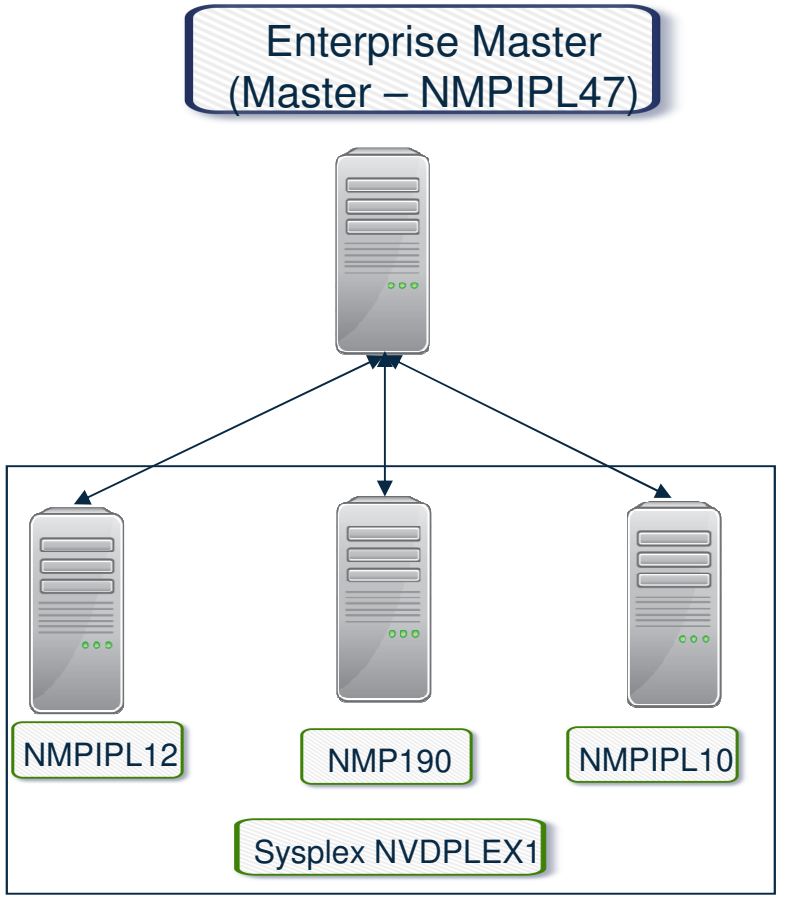
TN3270B not present when inactive

Scenario 4: Telnet server now active

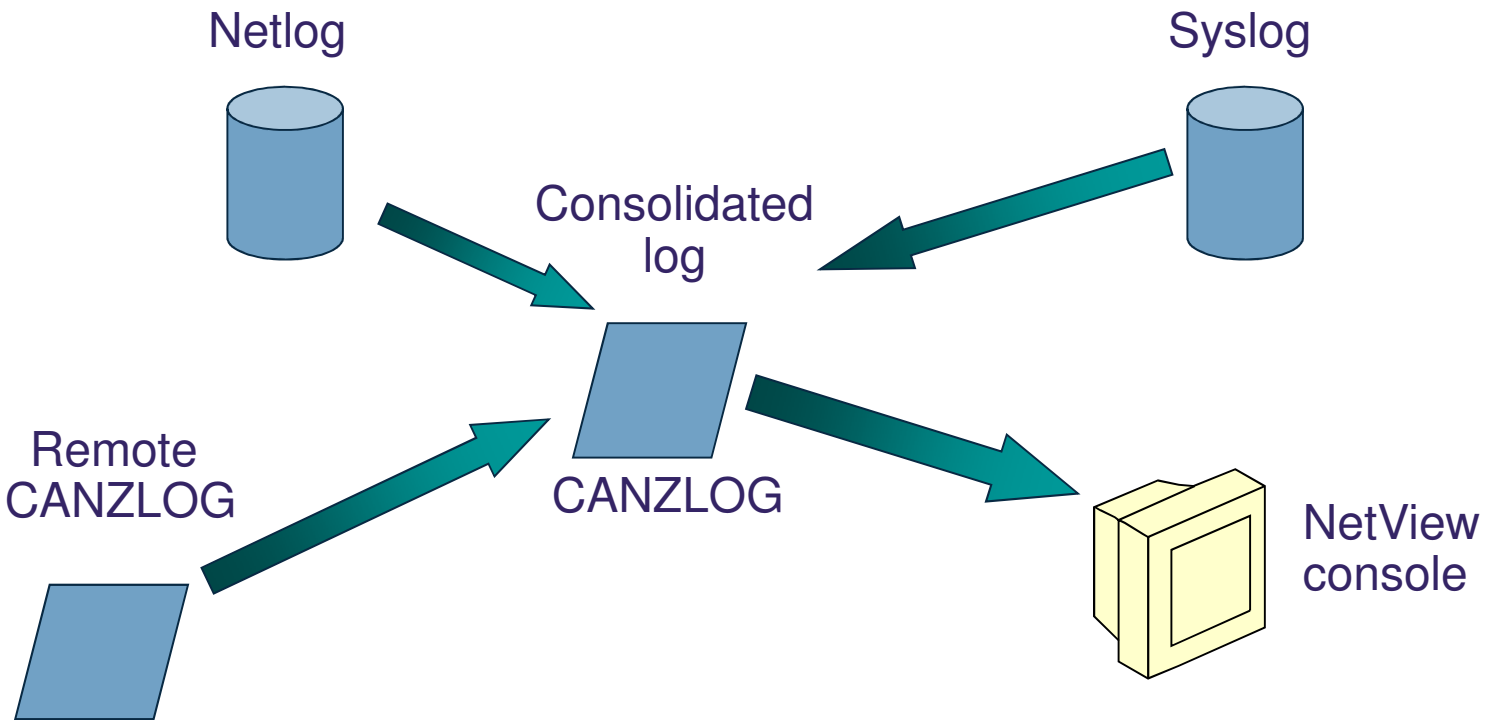


Scenario 5: DDVIPA Configuration Changes

- Scenario:
  - All 3 systems in PLEX1 need to add a Sysplex Distributor. The changes are all scheduled to occur at the same time, but 2 of the new Sysplex Distributor IP addresses are not working.
- Resolution steps:
  - Using the Canzlog remote browse GROUP function from an enterprise master NetView, see why the DDVIPA configuration changes did not work on all 3 systems in the sysplex.
  - Also, take advantage of the CZFORMAT option (ORIGIN) and the new relative time filter.



Consolidated Log Browse with NetView V6.2



CANZLOG = **C**onsolidated **A**udit, **N**etView and **z**/OS **LOG**

Canzlog GROUP browse

- The Canzlog BR command can be used to browse a Canzlog from multiple domains
  - The messages from all the domains are consolidated into one log
  - The messages in the log are sorted by time
  - Use the new DEFAULTS/OVERRIDE CZFORMAT command to specify ORIGIN in front of each message
  - Additional filter options can be specified
  - A filter name, if used, is resolved on the local side before making the remote request

Scenario 5: GROUP information

NetView stylesheet:

```
RMTSYN.IP.NTV7A = NMPIPL12.TIVLAB.RALEIGH.IBM.COM/4022 ON USIBMNT
RMTALIAS.NTV7ATST = IP.NTV7A
RMTSYN.IP.NTV74 = NMP190.TIVLAB.RALEIGH.IBM.COM/4022 ON USIBMNT
RMTALIAS.NTV74TST = IP.NTV74
RMTSYN.IP.NTV70 = NMPIPL10.TIVLAB.RALEIGH.IBM.COM/4022 ON USIBMNT
RMTALIAS.NTV70TST = IP.NTV70
RMTSYN.IP.NTVE6 = NMPIPL30.TIVLAB.RALEIGH.IBM.COM/4022 ON USIBMNT
RMTALIAS.NTVE6TST = IP.NTVE6
ENT.GROUP.PLEX1 = NTV7ATST NTV74TST NTV70TST
```

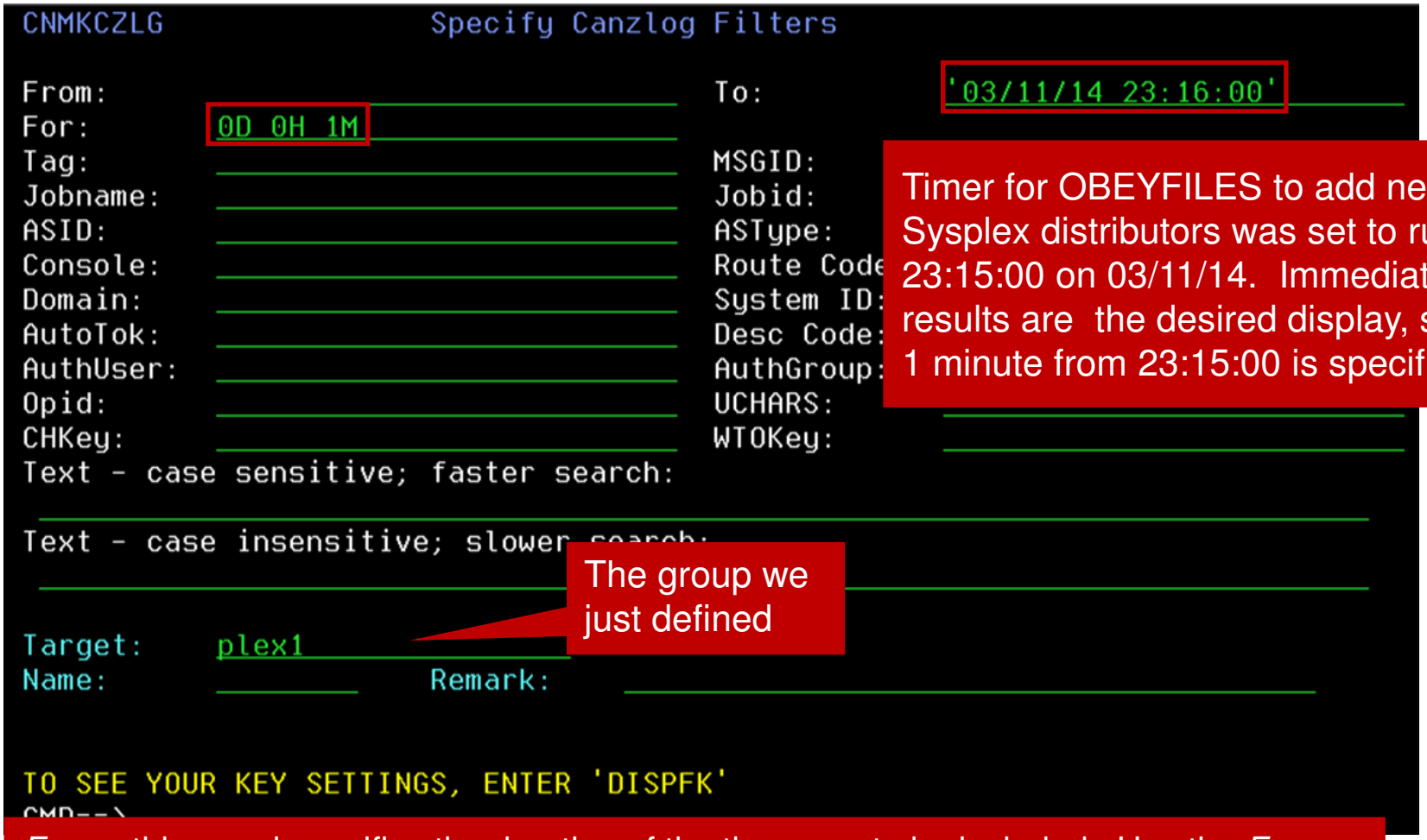
Issue RESTYLE ENT to dynamically add a GROUP.

QRYGROUP Output

```
NetView V6R2 - NM          Tivoli NetView    NTVAF NETOP1
* NTVAF     QRYGROUP
C NTVAF
CNM100I The list of groups stored in COMMON
PLEX1
* NTVAF     QRYGROUP PLEX1
C NTVAF
CNM100I The list of members stored in PLEX1
NTV7ATST
NTV70TST
NTV74TST
```

ENT.GROUP.groupname defines a group of local or remote NetView instances. You can use a group to define a logical cluster of NetView instances; you can then use the group with the BROWSE command to see data from all NetView instances in the cluster. A group can include specific NetView domains, sysplexes, and other groups.

Scenario 5: Relative Time

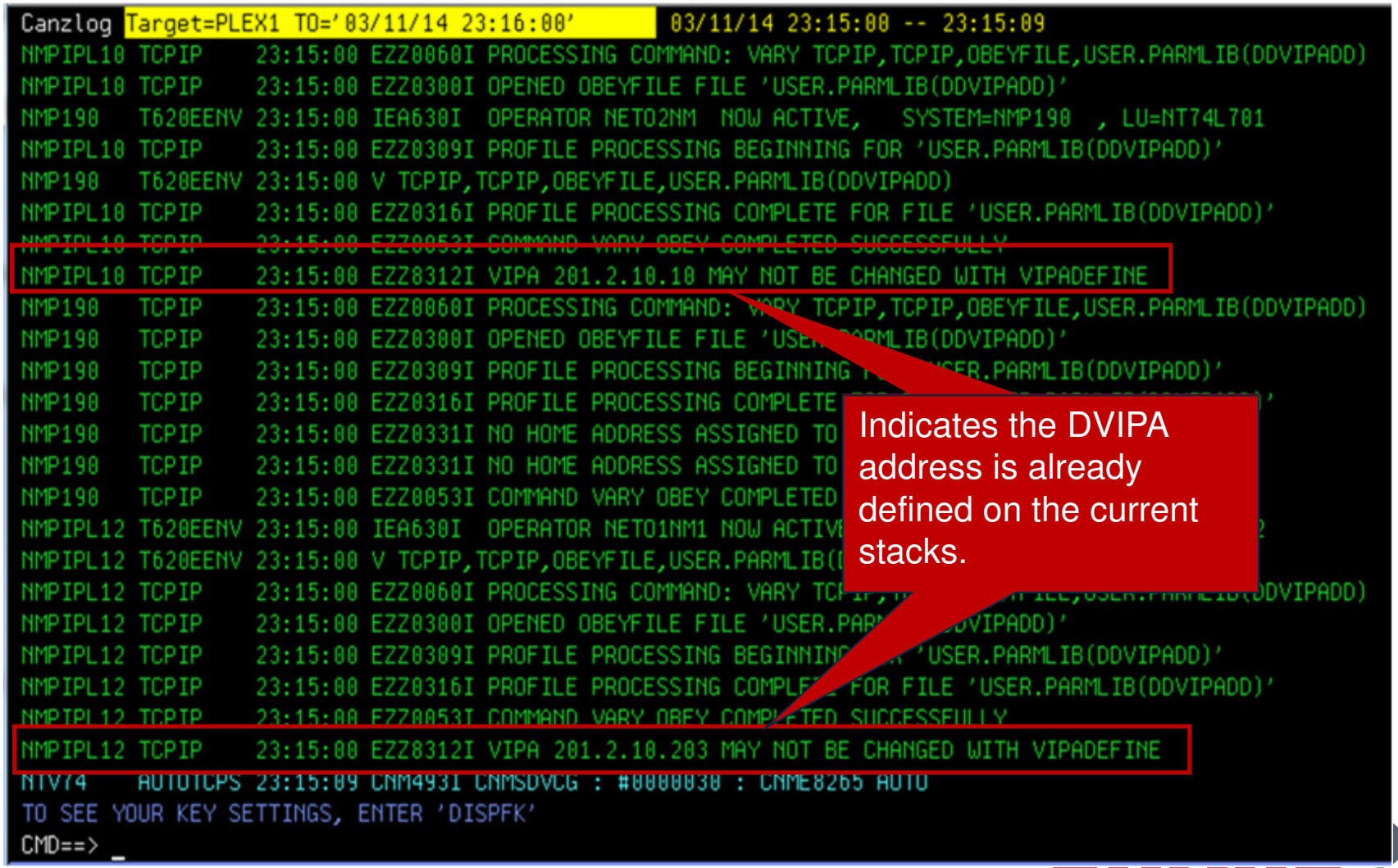


Timer for OBEYFILES to add new Sysplex distributors was set to run at 23:15:00 on 03/11/14. Immediate results are the desired display, so only 1 minute from 23:15:00 is specified.

The group we just defined

For on this panel specifies the duration of the timespan to be included. Use the *For* field if you want to specify the timespan in terms of duration, rather than specifying the the start and end times.

Scenario 5: Filtered Results

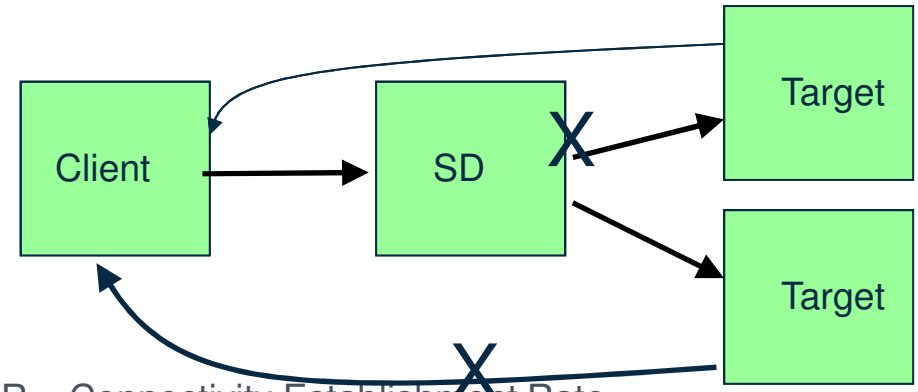


Scenario 6: Sysplex Distributor Health Notifications

- NetView provides situations with the NetView Agent.
  - Disabled by default
  - “Shipped” situations can be customized
  - New situations can be created
- Scenario information:
  - Operator has 3 open situations on the TEP for Distributed DVIPAs for domain CNMZO related to DDVIPA Server Health
    - Server Accept Efficiency Fraction (SEF) < 70%
      - Created for this scenario
    - Target Server Responsiveness Rate (TSR) < 80%
    - WLM Weight = 0
  - Looking at the Navigator Tree, LPAR ZOR, shows the situation icon, so we’ll start there.
  - We also have a DDVIPA Unhealthy Servers workspace
    - Let’s look at that

Sysplex Distributor built-in awareness of abnormal conditions

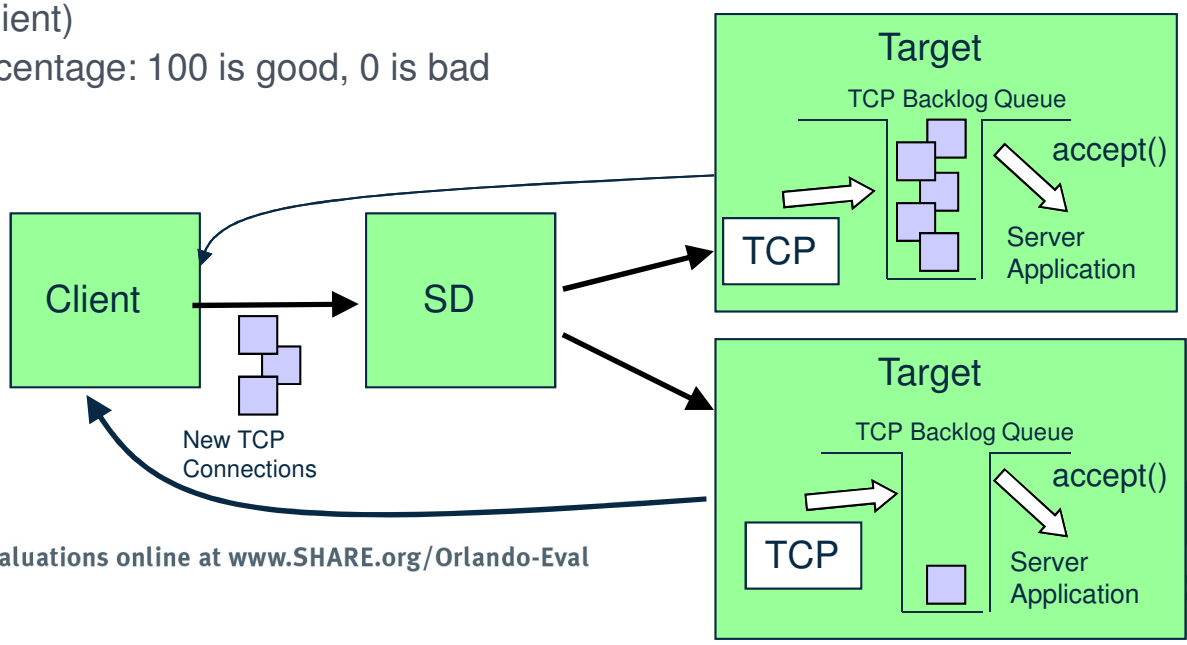
- TSR – Target Server Responsiveness
  - How healthy is the target system and application from an SD perspective? A percentage, 0-100%
  - Comprised of several individual health metrics:
    - TCSR – Target Connectivity Success Rate
    - Are connections being sent to the Target System making it there?
    - A Percentage: 100 is good, 0 is bad



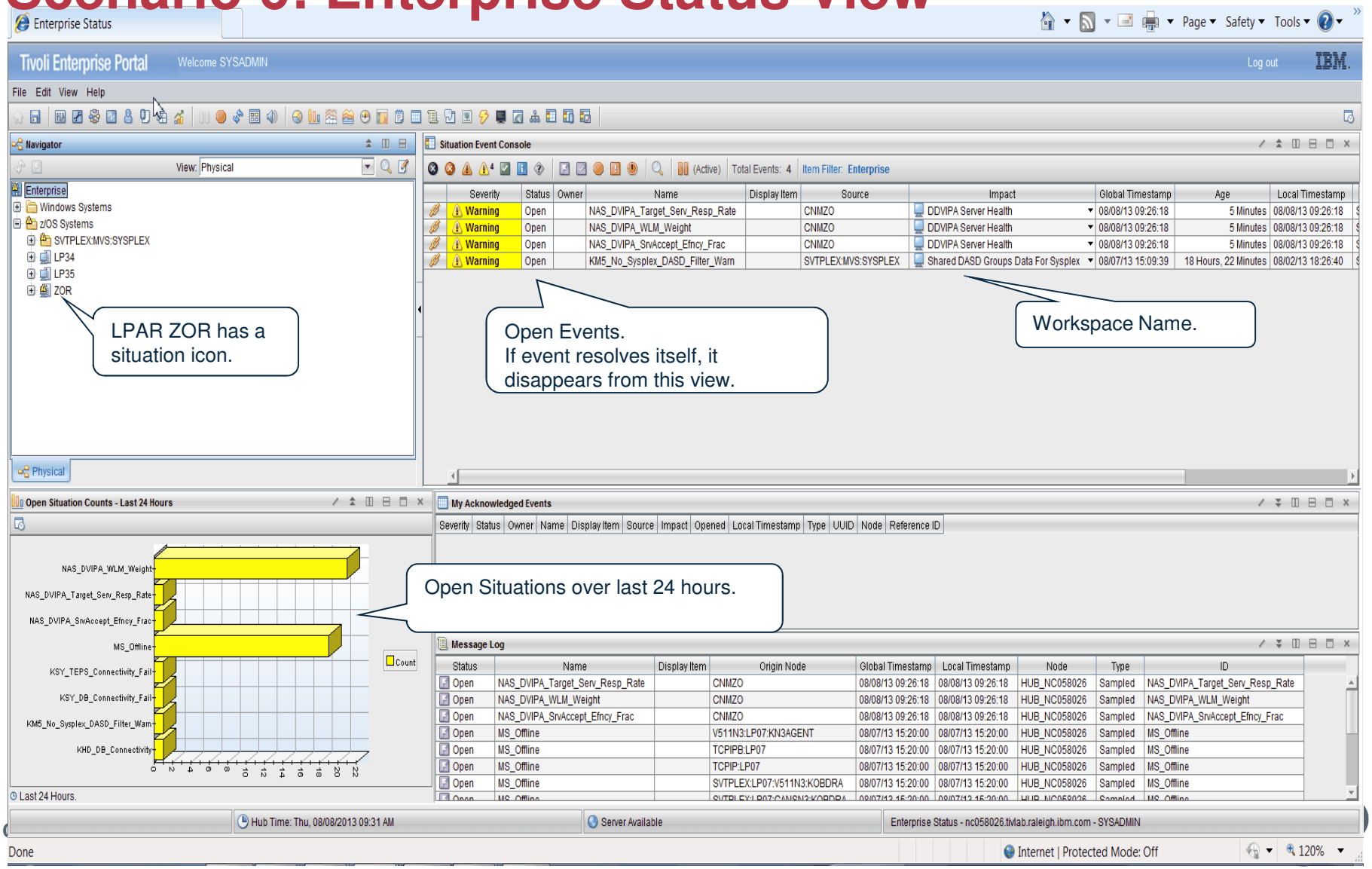
    - CER – Connectivity Establishment Rate
    - Is connectivity between the target system and the client ok?
    - By monitoring TCP Connection Establishment state (requires 3 way handshake between client and server) we can detect whether a connectivity issue exists
    - A percentage: 100 is good, 0 is bad
    - Note: CER no longer part of TSR directly but is included in SEF and continues to be calculated and reported separately

Sysplex Distributor built-in awareness of abnormal conditions

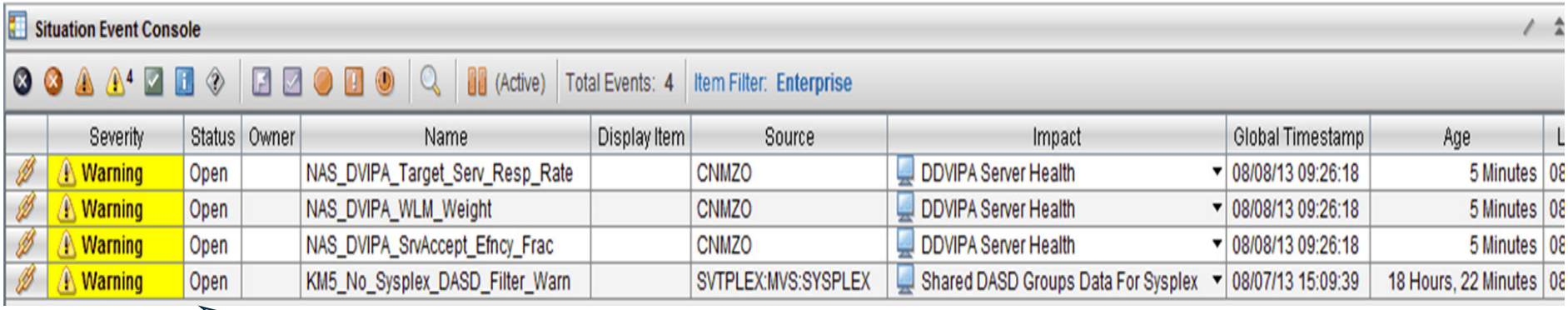
- TSR – Target Server Responsiveness (cont)
  - SEF – Server Efficiency Fraction
  - Is the target server application server keeping up with new connections in its backlog queue?
    - » Is the new connection arrival rate higher than the application accept rate? (i.e. is backlog growing over time)
    - » How many connections in the TCP backlog queue? How close to maximum backlog queue depth? Did we have to drop any new connections because the backlog queue max was exceeded?
    - » Is the server application hung? (i.e. not accepting any connections)
    - » Are the number of half-open connections on the backlog queue growing? (Similar to CER – One such scenario is when the target system does not have network connectivity to the client)
  - A Percentage: 100 is good, 0 is bad



Scenario 6: Enterprise Status View



Scenario 6: Situation Event Console

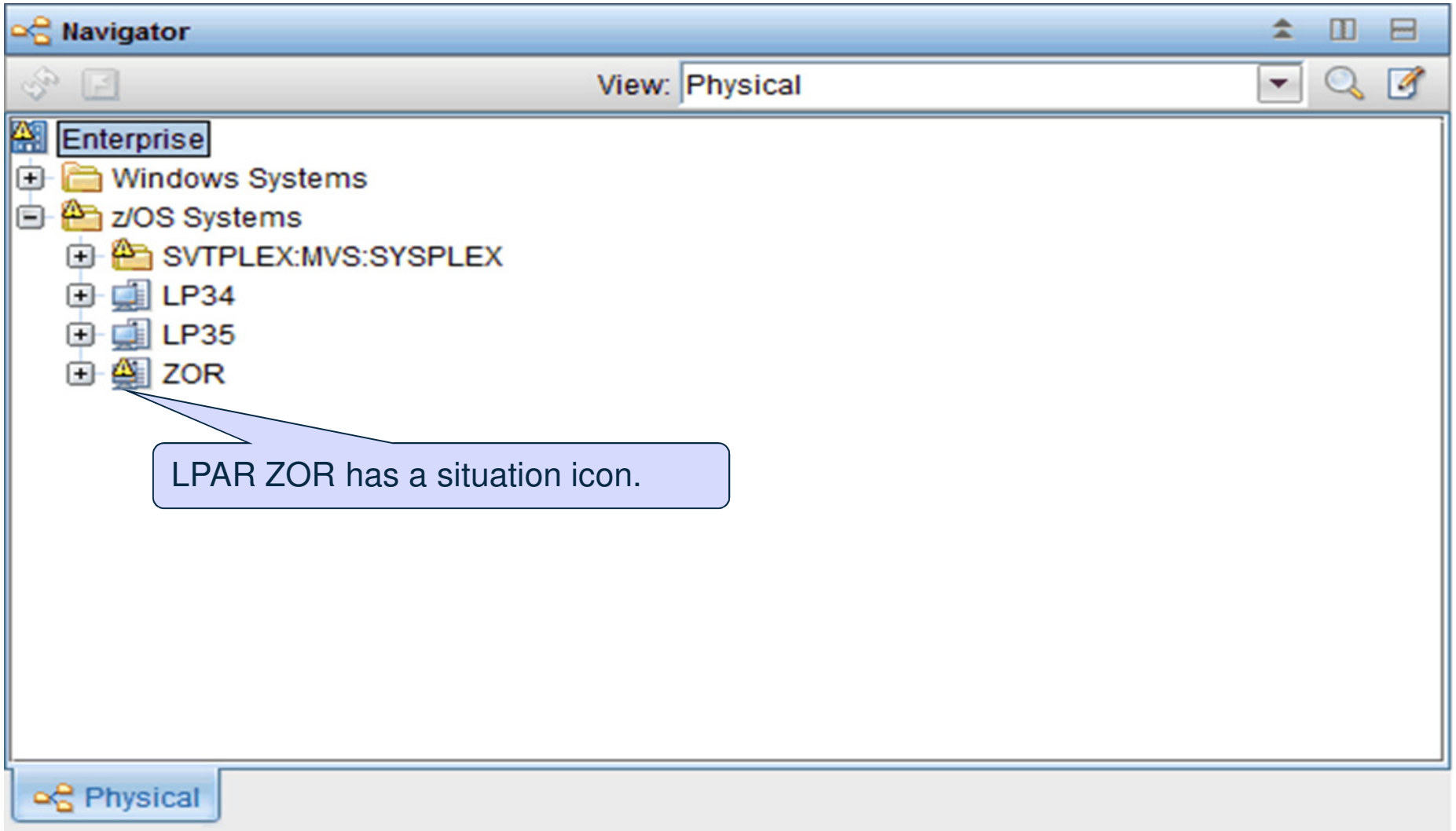


	Severity	Status	Owner	Name	Display Item	Source	Impact	Global Timestamp	Age	L
	Warning	Open		NAS_DVIPA_Target_Serv_Resp_Rate		CNMZO	DDVIPA Server Health	08/08/13 09:26:18	5 Minutes	08
	Warning	Open		NAS_DVIPA_WLM_Weight		CNMZO	DDVIPA Server Health	08/08/13 09:26:18	5 Minutes	08
	Warning	Open		NAS_DVIPA_SrvAccept_Efncy_Frac		CNMZO	DDVIPA Server Health	08/08/13 09:26:18	5 Minutes	08
	Warning	Open		KM5_No_Sysplex_DASD_Filter_Warn		SVTPLEX:MVS:SYSPLEX	Shared DASD Groups Data For Sysplex	08/07/13 15:09:39	18 Hours, 22 Minutes	08

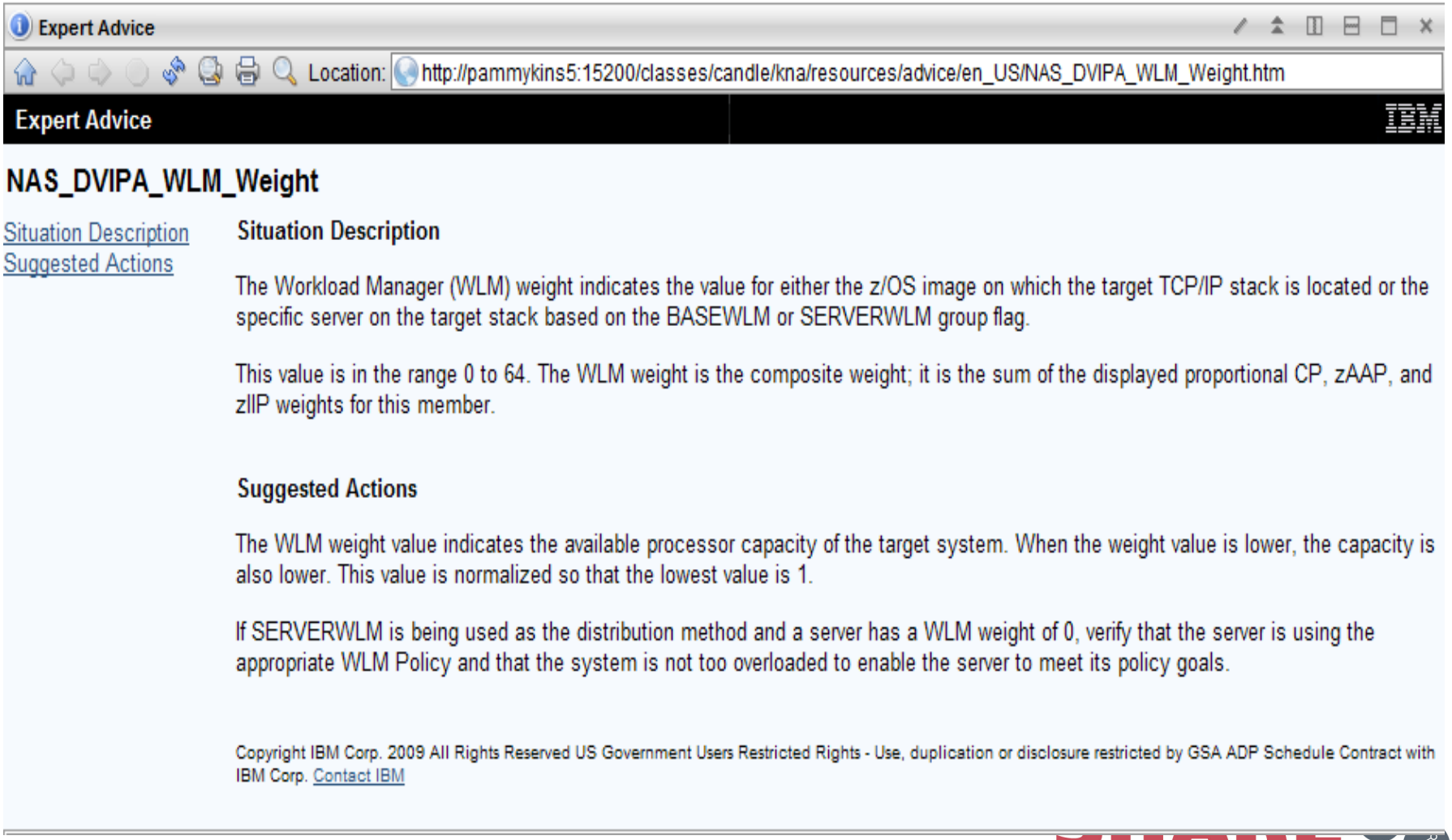
Open Events.
If event resolves itself, it disappears from this view.

Workspace Name.

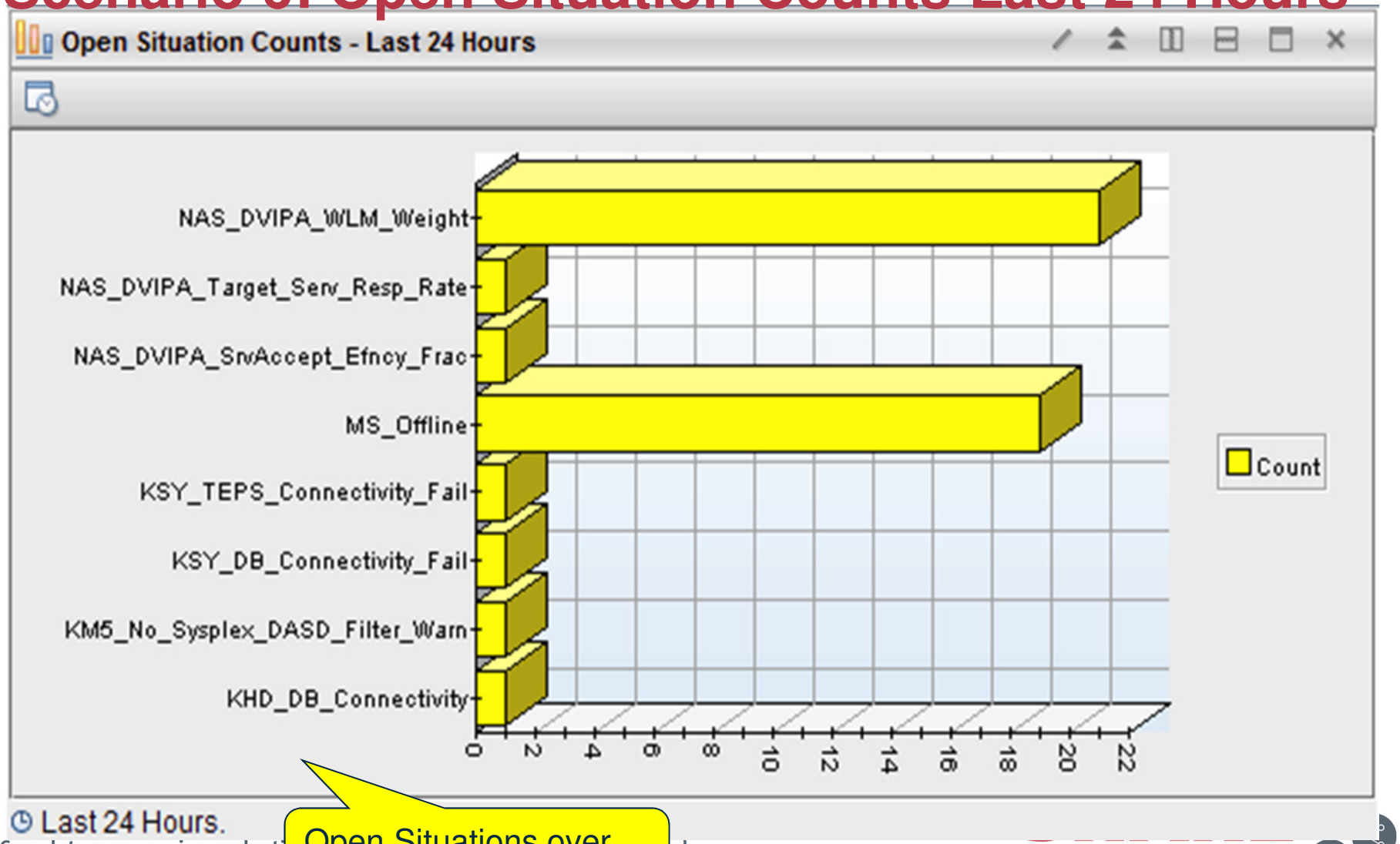
Scenario 6: Enterprise Status View



Scenario 6: WLM Weight = 0 Suggested Actions

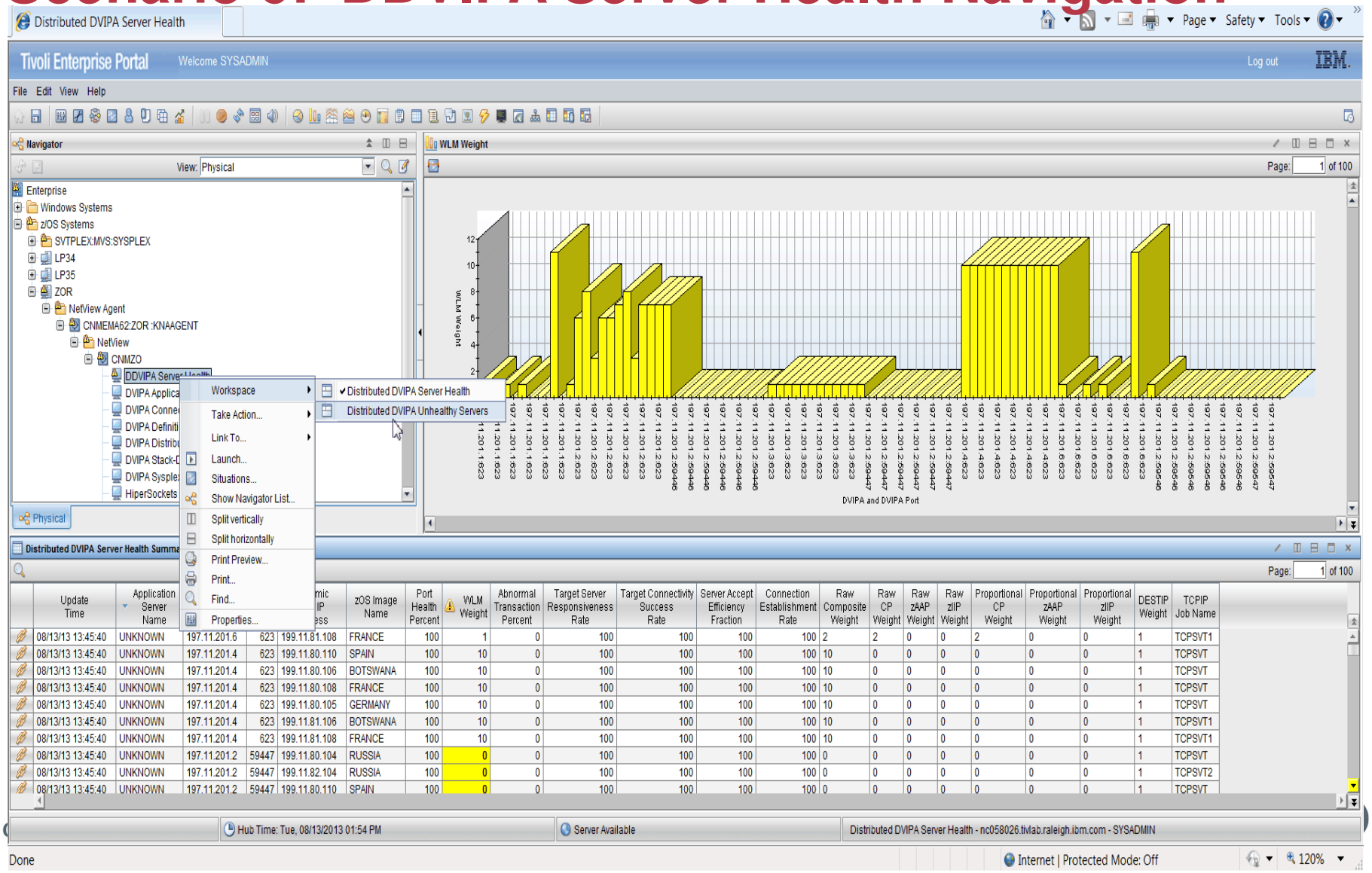


Scenario 6: Open Situation Counts Last 24 Hours

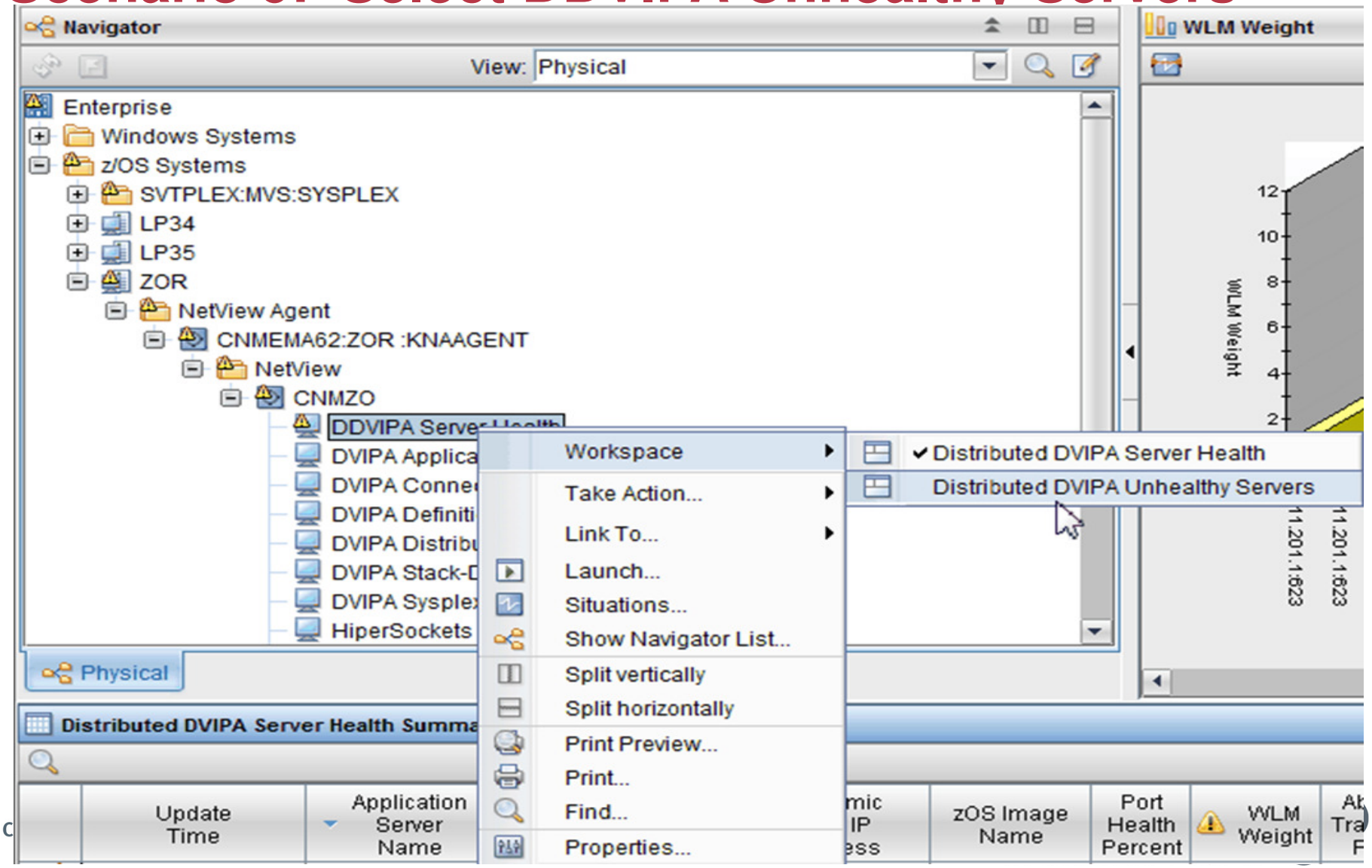


Open Situations over last 24 hours.

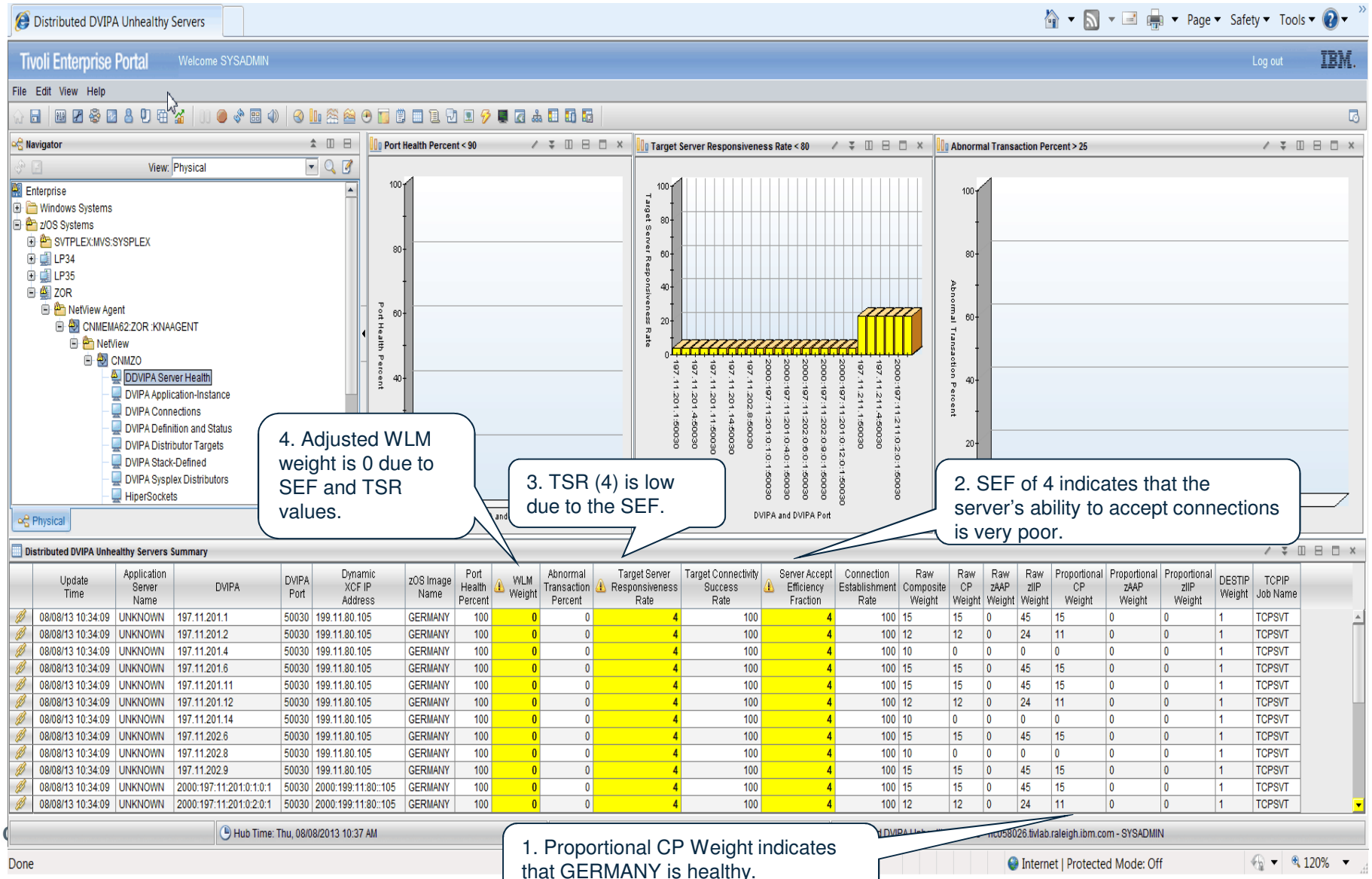
Scenario 6: DDVIPA Server Health Navigation



Scenario 6: Select DDVIPA Unhealthy Servers



Scenario 6: DDVIPA Unhealthy Servers



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	Raw zIIP Weight	Proportional CP Weight	Proportional zAAP Weight	Proportional zIIP Weight	DESTIP Weight	TCPIP Job Name
08/08/13 10:34:09	UNKNOWN	197.11.201.1	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	15	15	0	45	15	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.201.2	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	12	12	0	24	11	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.201.4	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	10	0	0	0	0	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.201.6	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	15	15	0	45	15	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.201.11	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	15	15	0	45	15	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.201.12	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	12	12	0	24	11	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.201.14	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	10	0	0	0	0	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.202.6	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	15	15	0	45	15	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.202.8	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	10	0	0	0	0	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	197.11.202.9	50030	199.11.80.105	GERMANY	100	0	0	4	100	4	100	15	15	0	45	15	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	2000:197:11:201:0:1:0:1	50030	2000:199:11:80::105	GERMANY	100	0	0	4	100	4	100	15	15	0	45	15	0	0	1	TCPSVT
08/08/13 10:34:09	UNKNOWN	2000:197:11:201:0:2:0:1	50030	2000:199:11:80::105	GERMANY	100	0	0	4	100	4	100	12	12	0	24	11	0	0	1	TCPSVT

Scenario 6: DDVIPA Unhealthy Servers

zOS Image Name	Proportional CP Weight	WLM Weight	Abnormal Transaction Percent	Target Server Responsiveness Rate	Target Connectivity Success Rate	Server Accept Efficiency Fraction
GERMANY	15	0	0	4	100	4
GERMANY	11	0	0	4	100	4
GERMANY	0	0	0	4	100	4
GERMANY	15	0	0	4	100	4
GERMANY	15	0	0	4	100	4
GERMANY	11	0	0	4	100	4
GERMANY	0	0	0	4	100	4
GERMANY	15	0	0	4	100	4
GERMANY	0	0	0	4	100	4
GERMANY	15	0	0	4	100	4
GERMANY	15	0	0	4	100	4
GERMANY	11	0	0	4	100	4

1. Proportional CP Weight indicates that GERMANY is healthy.

4. Adjusted WLM weight is 0 due to SEF and TSR values.

3. TSR (4) is low due to the SEF.

2. SEF of 4 indicates that the server's ability to accept connections is very poor.

More Information

- NetView website

  https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli System z Monitoring and Application Management/page/IBM NetView for zOS

- Service Management Suite for z/OS

  https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wfb8610d29f30_4f81_802f_2b8d115202ec

- IP management with NetView for z/OS

  https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli+System+z+Monitoring+and+Application+Management/page/Tivoli+NetView+for+zOS

- NetView customer forum

  http://tech.groups.yahoo.com/group/NetView/

- NetView documentation

  http://www-01.ibm.com/support/knowledgecenter/SSZJDU_6.2.1/com.ibm.itnetviewforzos.doc_6.2.1/netv621_welcome_kc.htm?cp=SSZJDU_6.2.1%2F0

Please fill out your session evaluation

- NetView for z/OS: New Directions
- Session # 17886
- QR Code:

Complete your session evaluations online at www.SHARE.org/Orlando-Eval