# NetView for z/OS: IP Management Topics and Solutions

*Larry Green and Jeff Weiner*
*Design/development, Netview for z/OS*
*IBM*
*Session 16833*

Insert Custom Session QR if Desired.

#SHAREorg

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

SHARE in Seattle 2015

# 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.

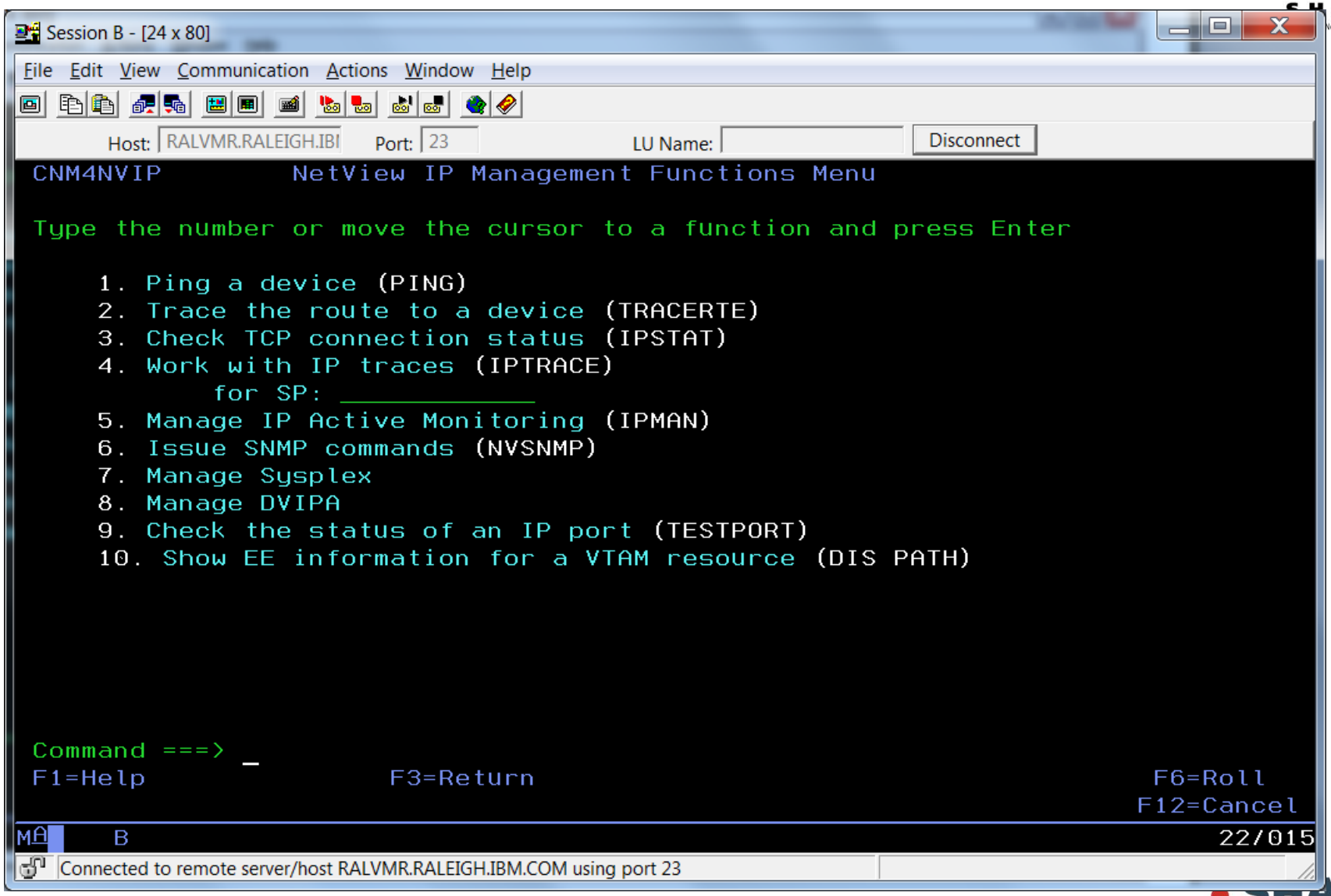
Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

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 Management Menu, Sysplex Data Discovery
- TCP/IP Connection Management
- Intrusion Detection and Automation
- Packet Trace (scenario 1)
- DDVIPA Changes (scenario 2)
- Monitoring Sysplex Distributor (scenario 3)

# IP Management menu: Additions and new option panels



# Sysplex Data Discovery

- Coupling Facility
- TELNET Servers
- TCP/IP Interfaces (OSA and Hipersockets)
- Active Listeners as they relate to DVIPA
- Items to complete a physical view related to OSA and Hipersockets

# 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

# 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

# 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

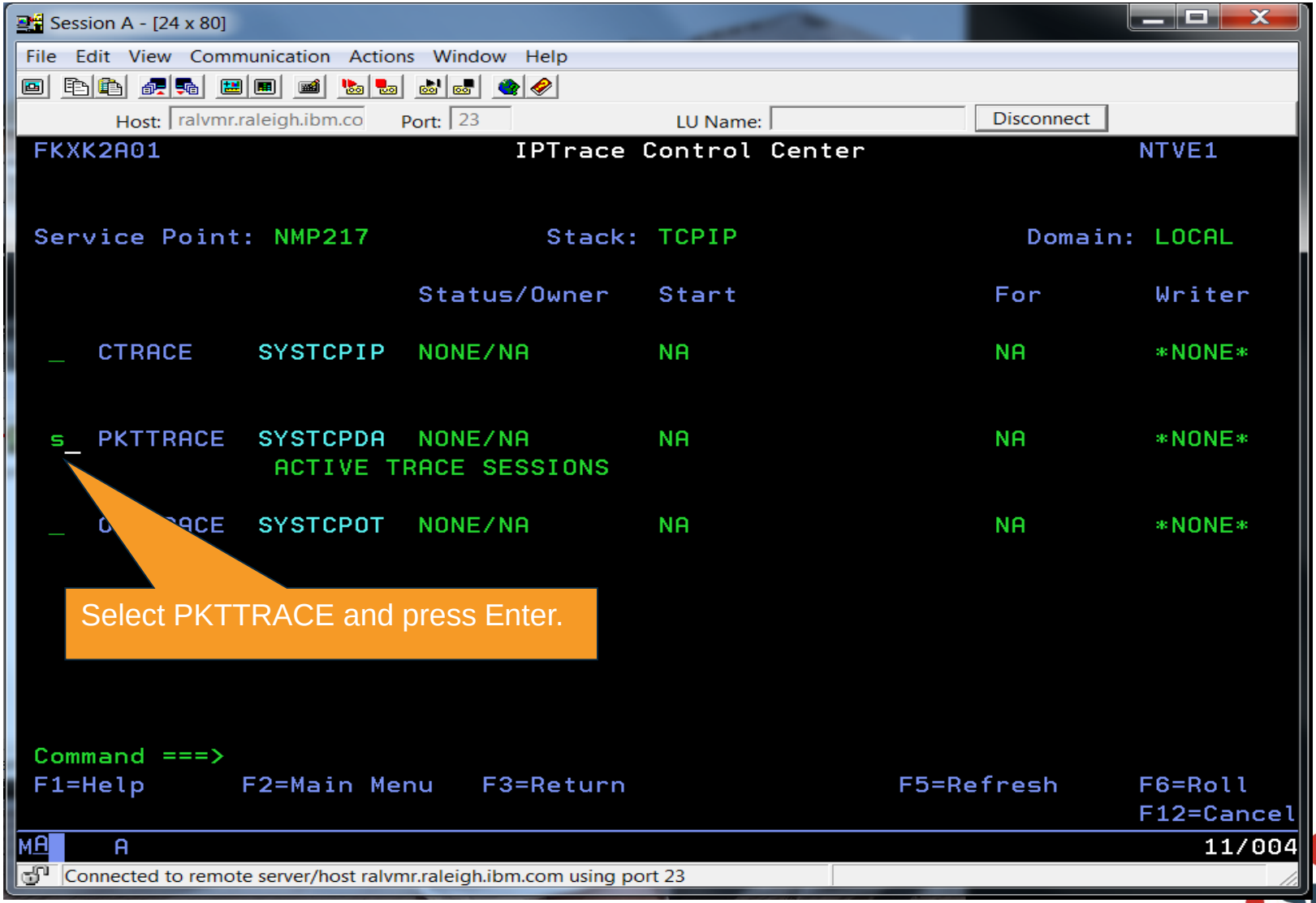
# New in NetView for z/OS V6.2

- 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

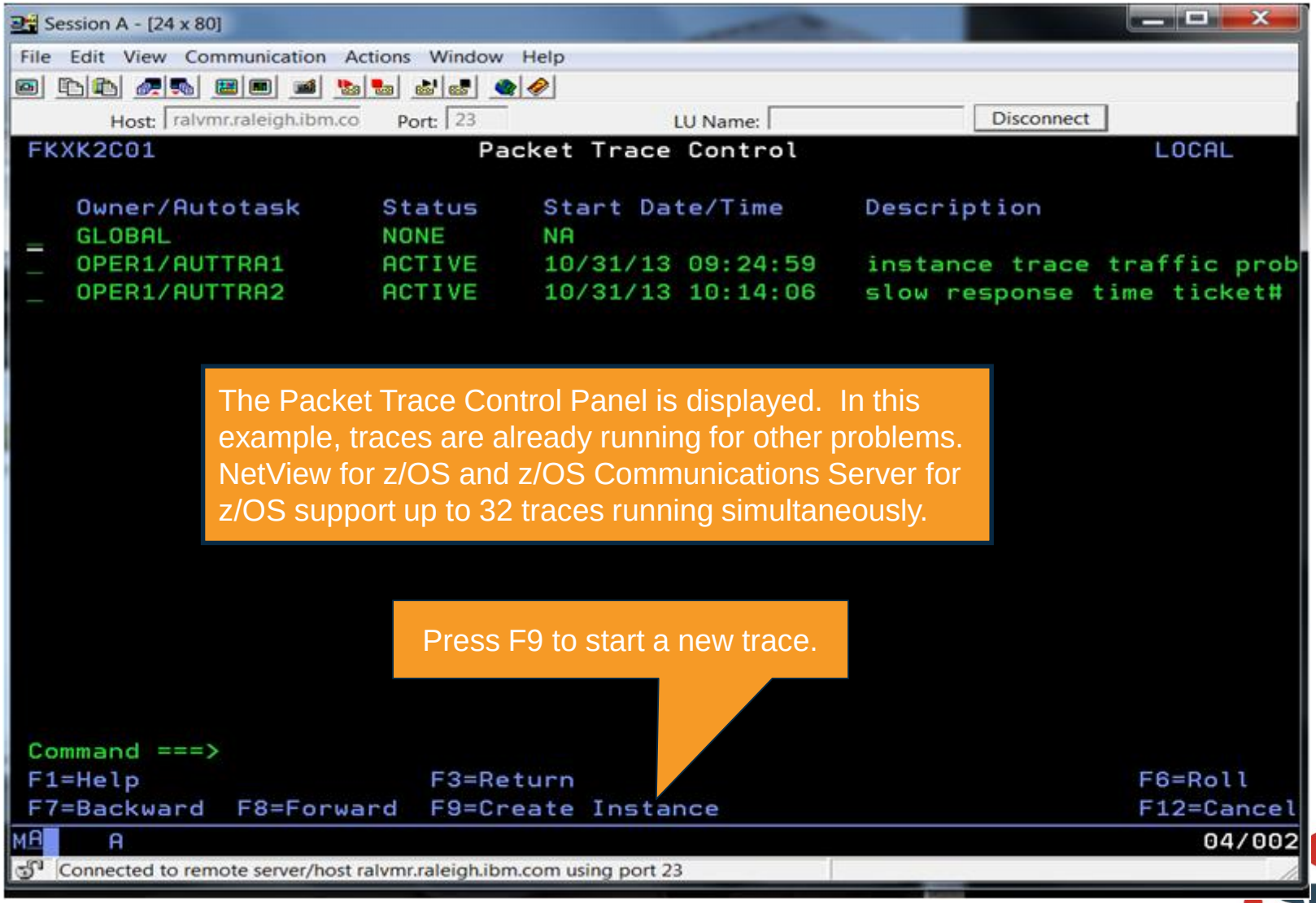
# Scenario: Packet Trace Connectivity

- 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



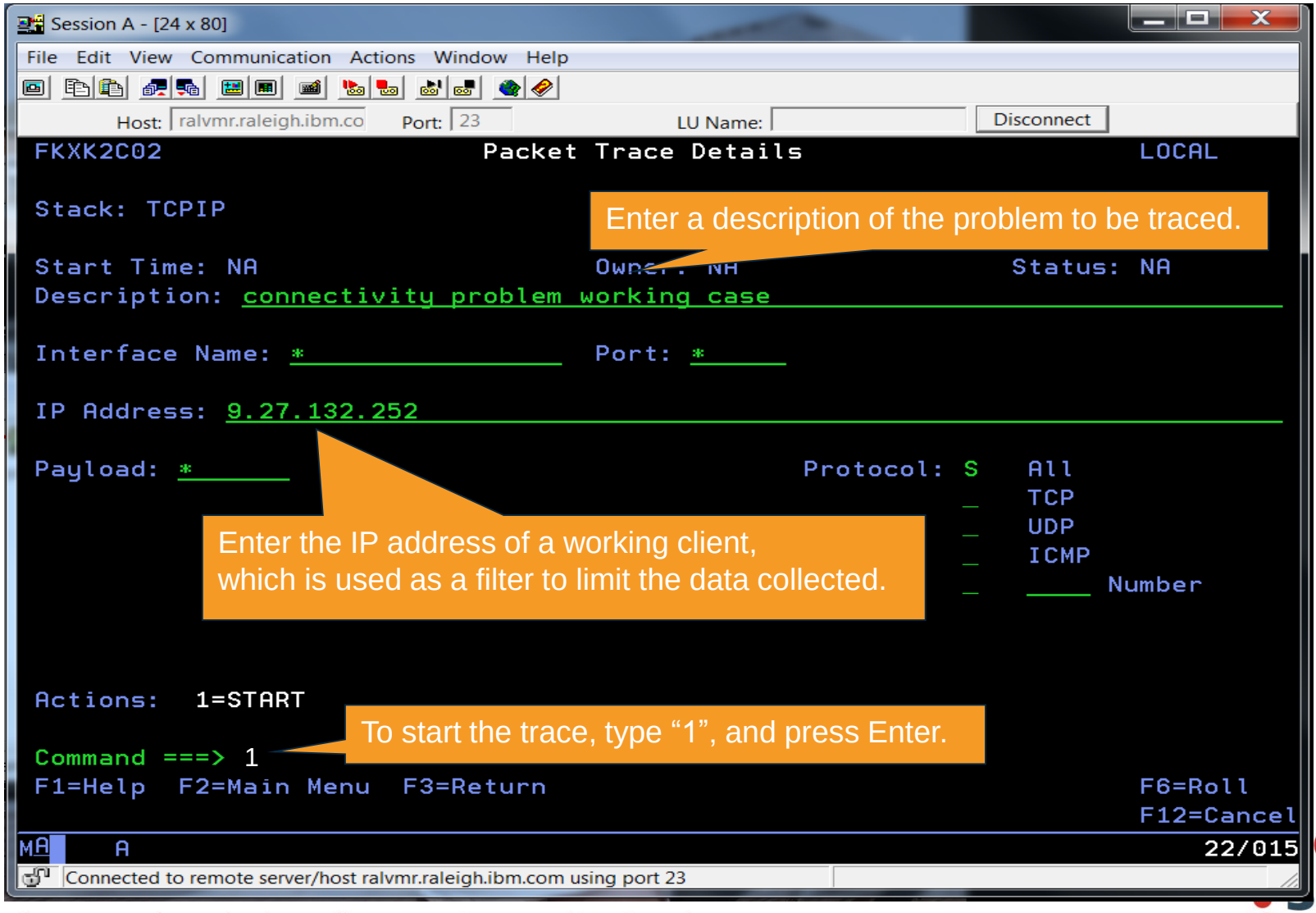
# Scenario 1: Packet Trace



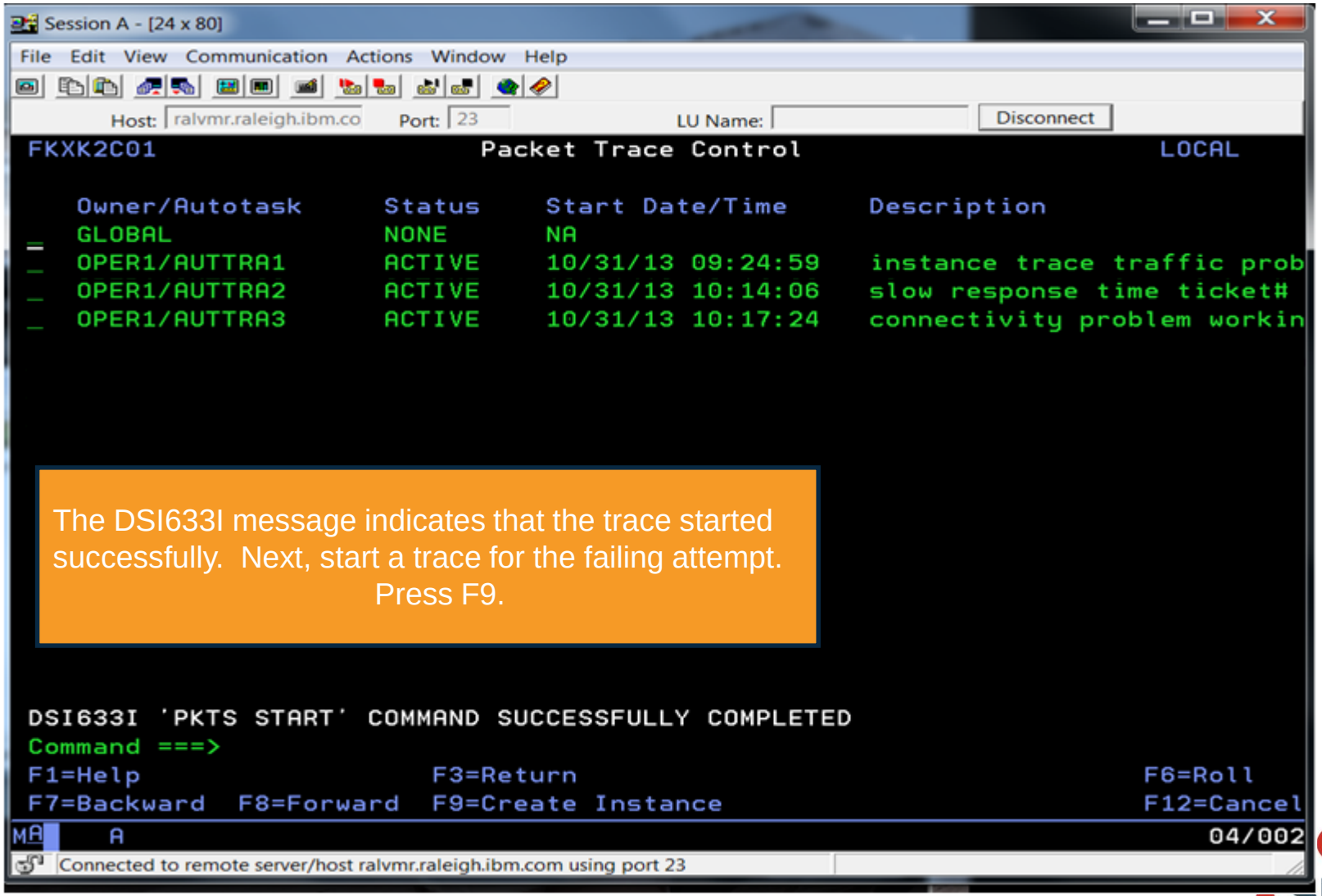

The Packet Trace Control Panel is displayed. In this example, traces are already running for other problems. NetView for z/OS and z/OS Communications Server for z/OS support up to 32 traces running simultaneously.

Press F9 to start a new trace.

# Scenario 1: Packet Trace

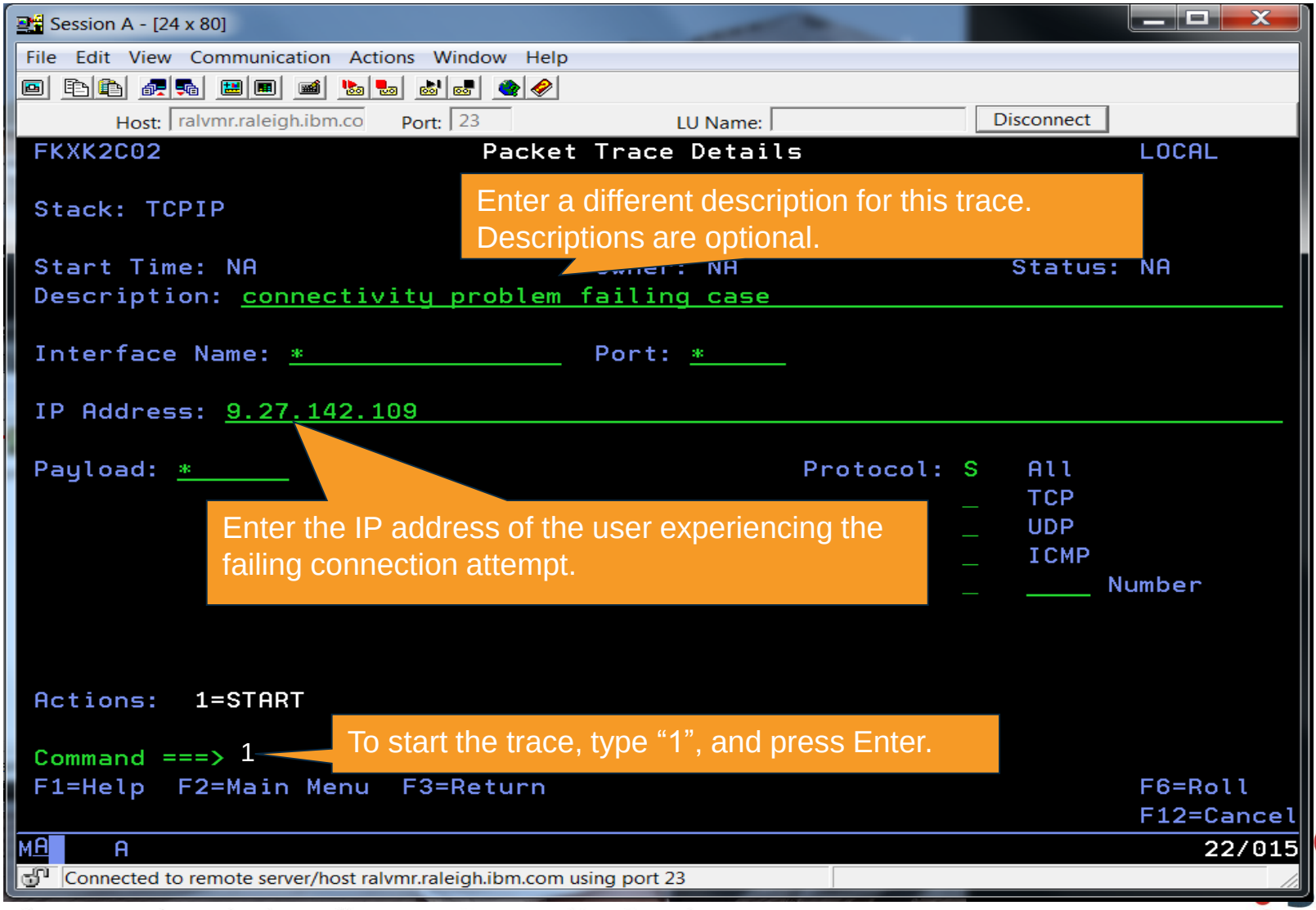


# Scenario 1: Packet Trace

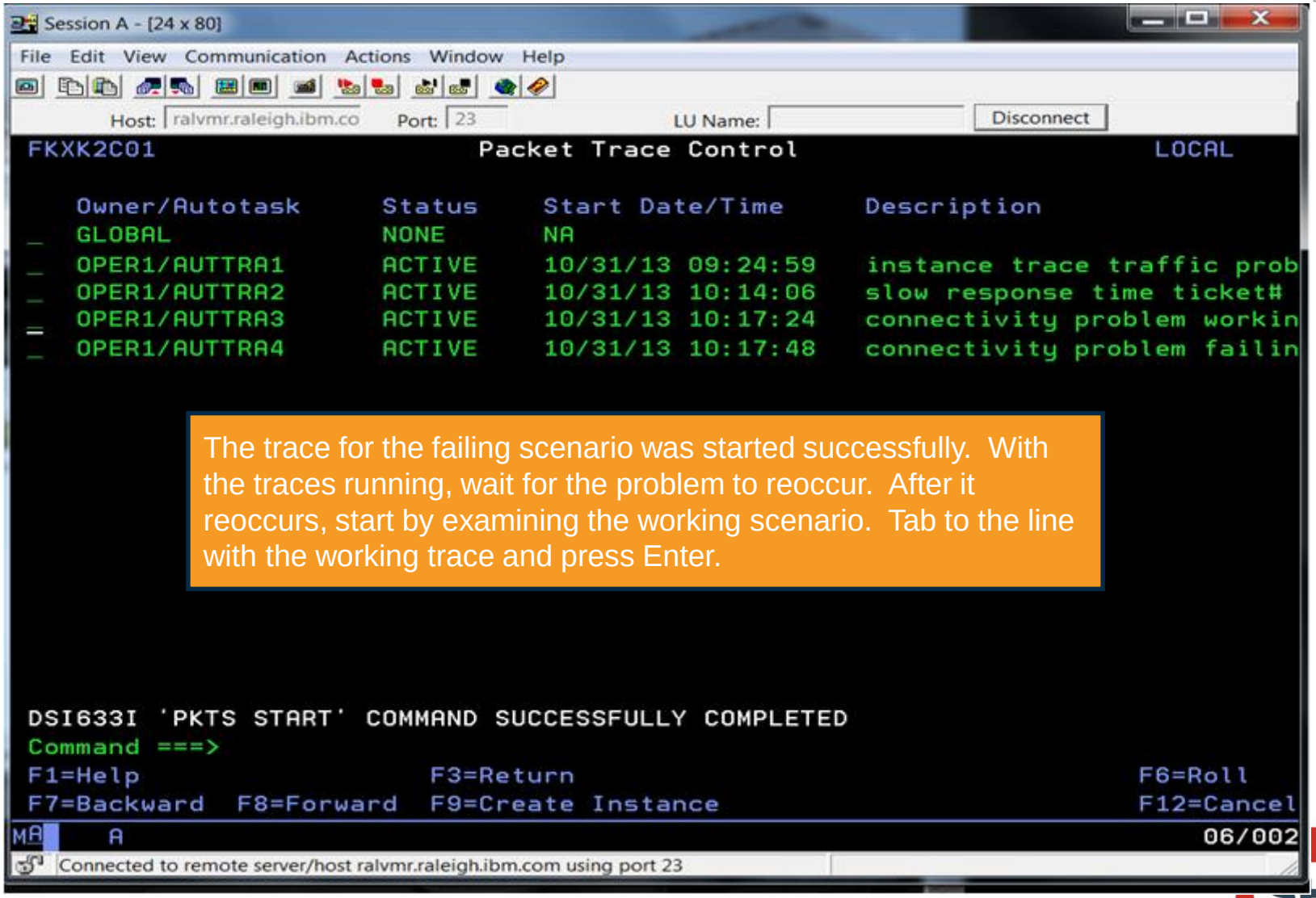



The DSI633I message indicates that the trace started successfully. Next, start a trace for the failing attempt. Press F9.

# Scenario 1: Packet Trace

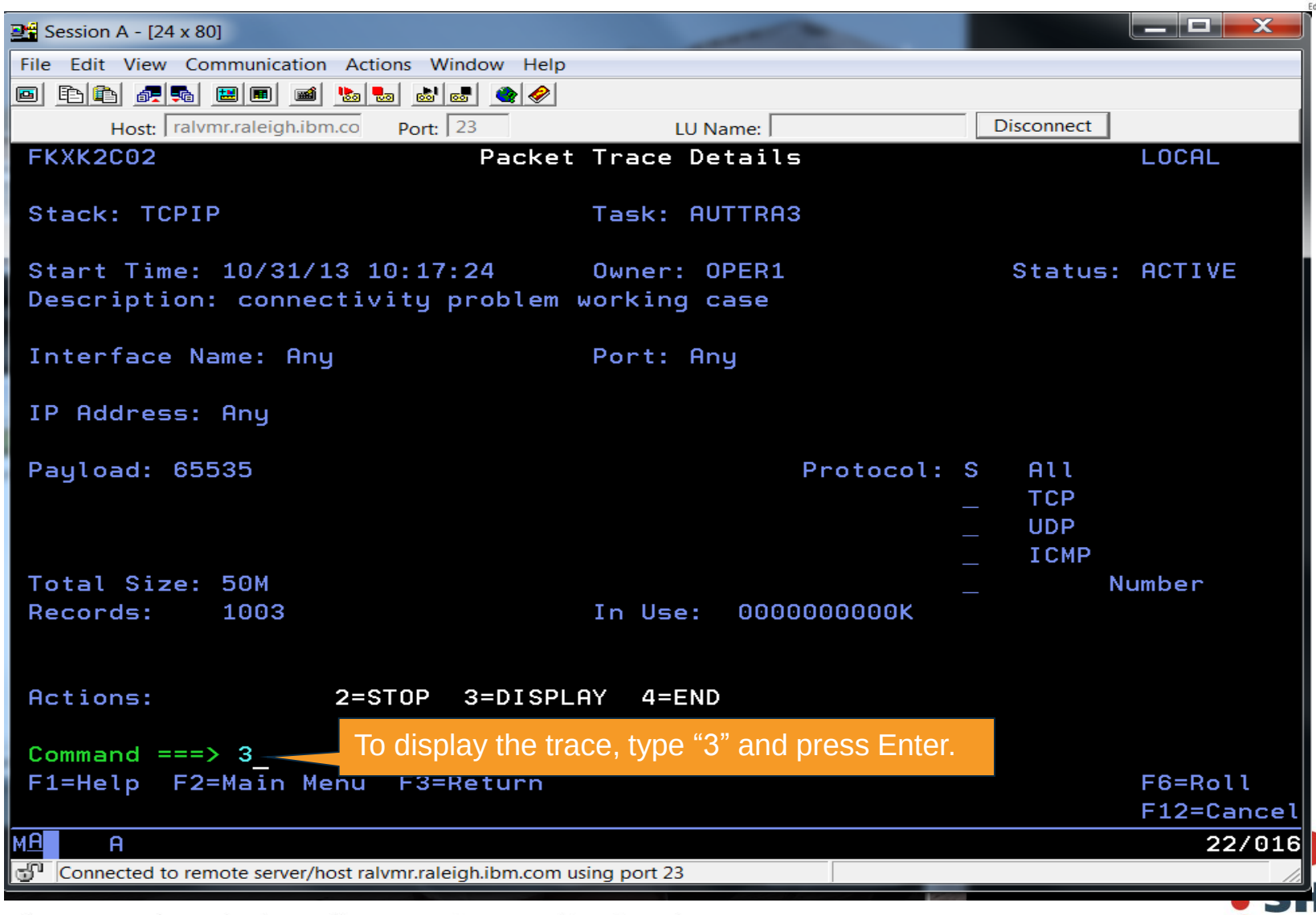


# Scenario 1: Packet Trace



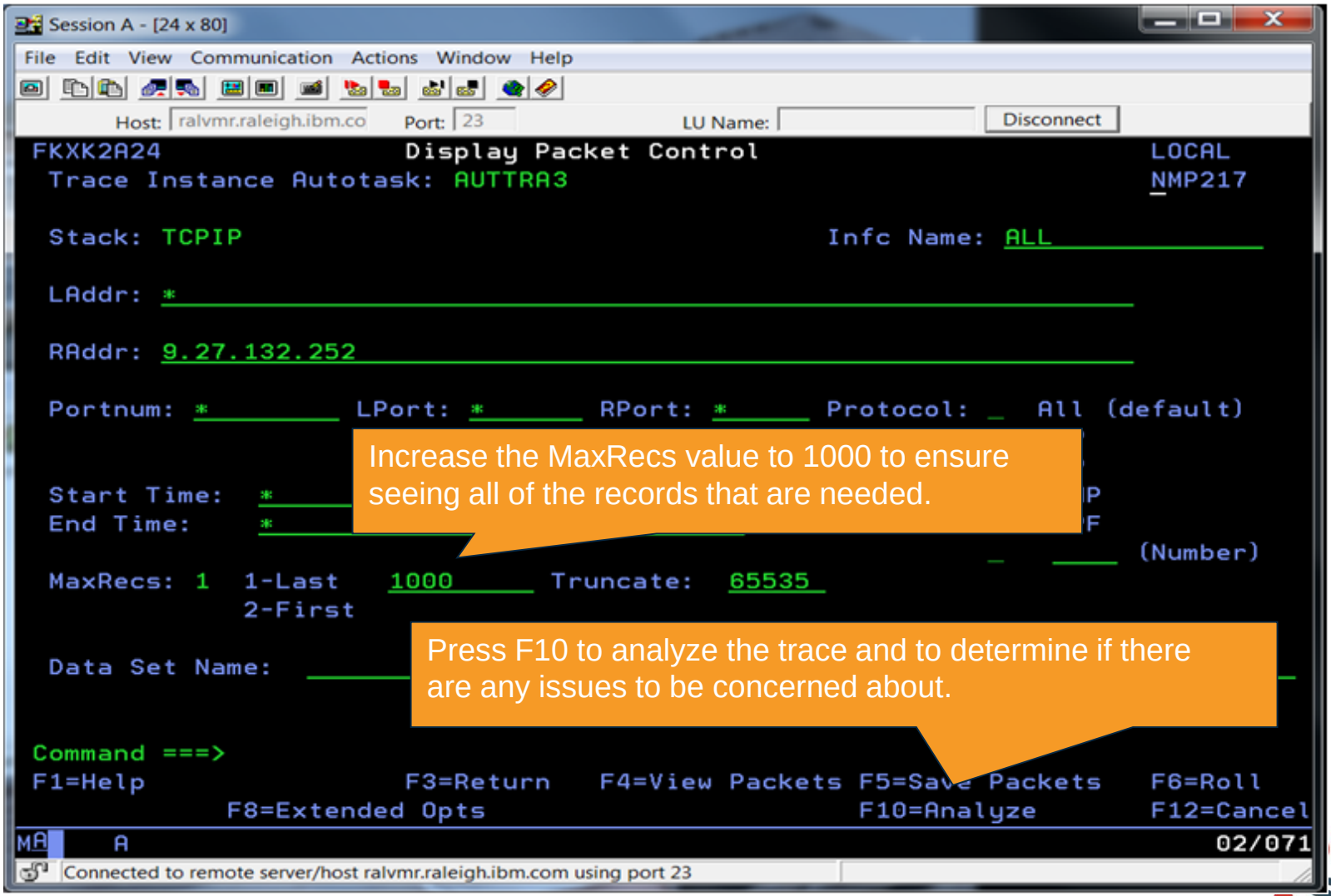

The trace for the failing scenario was started successfully. With the traces running, wait for the problem to reoccur. After it reoccurs, start by examining the working scenario. Tab to the line with the working trace and press Enter.

# Scenario 1: Packet Trace




To display the trace, type “3” and press Enter.

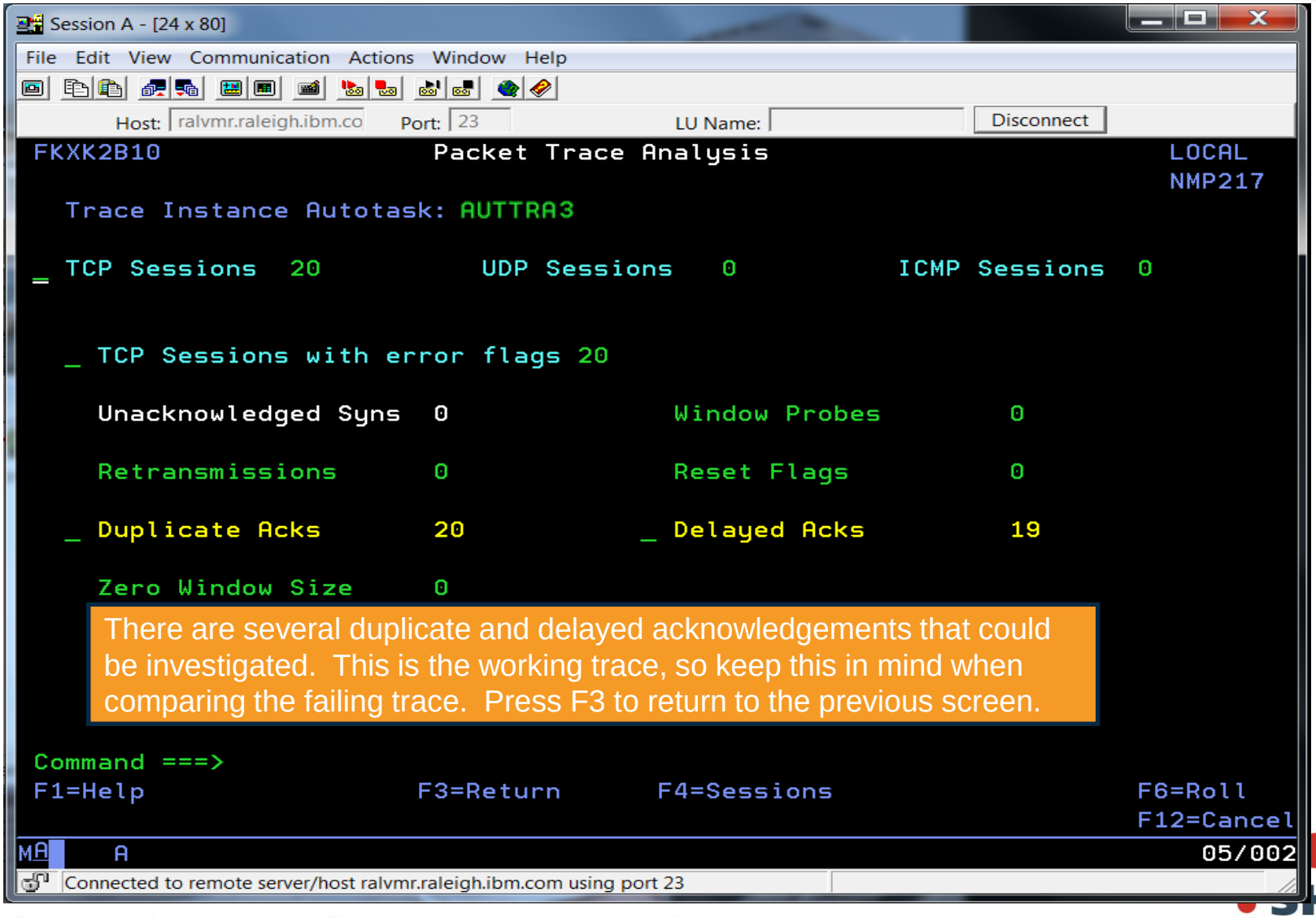
# Scenario 1: Packet Trace



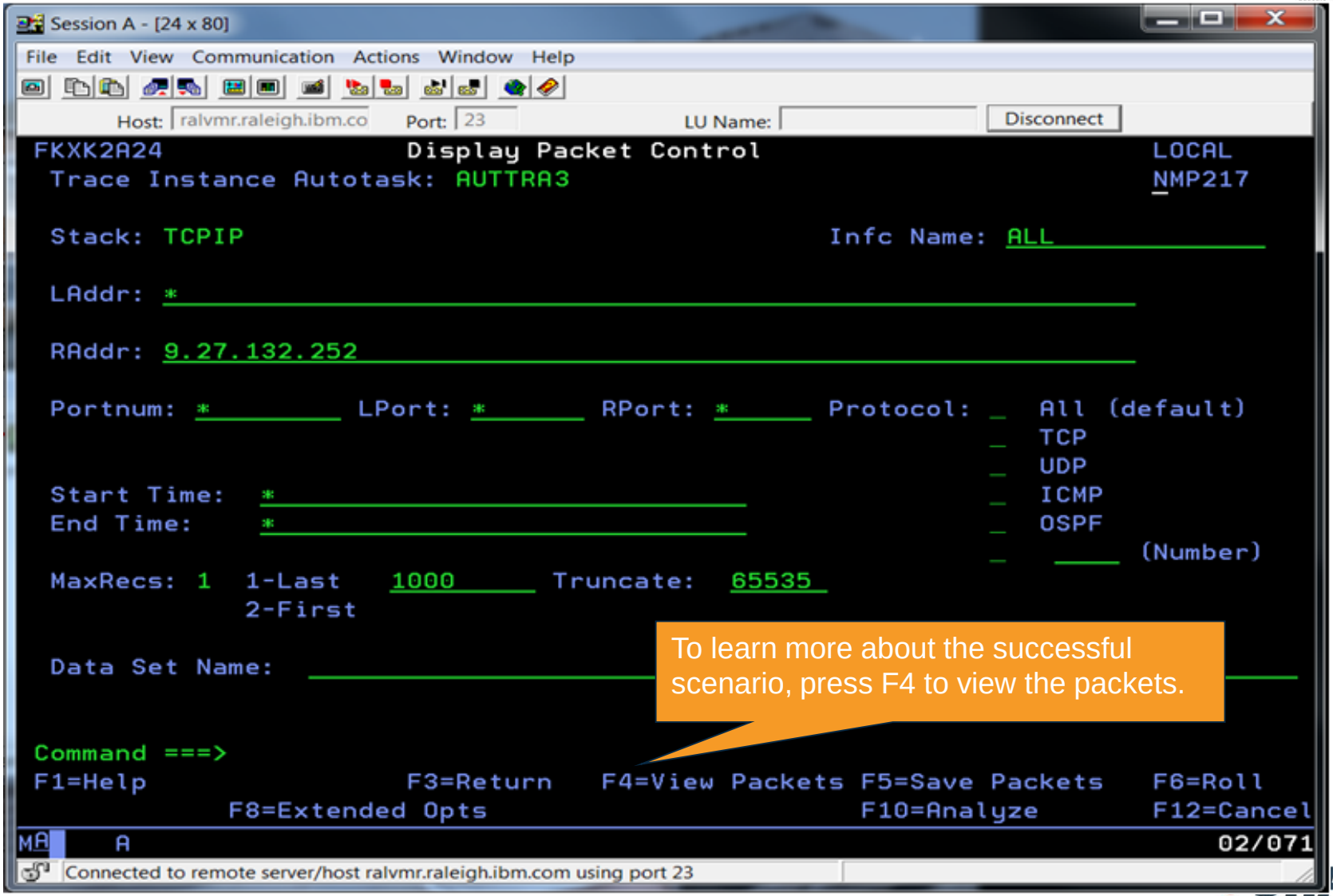

Increase the MaxRecs value to 1000 to ensure seeing all of the records that are needed.

Press F10 to analyze the trace and to determine if there are any issues to be concerned about.

# Scenario 1: Packet Trace

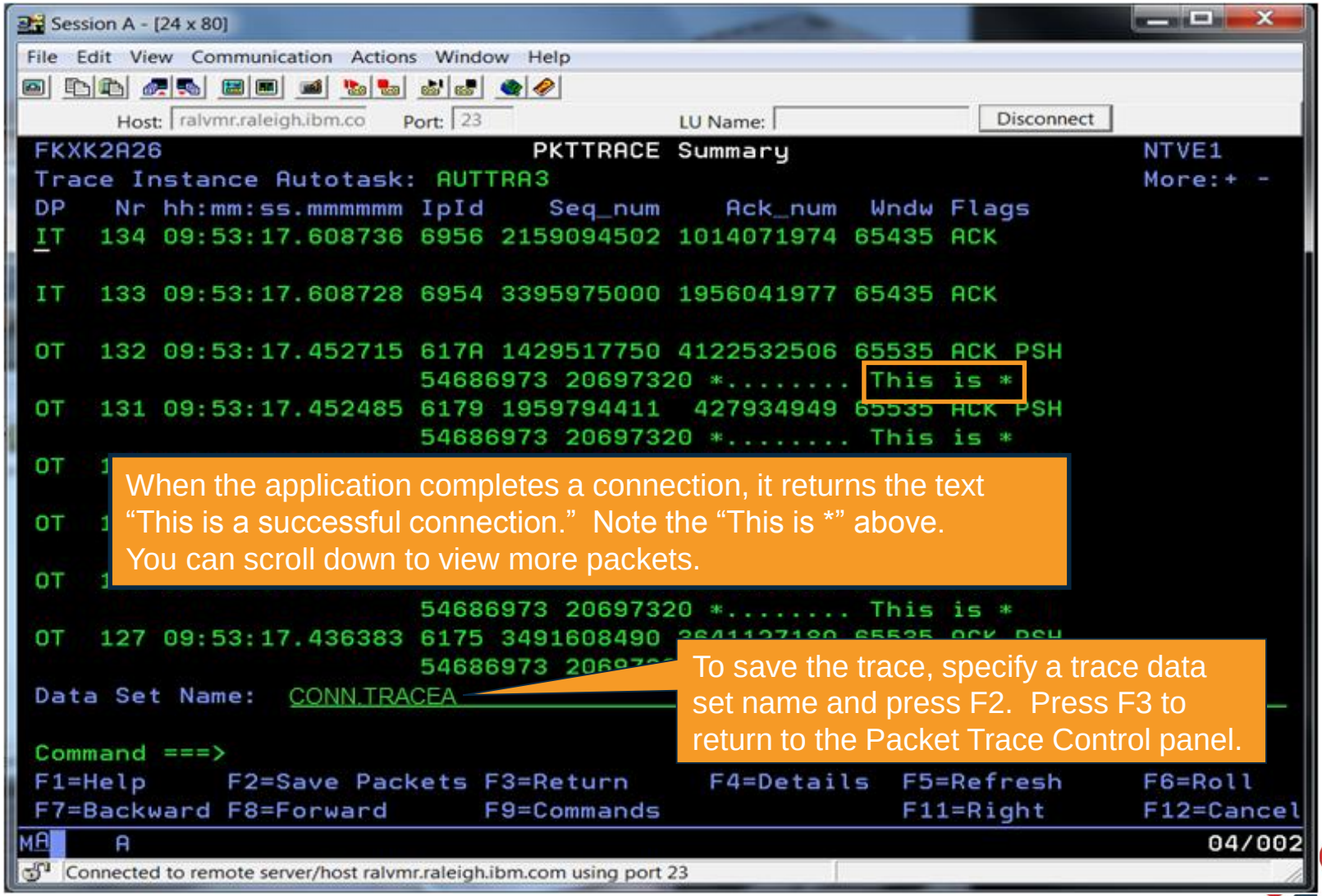


# Scenario 1: Packet Trace




To learn more about the successful scenario, press F4 to view the packets.

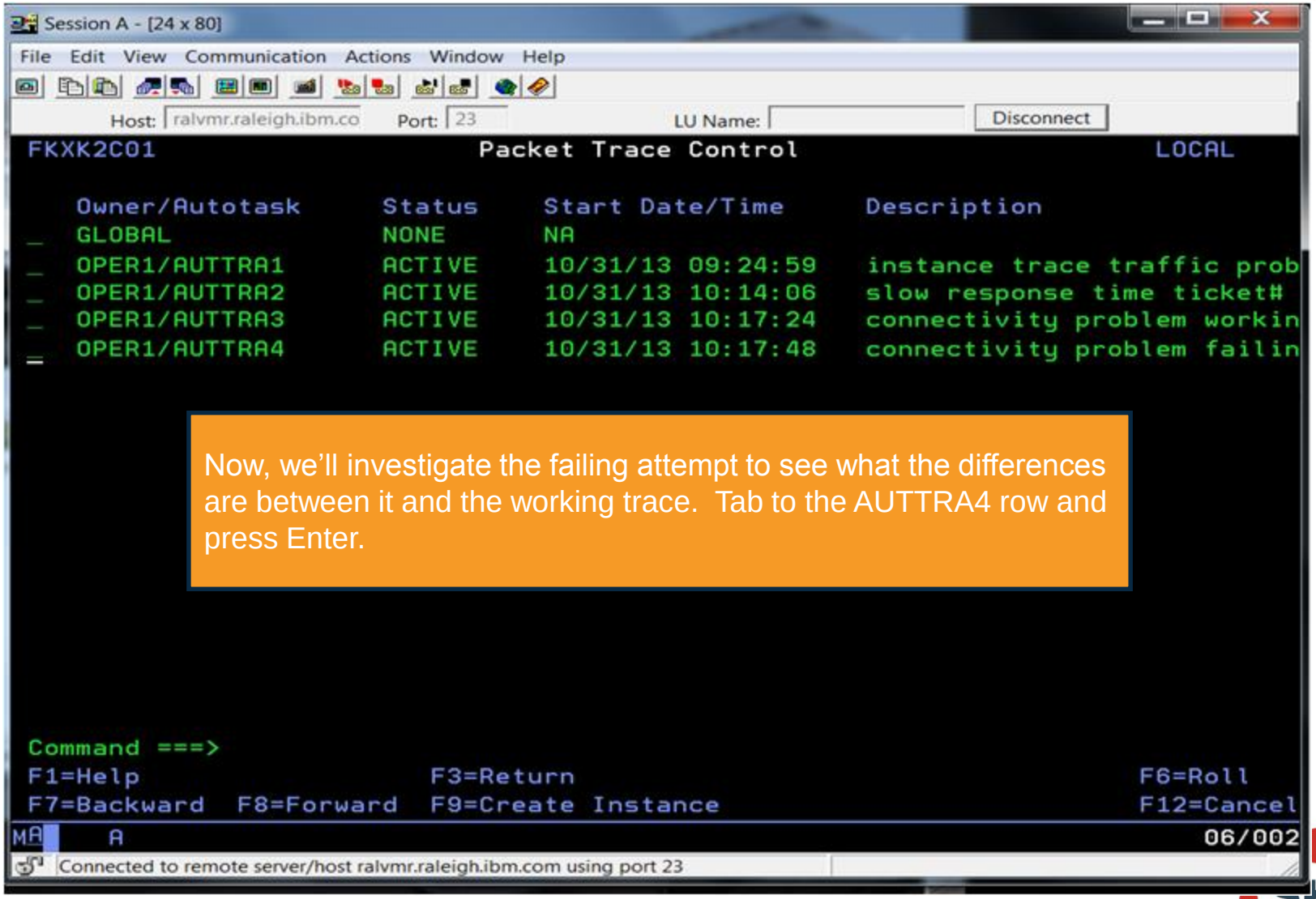
# Scenario 1: Packet Trace




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.

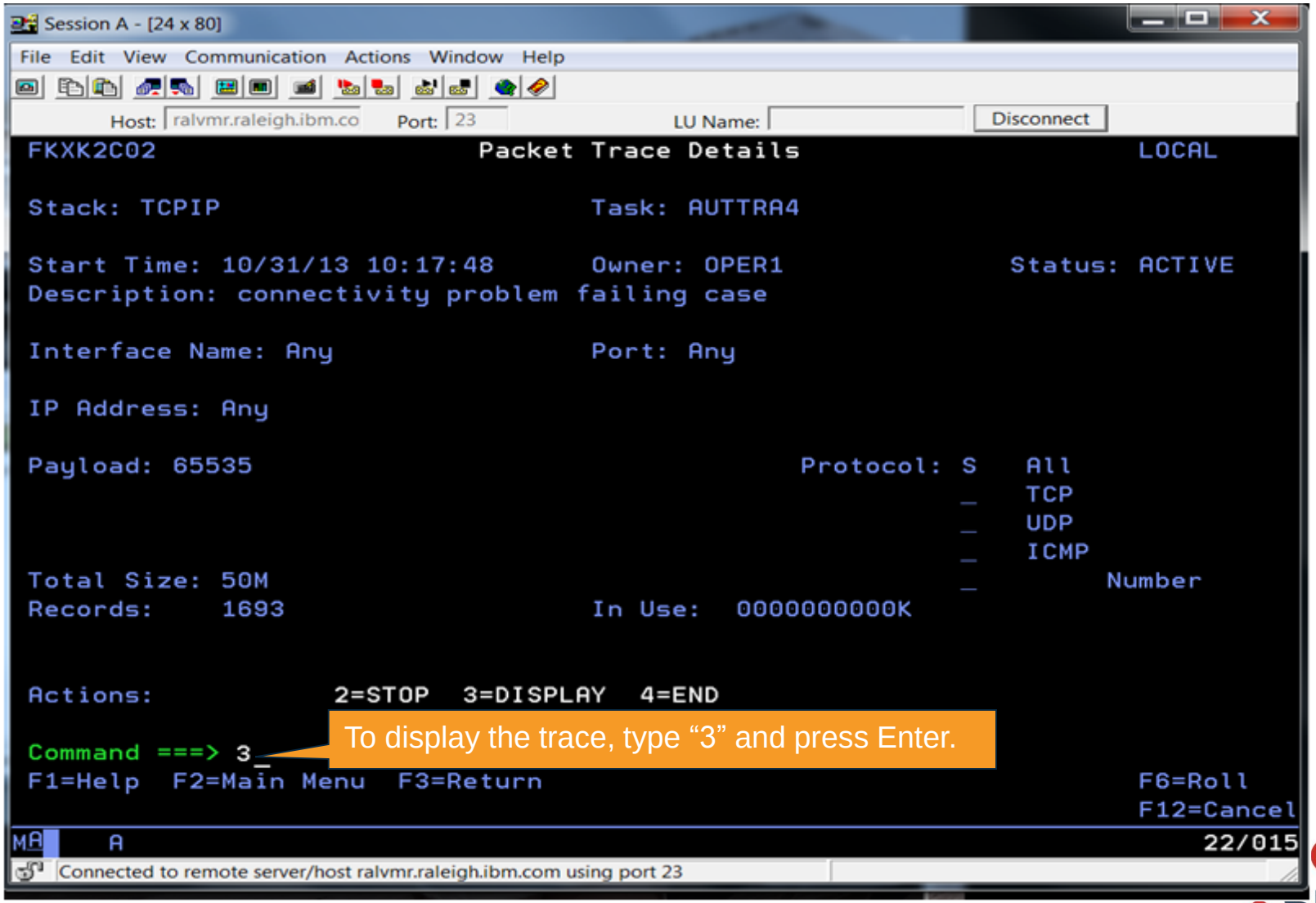
To save the trace, specify a trace data set name and press F2. Press F3 to return to the Packet Trace Control panel.

# Scenario 1: Packet Trace



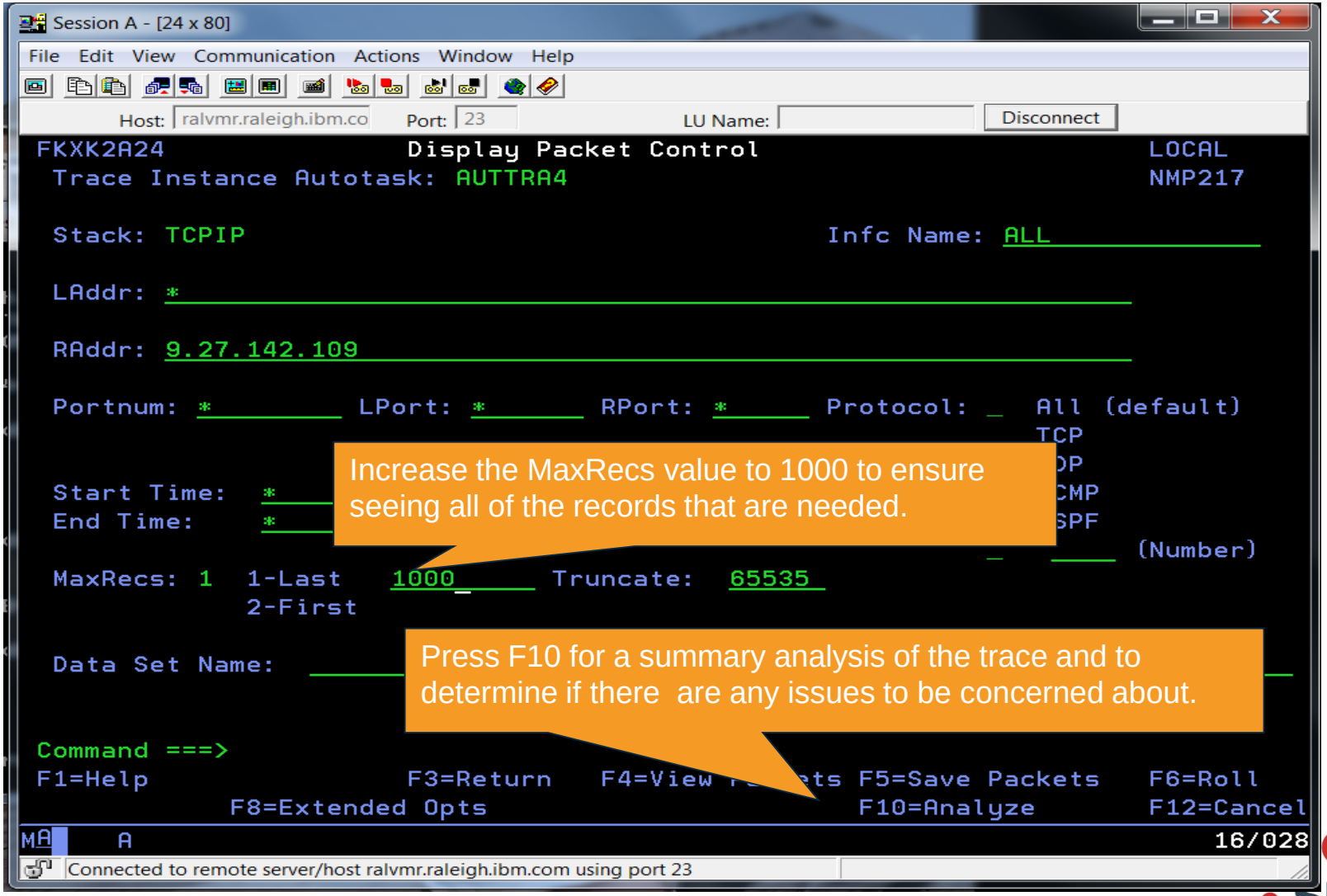

Now, we'll investigate the failing attempt to see what the differences are between it and the working trace. Tab to the AUTTRA4 row and press Enter.

# Scenario 1: Packet Trace

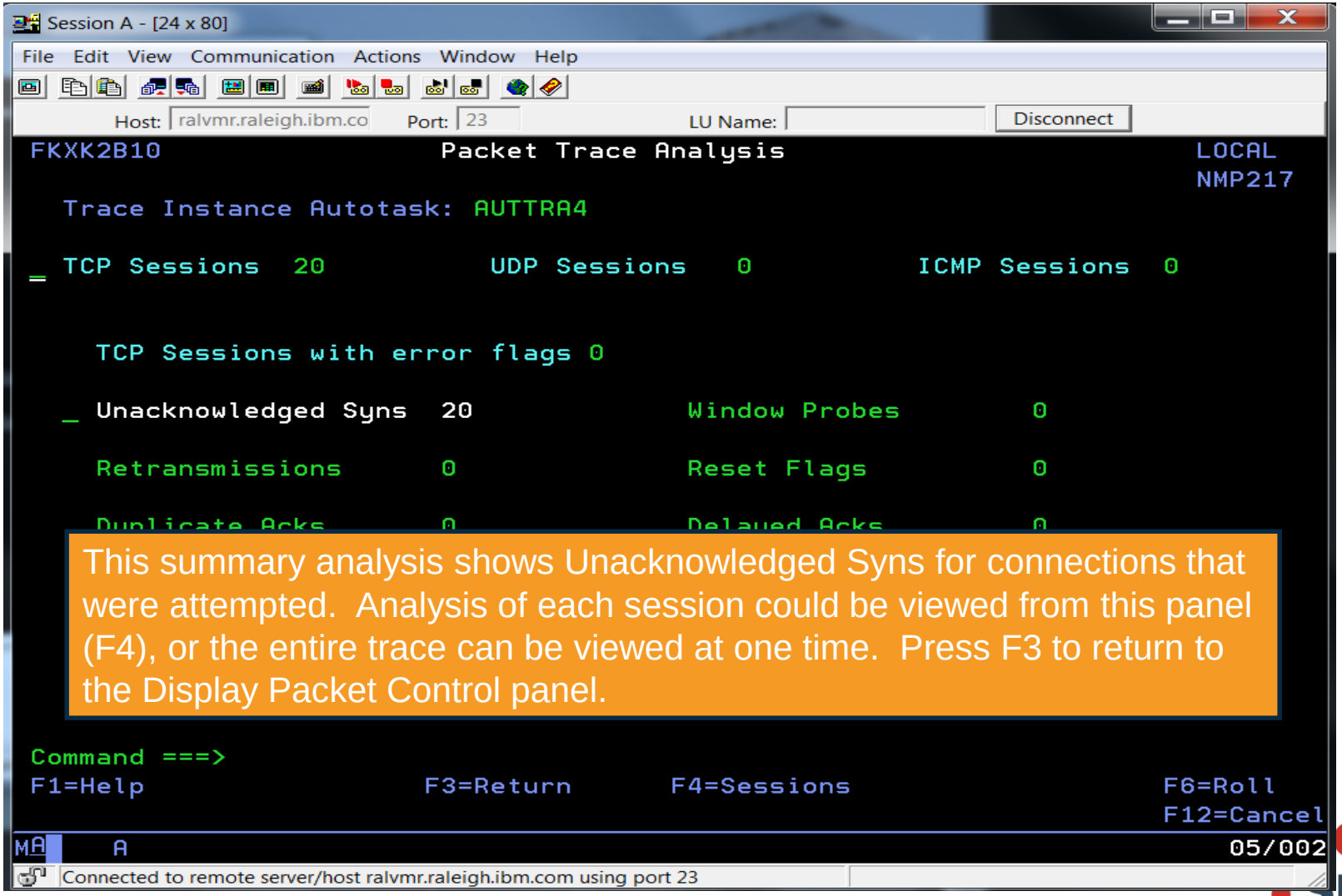



To display the trace, type “3” and press Enter.

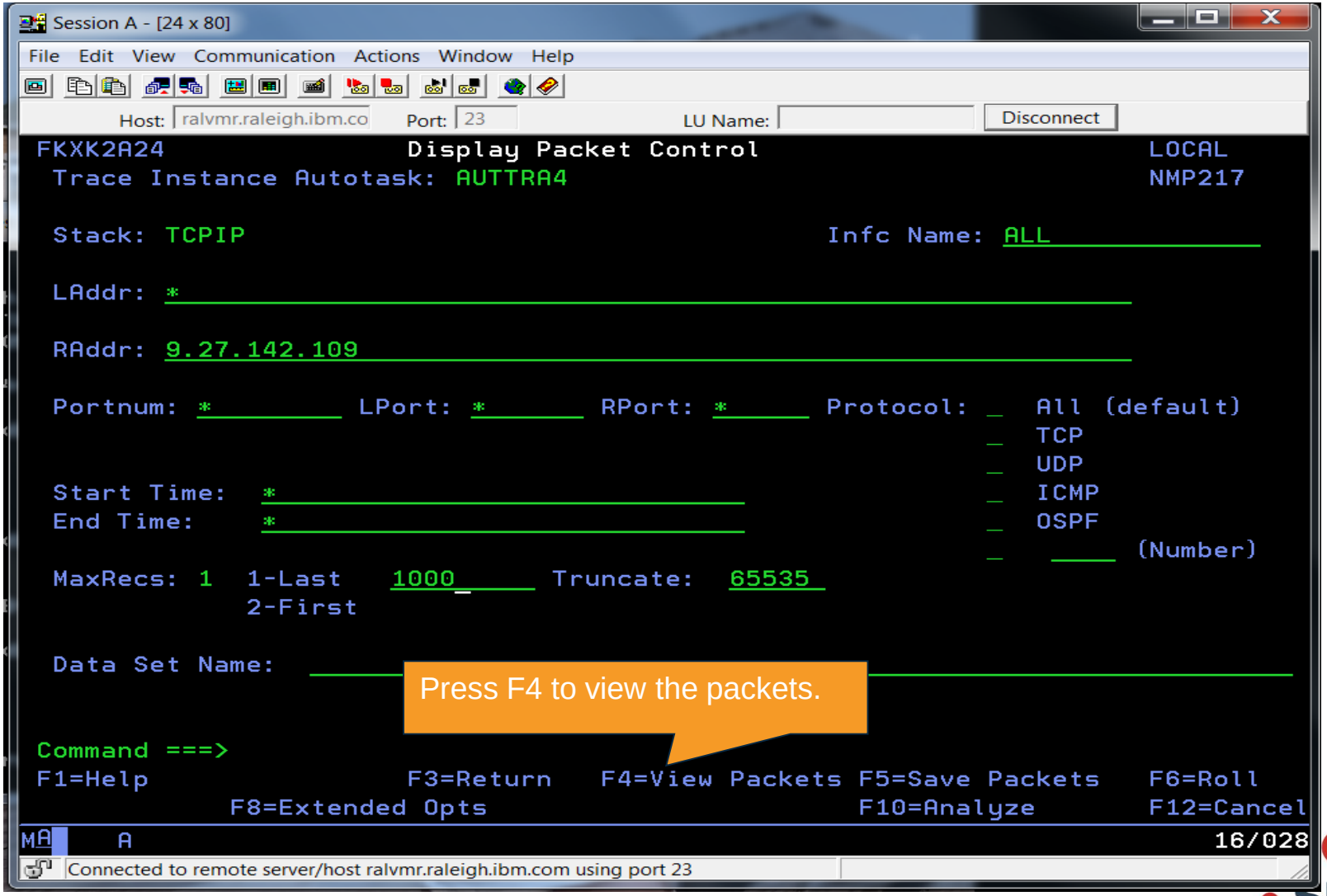
# Scenario 1: Packet Trace



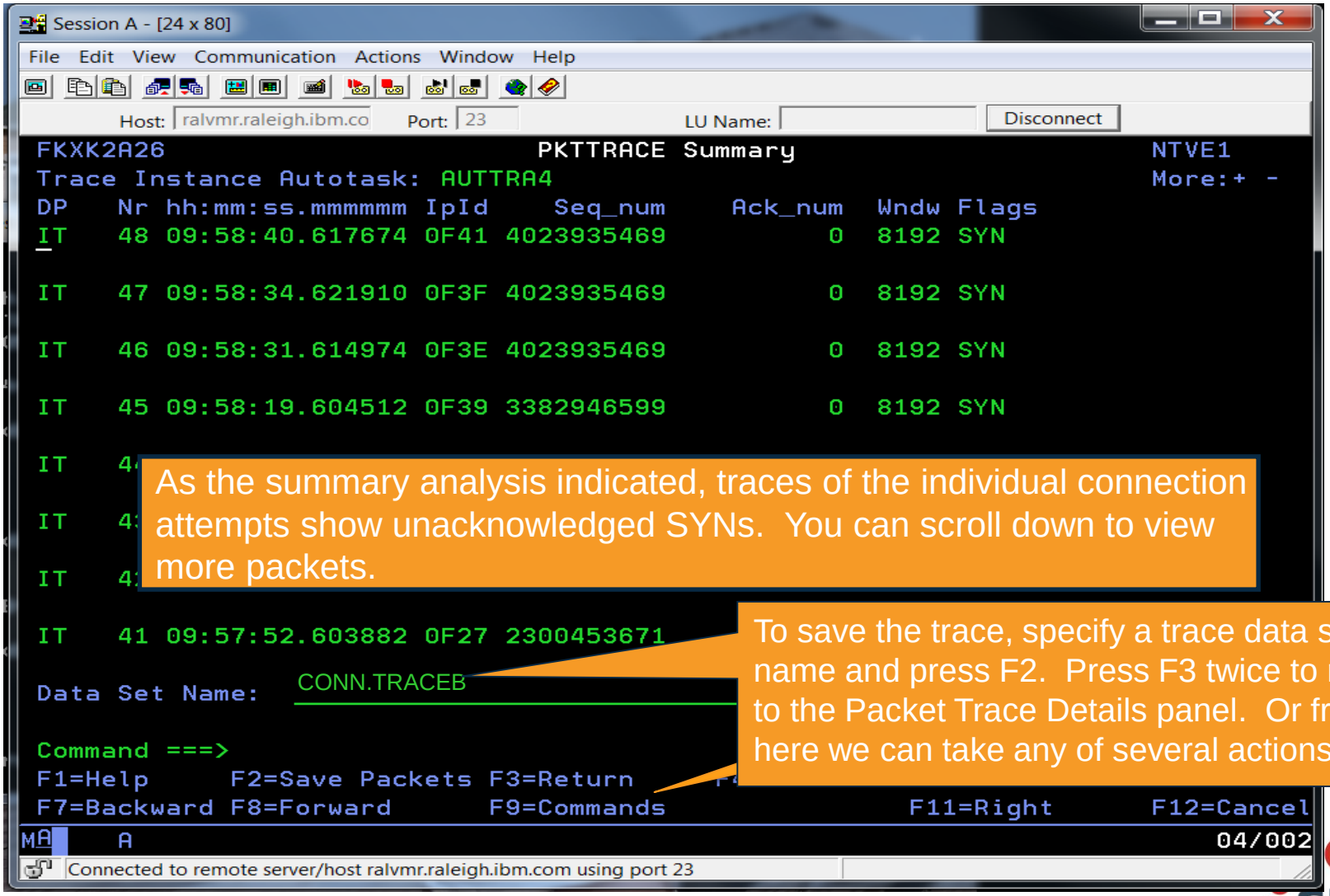
# Scenario 1: Packet Trace



# Scenario 1: Packet Trace



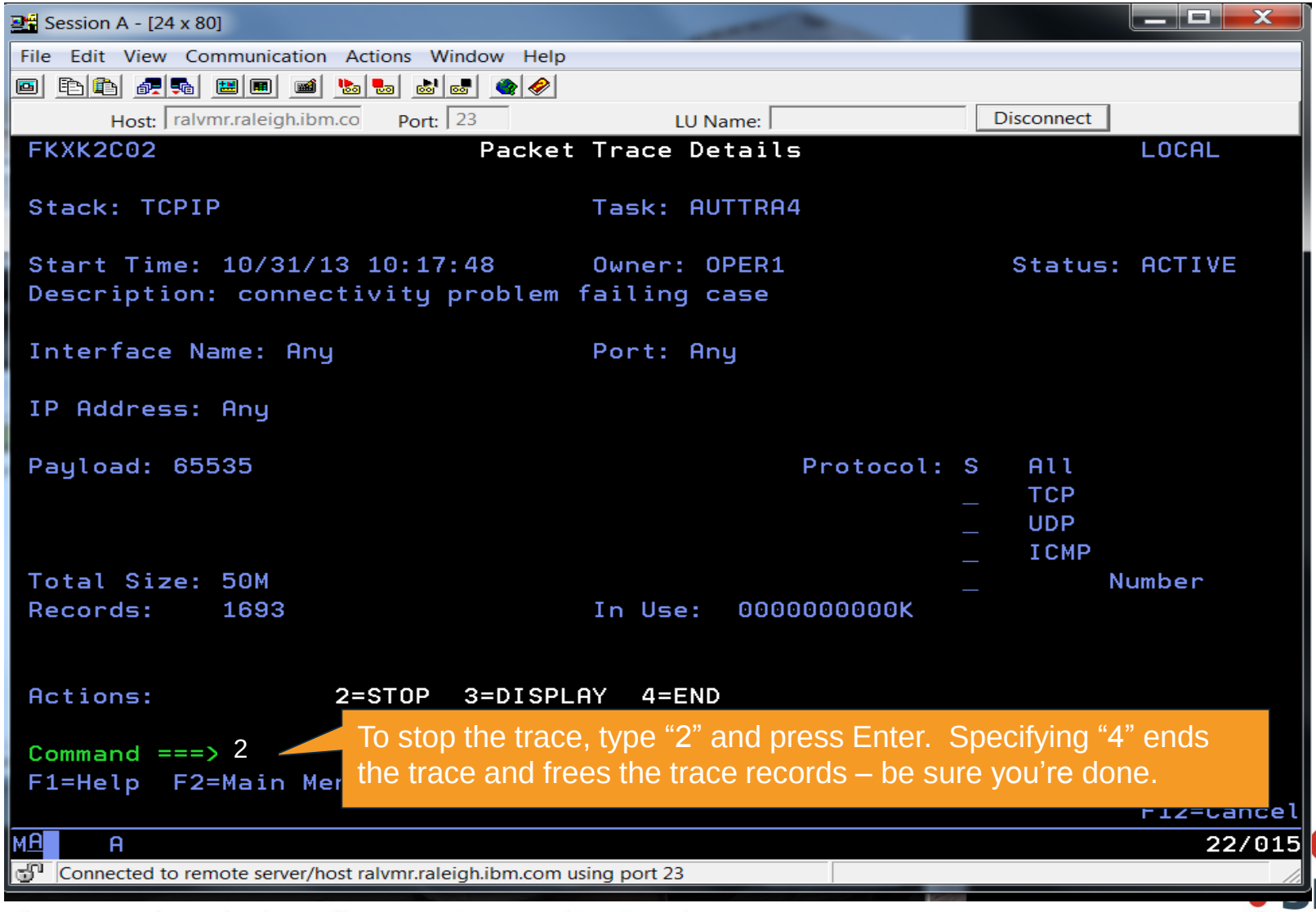
# Scenario 1: Packet Trace




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

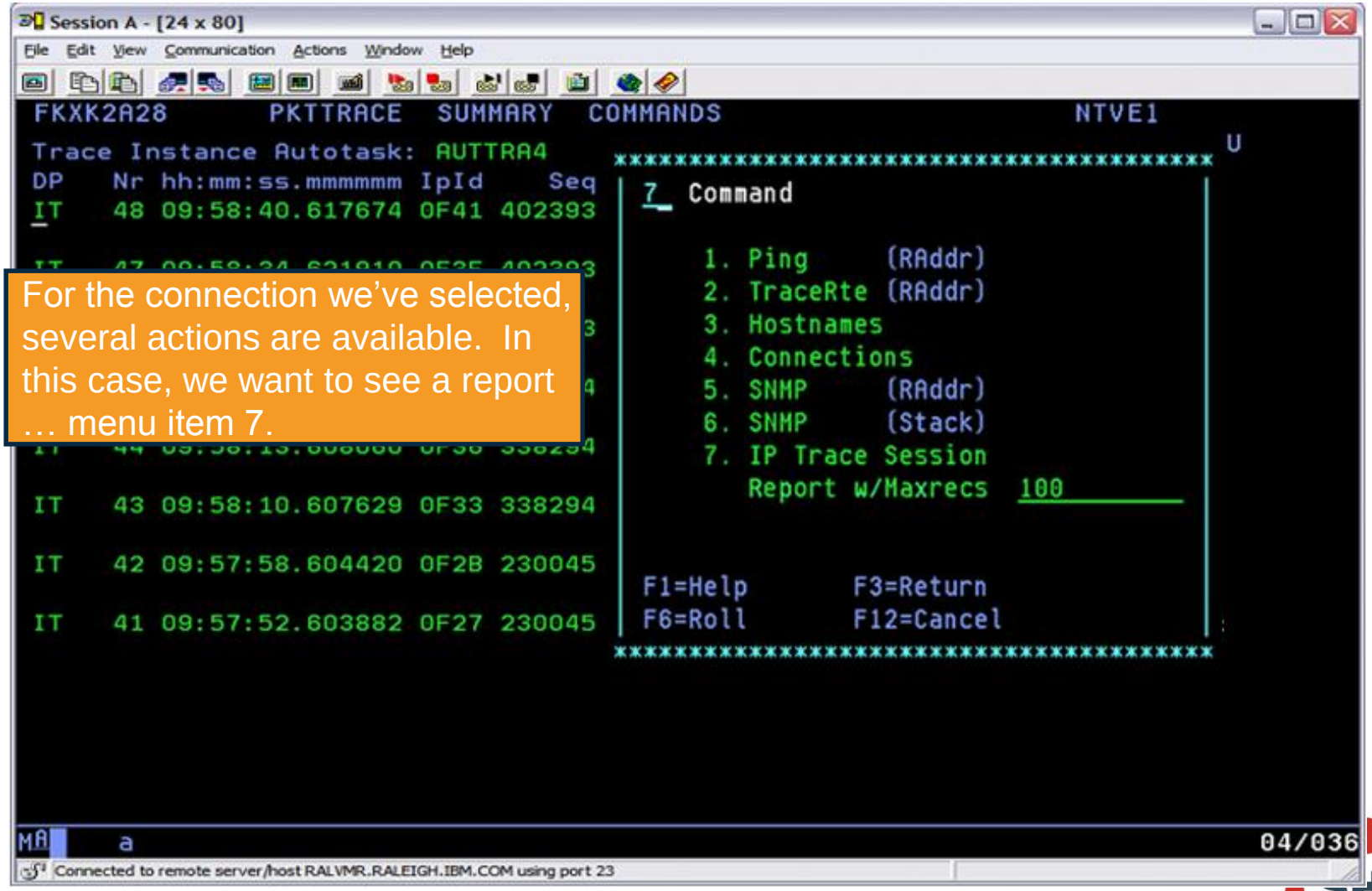
To save the trace, specify a trace data set name and press F2. Press F3 twice to return to the Packet Trace Details panel. Or from here we can take any of several actions: F9

# Scenario 1: Packet Trace



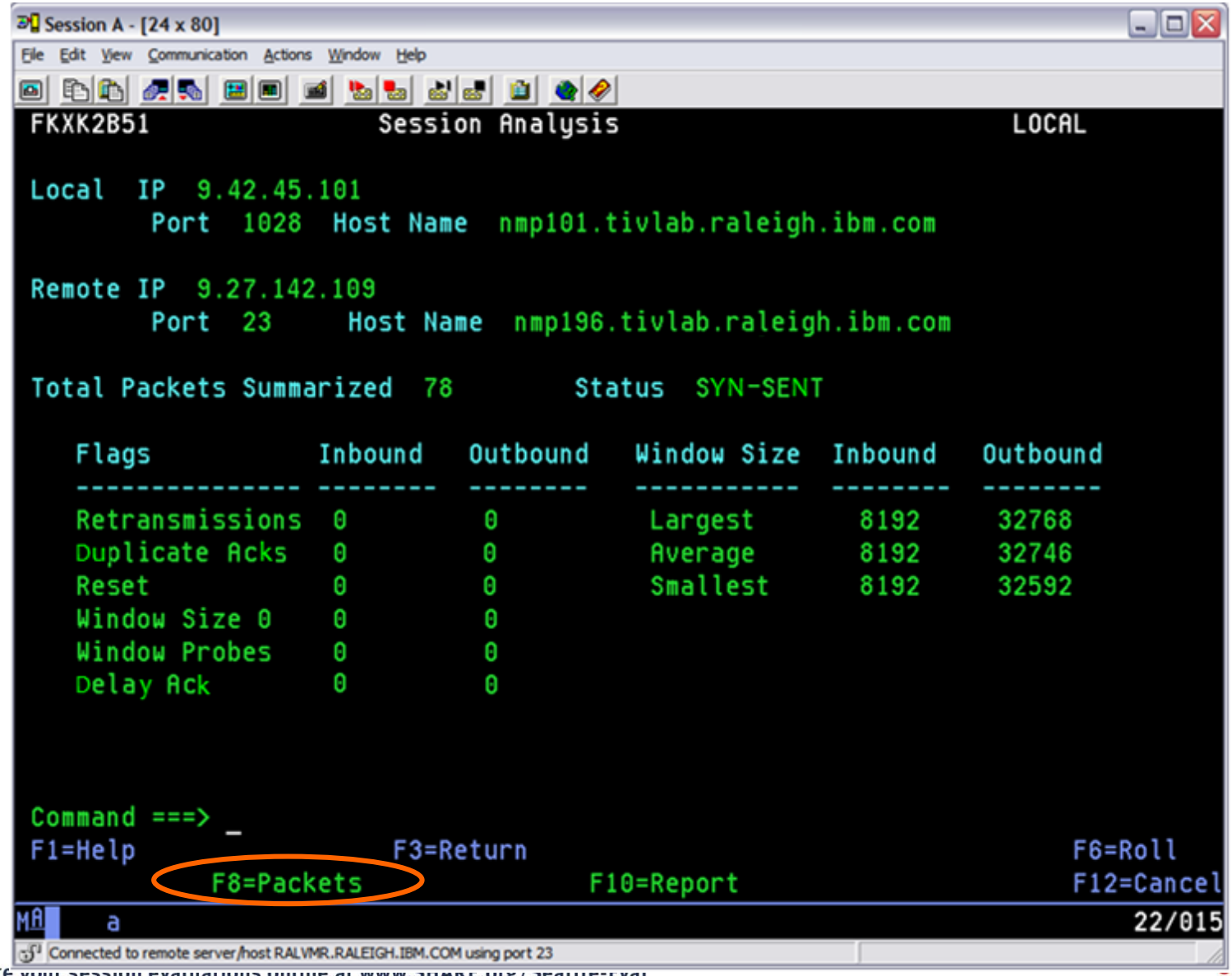

To stop the trace, type “2” and press Enter. Specifying “4” ends the trace and frees the trace records – be sure you’re done.

# Scenario 1: Packet Trace

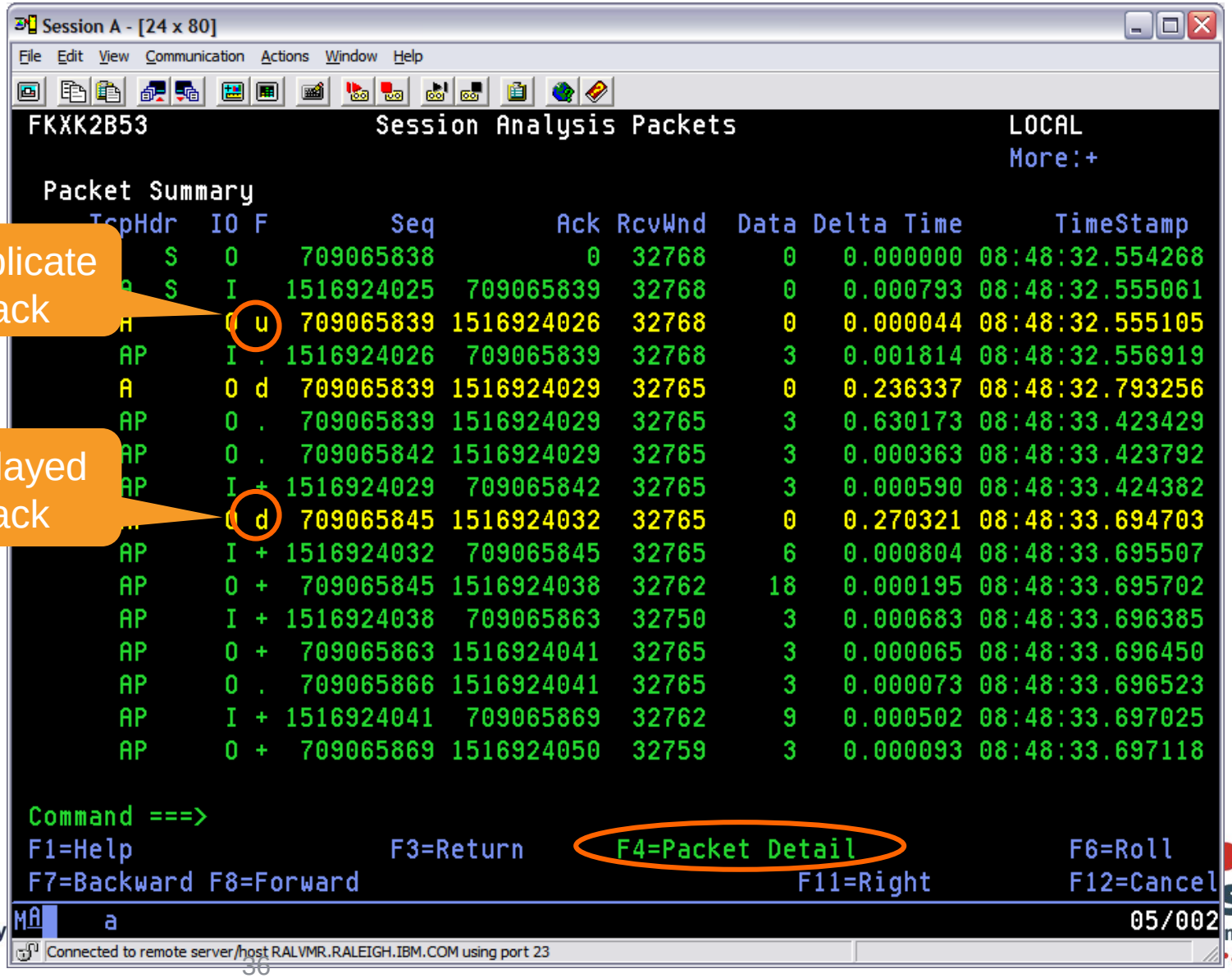



For the connection we've selected, several actions are available. In this case, we want to see a report … menu item 7.

# Scenario 1: Analysis for selected session



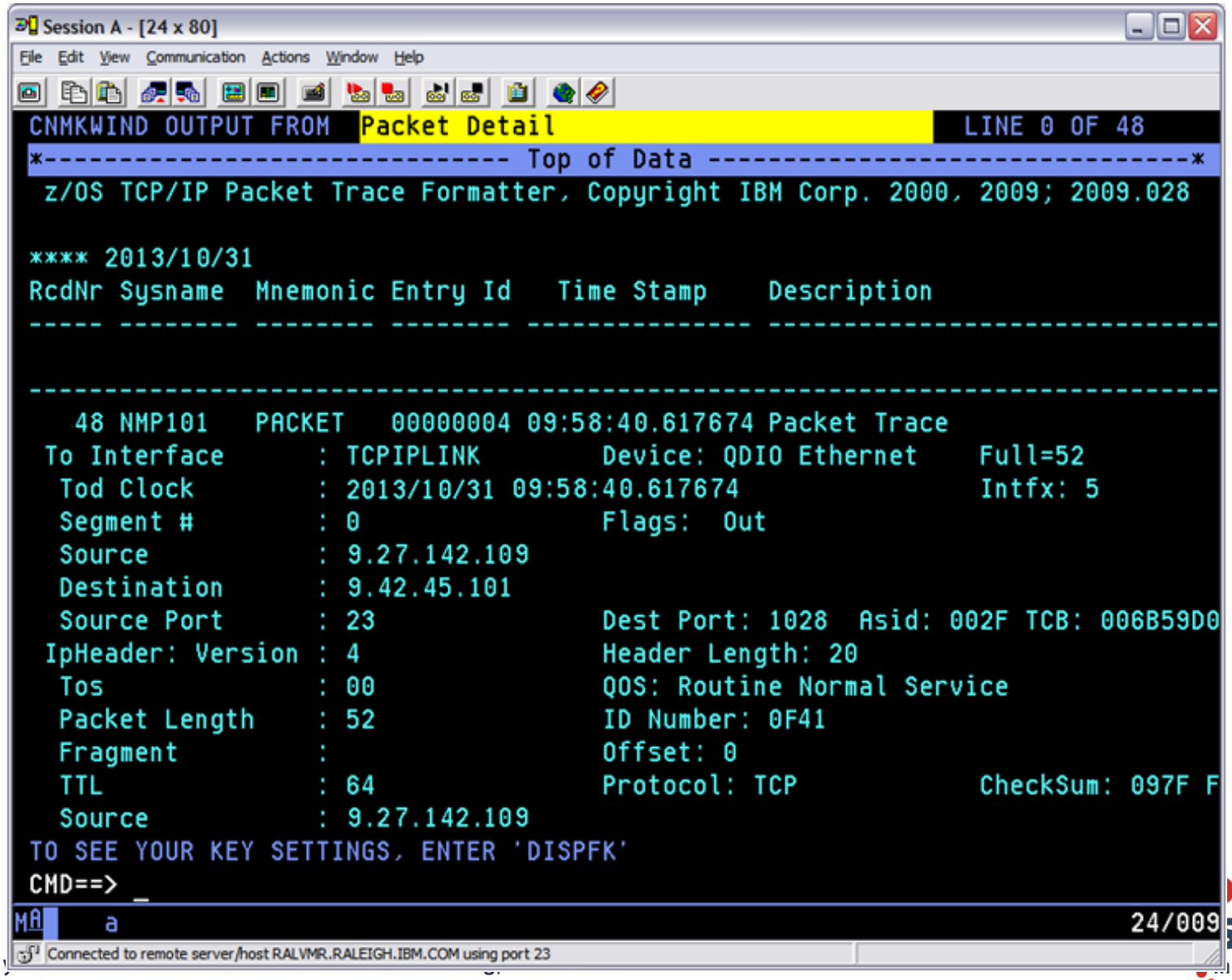
# Scenario 1: Individual packets for the session



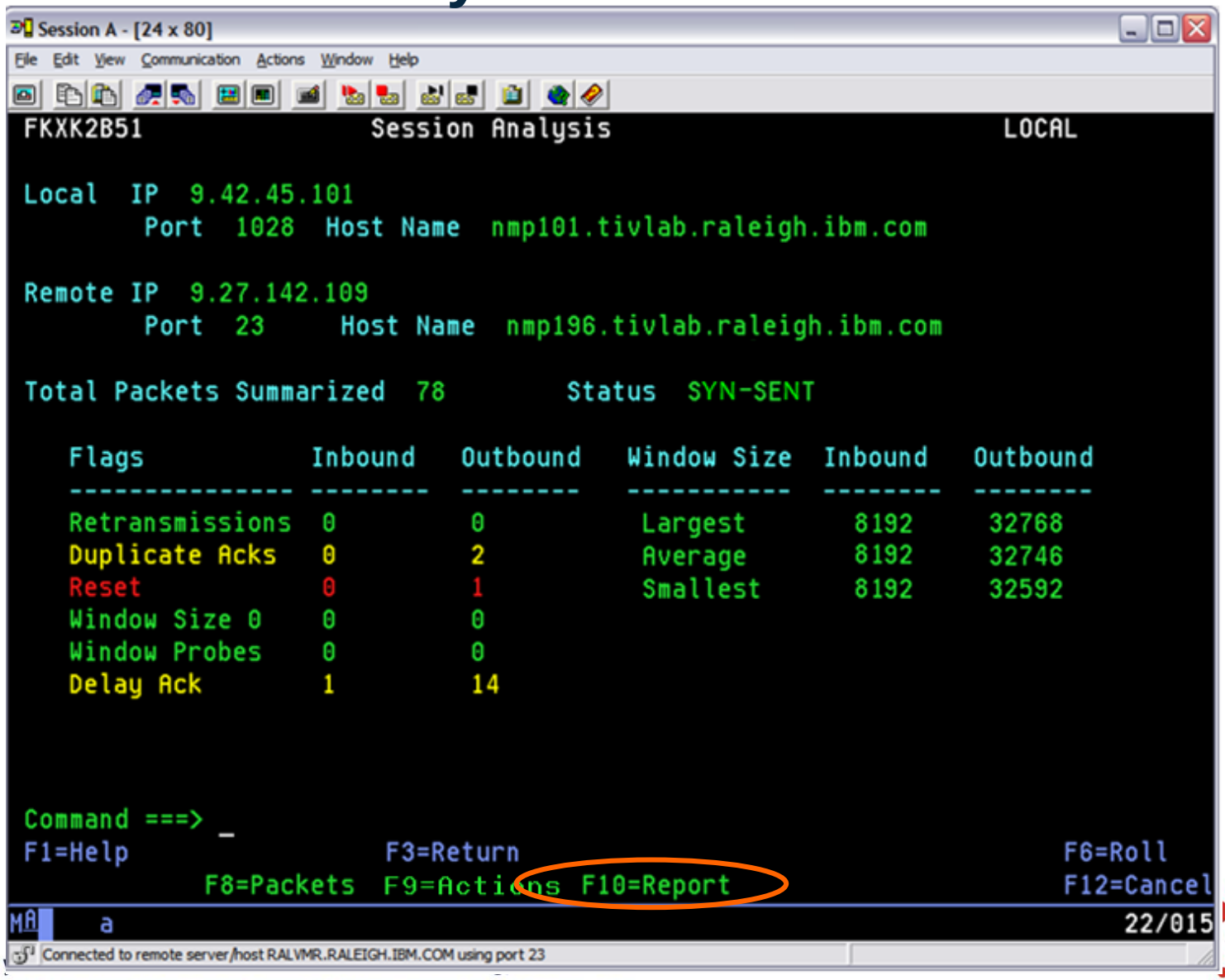

duplicate ack

delayed ack

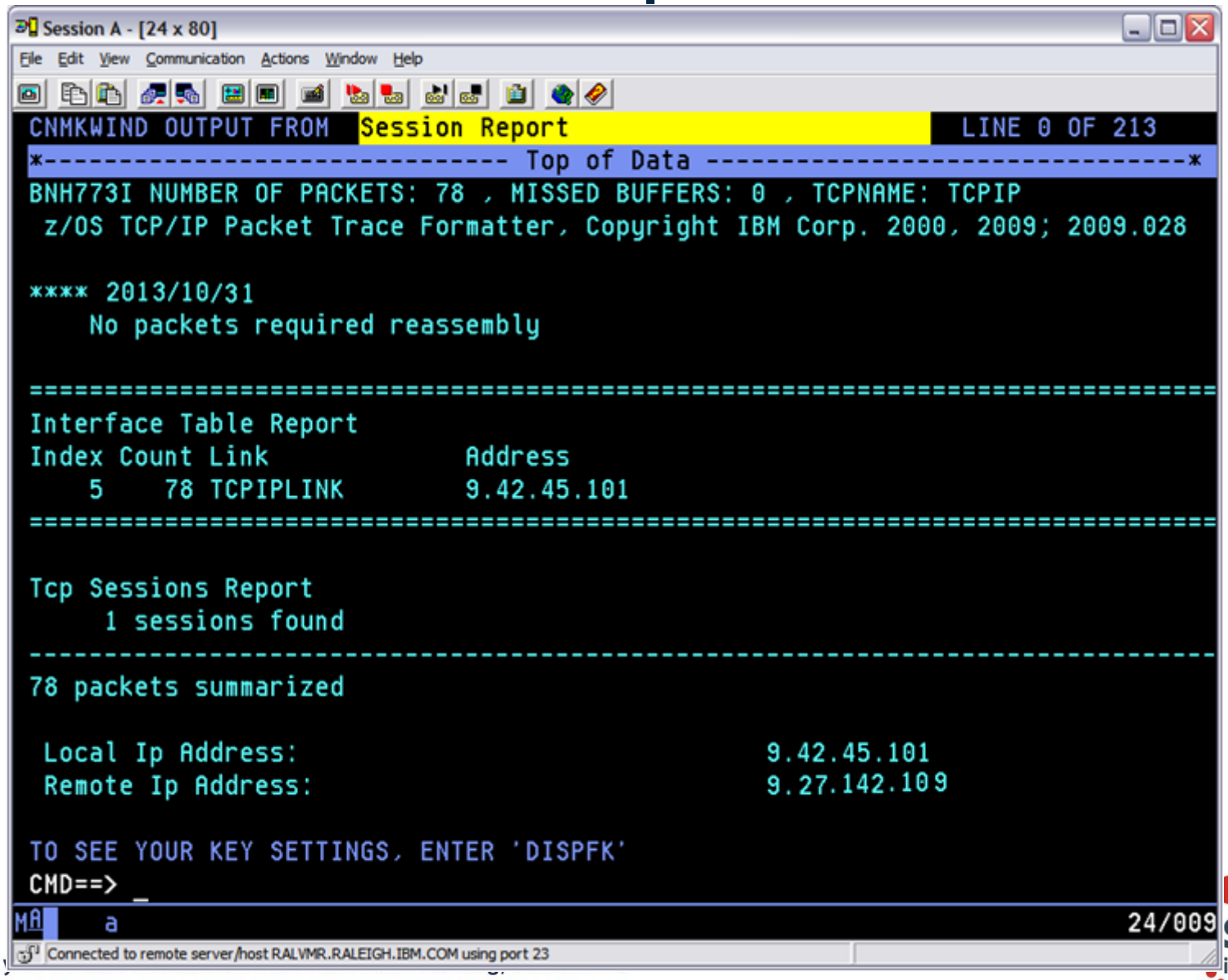
# Scenario 1: Packet Details



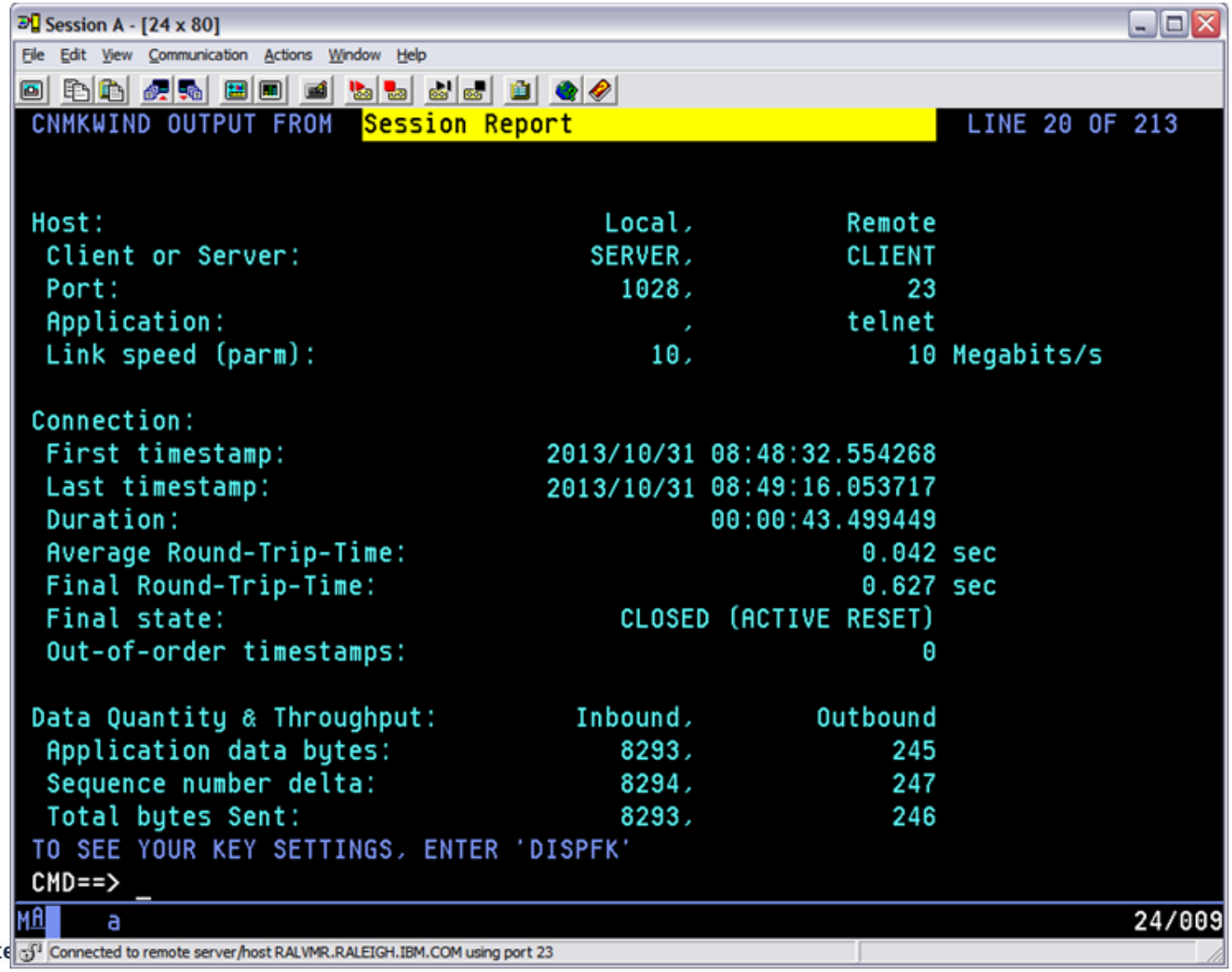
# Scenario 1: Analysis for selected session



# Scenario 1: Session Report

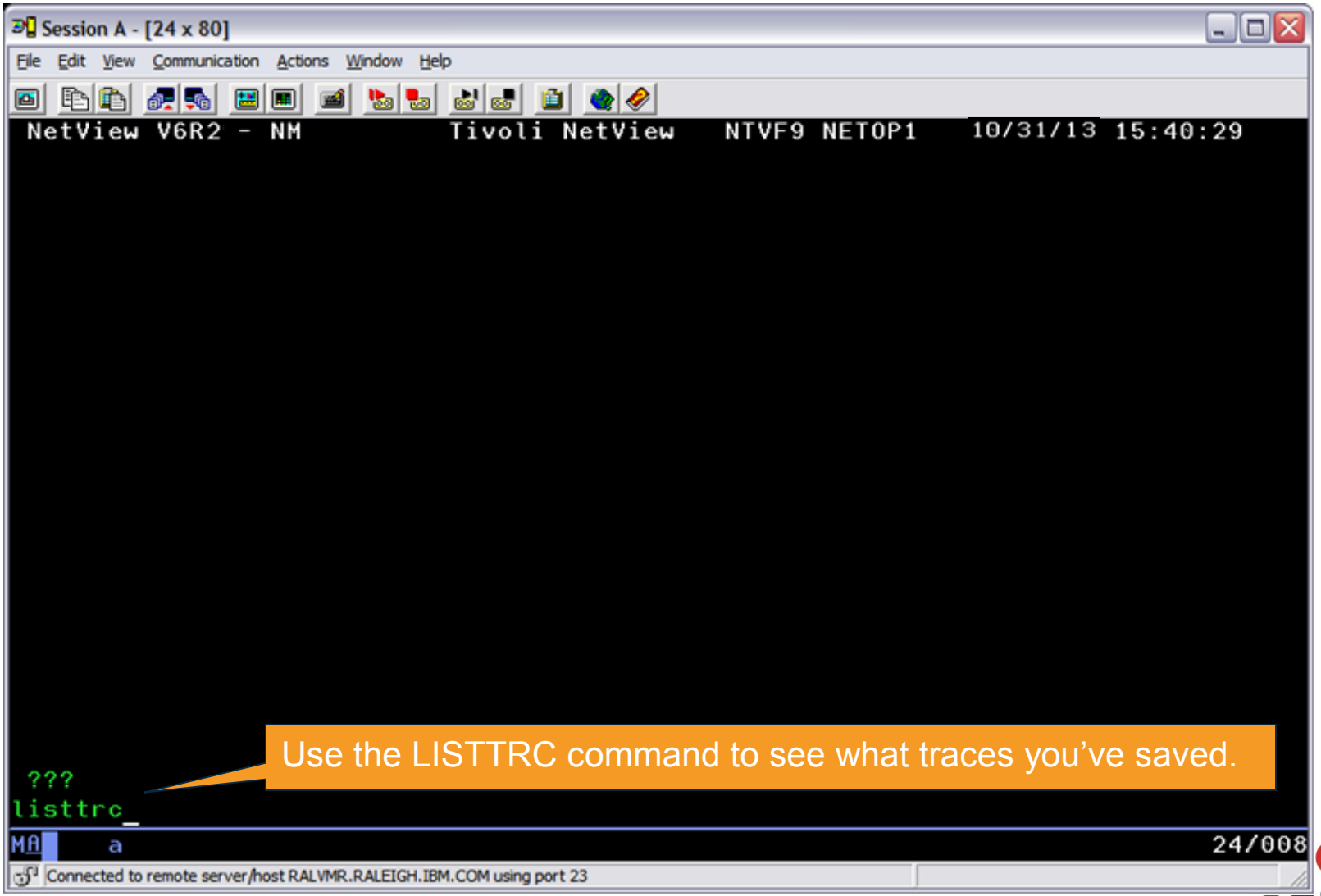


# Scenario 1: Session Report (cont.)

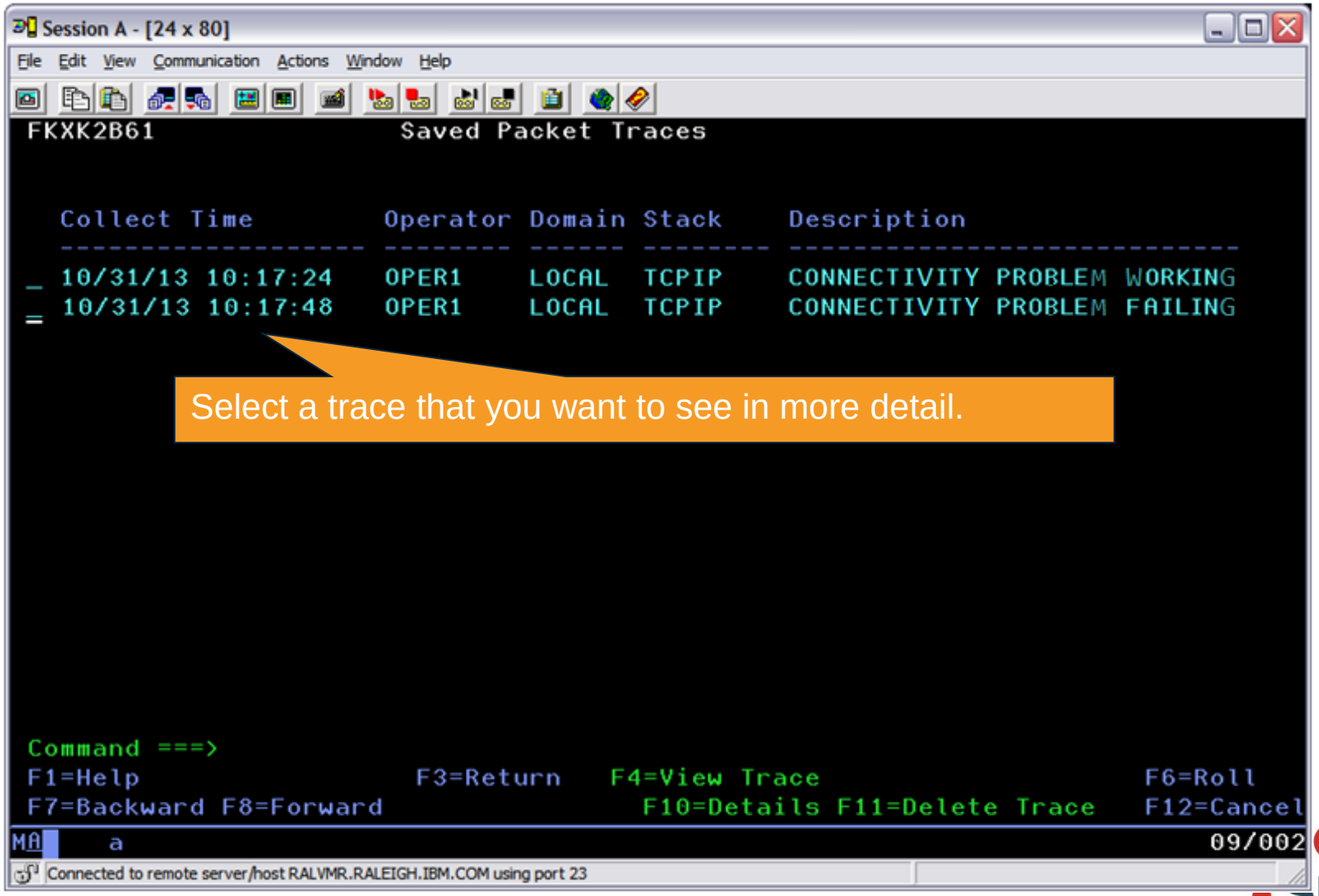



Complete

# Scenario 1: Packet Trace



# Scenario 1: Packet Trace

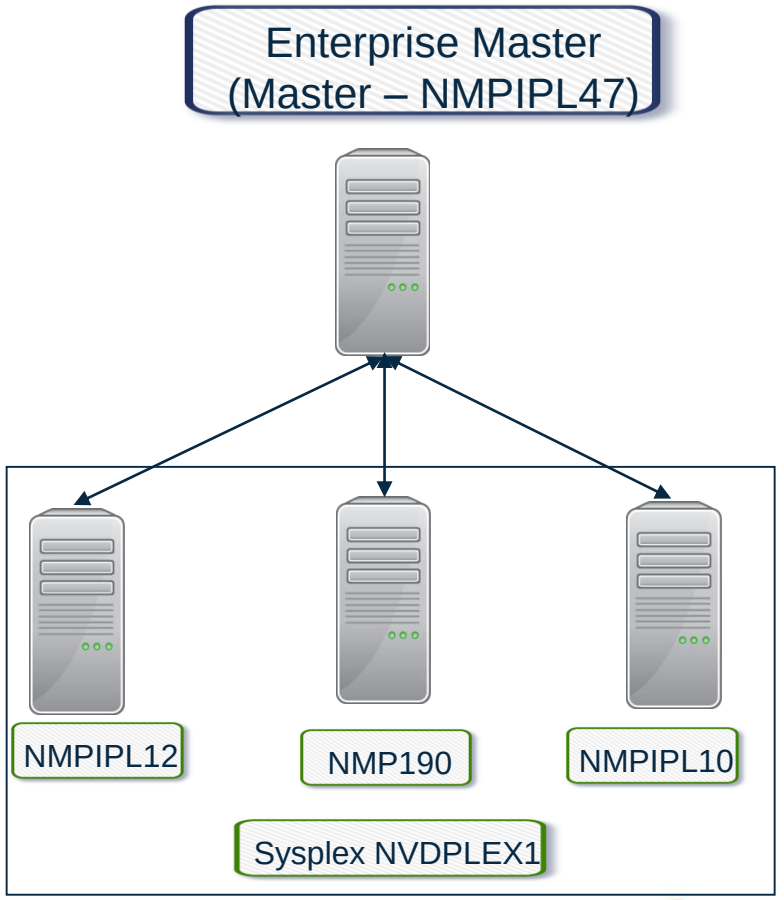


# Packet Trace Summary

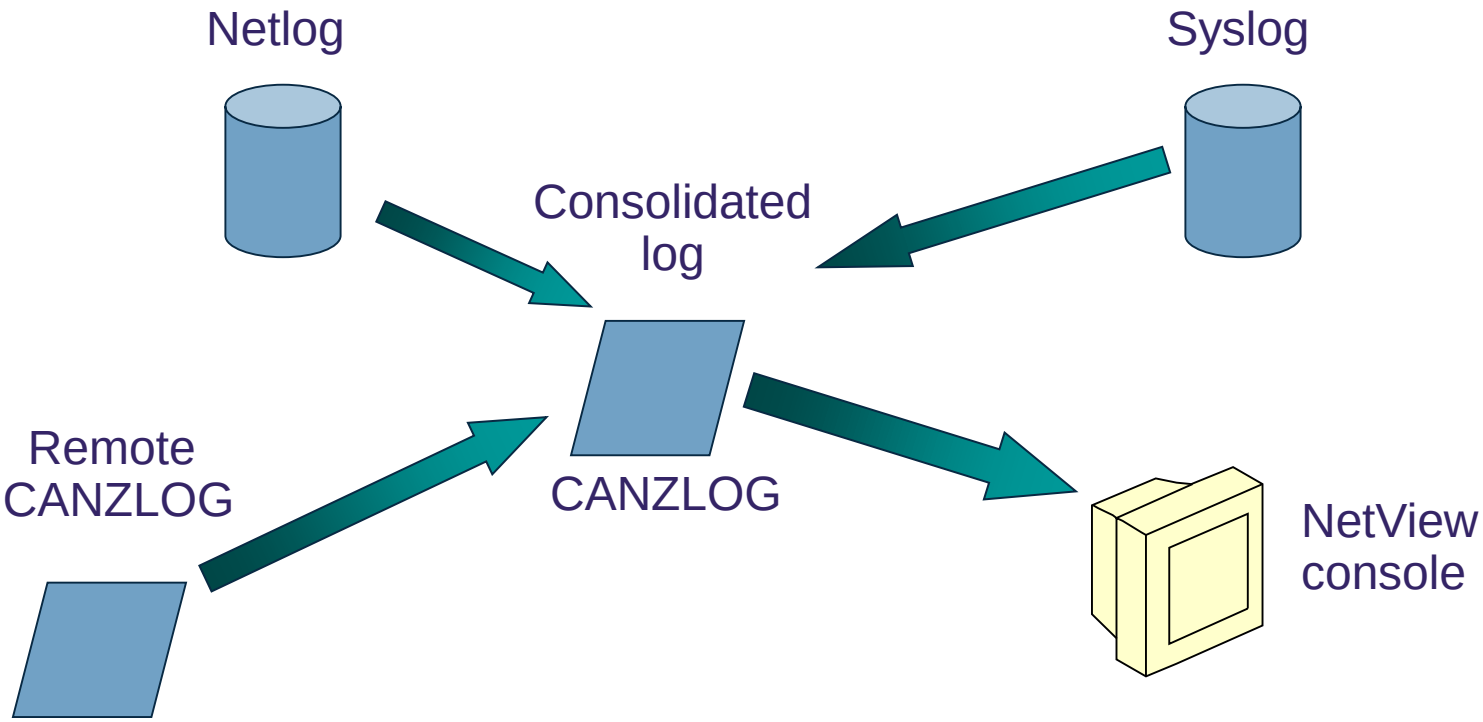
- Packet trace can be controlled through the global trace or multiple instance traces
  - “Global” trace:  only 1 per stack
  - “Instance” traces:  up to 32 per stack
- Multi-trace function requires z/OS Communications Server V2.1 and NetView for z/OS V6.2 or later.
- Multiple traces can be useful for tracing specific parts of a network, avoiding extraneous data.
- Traces can be saved in CTRACE format for further analysis in IPCS.

# Scenario 2: 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 new 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 Enhancements

- Recording of messages before NetView SSI initializes (early IPL)
- Truncation of long MLWTOs
- Remote browse support
- New formatting options
- Relative time filter

# Canzlog Remote Browse

- The updated BROWSE command can accept a remote domain, a remote alias, a Canzlog group, or a sysplex name.
- The BROWSE command can browse a data set member from a remote domain, such as the CNMSTYLE member.
- A Canzlog group (a set of arbitrary NetView domains in the enterprise) can be defined in the CNMSTYLE member.
- The Canzlog panel has been updated to accept a remote Canzlog browse request (Target).

# 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 2: 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
```

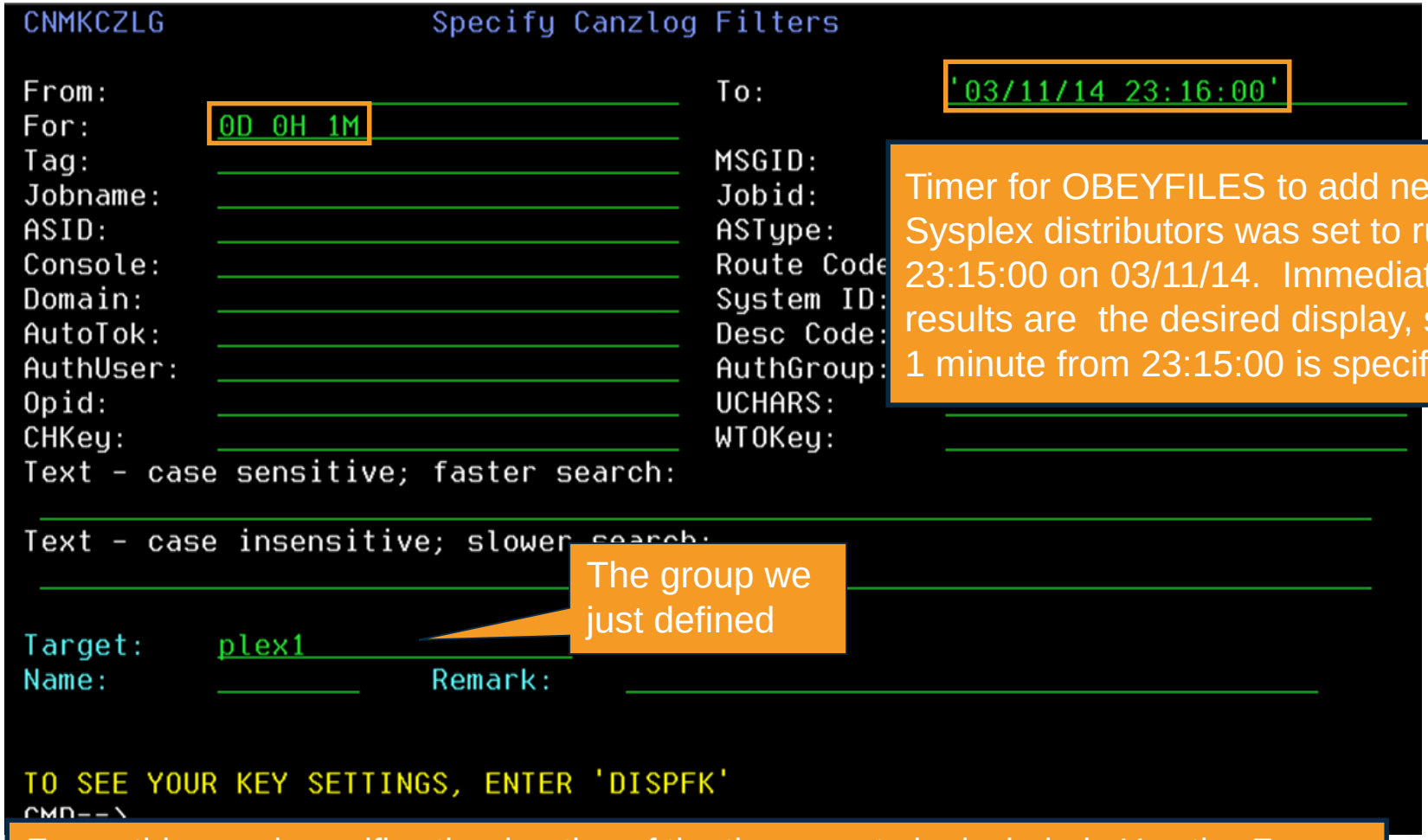
Issue RESTYLE ENT to dynamically add a GROUP.

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 2: Relative Time

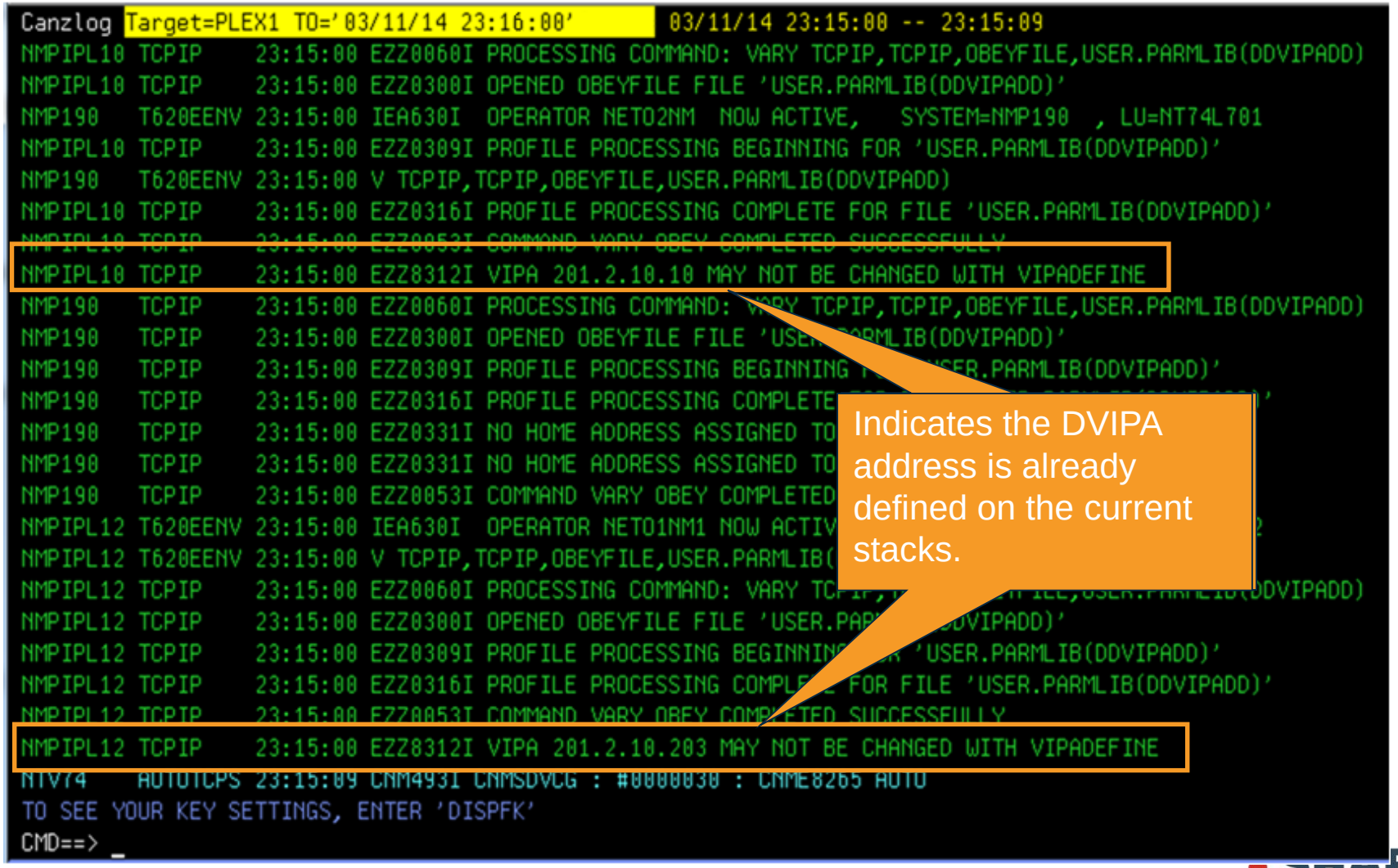



Timer for OBEYFILES to add new Sysplex distributors was set to run at 23:15:00 on 03/11/14. Immediate results are the desired display, so only 1 minute from 23:15:00 is specified.

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 2: Filtered Results

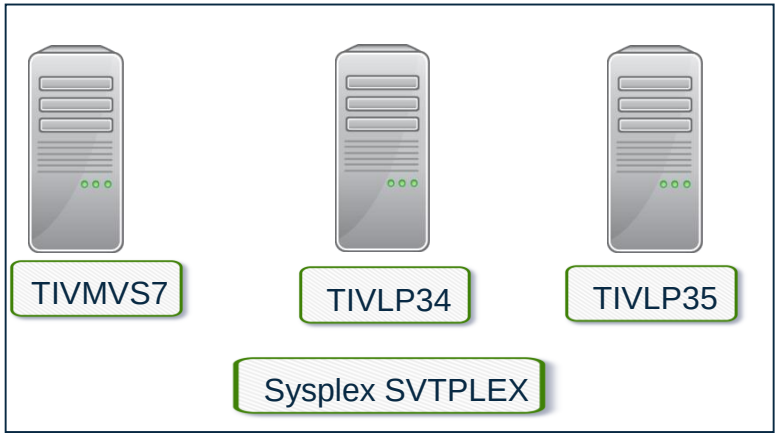


# Summary

- CANZLOG brings together syslog and netlog messages, from local and/or remote systems
- Very robust, flexible filtering
  - Any message attribute or combination
    - “What happened over the weekend?”
    - “Show me all the IEF123 messages from systems X, Y and Z.”
    - “I need to see all the ABC* and DEF* messages from jobs JOB1 and JOB2 during first shift last Tuesday with descriptor code 2.”
  - Scope
    - Common (public): available to all operators (subject to authorization check)
    - Task (private): available only to operator who defined the filter criteria
  - Actions
    - Save: save filter to storage and on disk
    - Replace: replace an existing filter in storage and on disk
    - Delete: delete filter from storage and disk
- Seamless archiving and retrieval
- Export to IBM Service

# Scenario 3: Monitoring Sysplex Distributor

- Scenario:
  - Sysplex Distributor seems to be favoring one z/OS system significantly more than others for new TCP connections. Why?
- Resolution steps:
  - Check the WLM weight for the target systems
  - Consider machine types



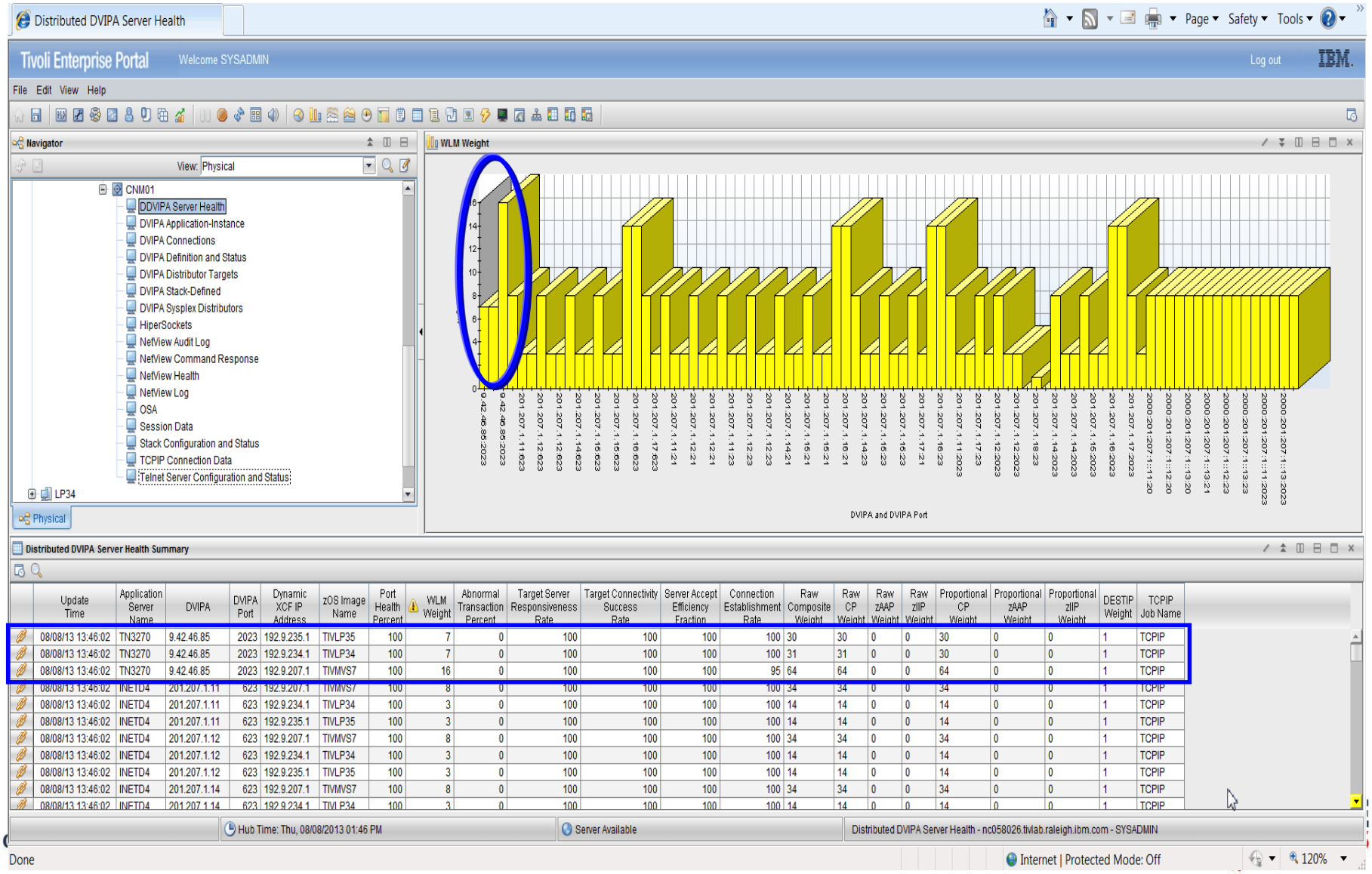
# NetView DVIPA Monitoring

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

# Scenario 3: Sysplex Distributor Favoring a System

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

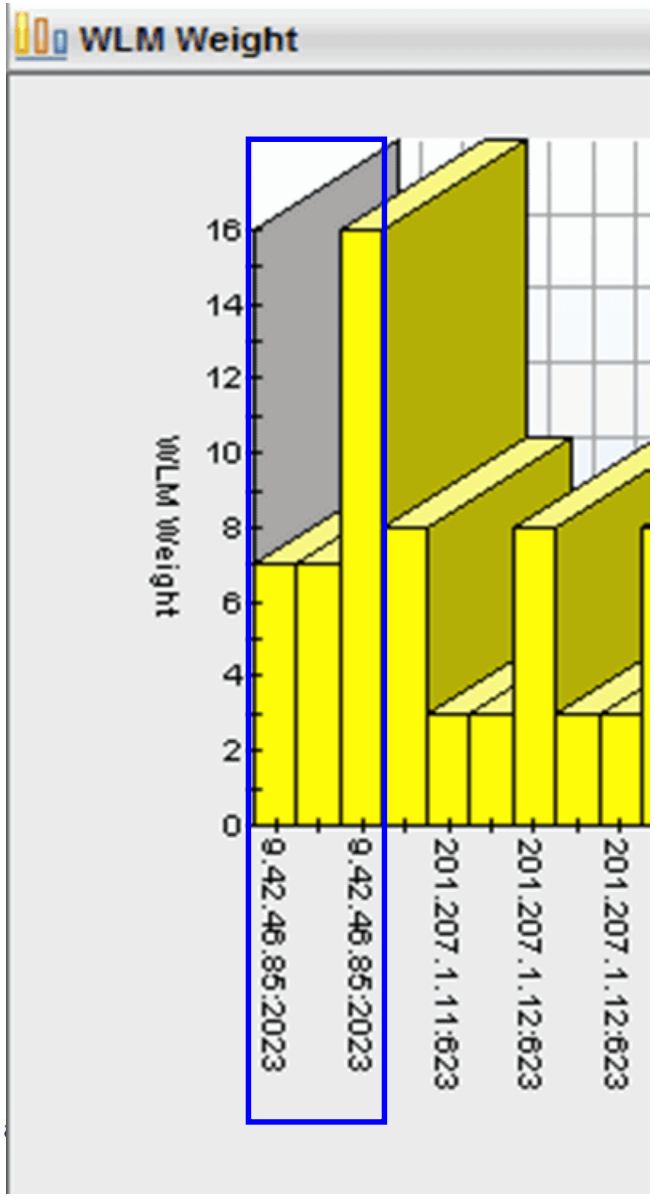
# Scenario 3: WLM Weight and DDVIPA Server Health




| 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 3: WLM Weight Bar Chart

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



# Scenario 3: 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).

# NetView for z/OS in the Portal (and more discovered host resources)

- IP Connections (active and inactive)
- DVIPA
  - Connections
  - Connection routing
  - Definition and Status
  - Sysplex Distributors
  - Targets
  - Server Health
  - Unhealthy Servers
  - Application Instances
  - Workload

- **NetView for z/OS also provides line-mode commands and 3270 formatting facilities for all data listed on this slide.**

- IP Stack Configuration & Status
- Telnet Server Configuration & Status
- HiperSocket Interfaces
- OSA Ports
- Audit Log
- Command Responses
- NetView Log
- SNA Session Data
- NetView Health (current & history)
- Active/Active Sites (several workspaces)

# DVIPA line-mode and 3270 formatting samples

- CNMSDVIP DVIPSTAT definition and status information about DVIPAs
- CNMSPLEX DVIPPLEX information about DVIPA sysplex distributors
- CNMSDVPC DVIPCONN DVIPA connections
- CNMSTARG DVIPTARG DVIPA distributed targets
- CNMSDVPH DVIPHLTH distributed DVIPA server health information
- CNMSDDCR DVIPDDCR distributed DVIPA connection routing information
- CNMSVPRT VIPAROUT status information about VIPA routes

# Line-mode and 3270 formatting samples

- CNMSTCPC TCPCONN TCP/IP connection information
- CNMSSTAC STACSTAT configuration and status information about TCP/IP stacks
- CNMSIFST IFSTAT TCP/IP stack interfaces
- CNMSTNST TELNSTAT configuration and status information about Telnet servers
- CNMSTPST TNPTSTAT configuration and status information about Telnet server ports
- CNMSNVST NVSTAT configuration and status information about the NetView domains known to this NetView program
- CNMSOSAP OSAPORT OSA channel and port information
- CNMSHIPR HIPERSOC View HiperSockets adapter information

# Summary

- NetView monitors a wide variety of DVIPA metrics and brings them together for easy analysis
- Allows quick assessment of DDIPVA Server health
- Allows easy determination of problems

# More Information

- 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 website

  http://www.ibm.com/software/tivoli/products/netview-zos/
- NetView customer forum

  http://tech.groups.yahoo.com/group/NetView/
- NetView media gallery

  https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli+System+z+Monitoring+and+Application+Management/page/Media+Gallery+for+Tivoli+NetView+for+zOS
- 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=SSANTA_1.2.0%2F0-1-1&lang=en

# IBM System z Service Management critical for moving to Mobile, Big Data and Cloud

IBM continues to improve z/OS environment to support new technologies

- IBM SmartCloud Analytics – Log Analysis z/OS Insight Packs 1.1.0.1
- IBM Service Management Suite for z/OS V1.2
- IBM Tivoli OMEGAMON Performance Management Suite for z/OS V5.3.0
- IBM Tivoli OMEGAMON XE on z/OS 5.3.0, IBM Tivoli OMEGAMON Dashboard Edition on z/OS 5.3.0, IBM Tivoli OMEGAMON XE for Messaging for z/OS 7.3.0, IBM Tivoli OMEGAMON XE for CICS on z/OS 5.3.0, IBM Tivoli OMEGAMON XE for Storage on z/OS 5.3.0
- IBM Tivoli System Automation for z/OS V3.5
- IBM Automation Control for z/OS V1.1.1
- IBM Tivoli NetView for z/OS V6.2.1
- IBM Tivoli NetView Monitoring for GDPS V6.2.1
- IBM Tivoli Workload Scheduler for z/OS V9.2

Learn More: http://www-01.ibm.com/software/os/systemz/itsm/

Follow us on Service Management Connect:
https://www.ibm.com/developerworks/servicemanagement/z/

And, Mainframe Insights:
https://www-304.ibm.com/connections/blogs/systemz/?lang=en_us

Twitter: @ServMgmtConnect @systemz #mainframe #servicemgmt

# Please fill out your session evaluation

- NetView for z/OS:  IP Management Topics and Solutions
- Session # 16833
- QR Code:


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