

# 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.**



# Acknowledgements, Disclaimers and Trademarks



© Copyright IBM Corporation 2014. All rights reserved.

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](http://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](http://ibm.com/legal/copytrade.shtml)

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# 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



Session B - [24 x 80]

File Edit View Communication Actions Window Help

Host: RALVMR.RALEIGH.IBI Port: 23 LU Name: Disconnect

CNM4NVIP NetView IP Management Functions Menu

Type the number or move the cursor to a function and press Enter

1. Ping a device (PING)
2. Trace the route to a device (TRACERTE)
3. Check TCP connection status (IPSTAT)
4. Work with IP traces (IPTRACE)  
for SP: \_\_\_\_\_
5. Manage IP Active Monitoring (IPMAN)
6. Issue SNMP commands (NVSNMP)
7. Manage Sysplex
8. Manage DVIPA
9. Check the status of an IP port (TESTPORT)
10. Show EE information for a VTAM resource (DIS PATH)

Command ==> \_

F1=Help F3=Return F6=Roll F12=Cancel

M B 22/015

Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23

# 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

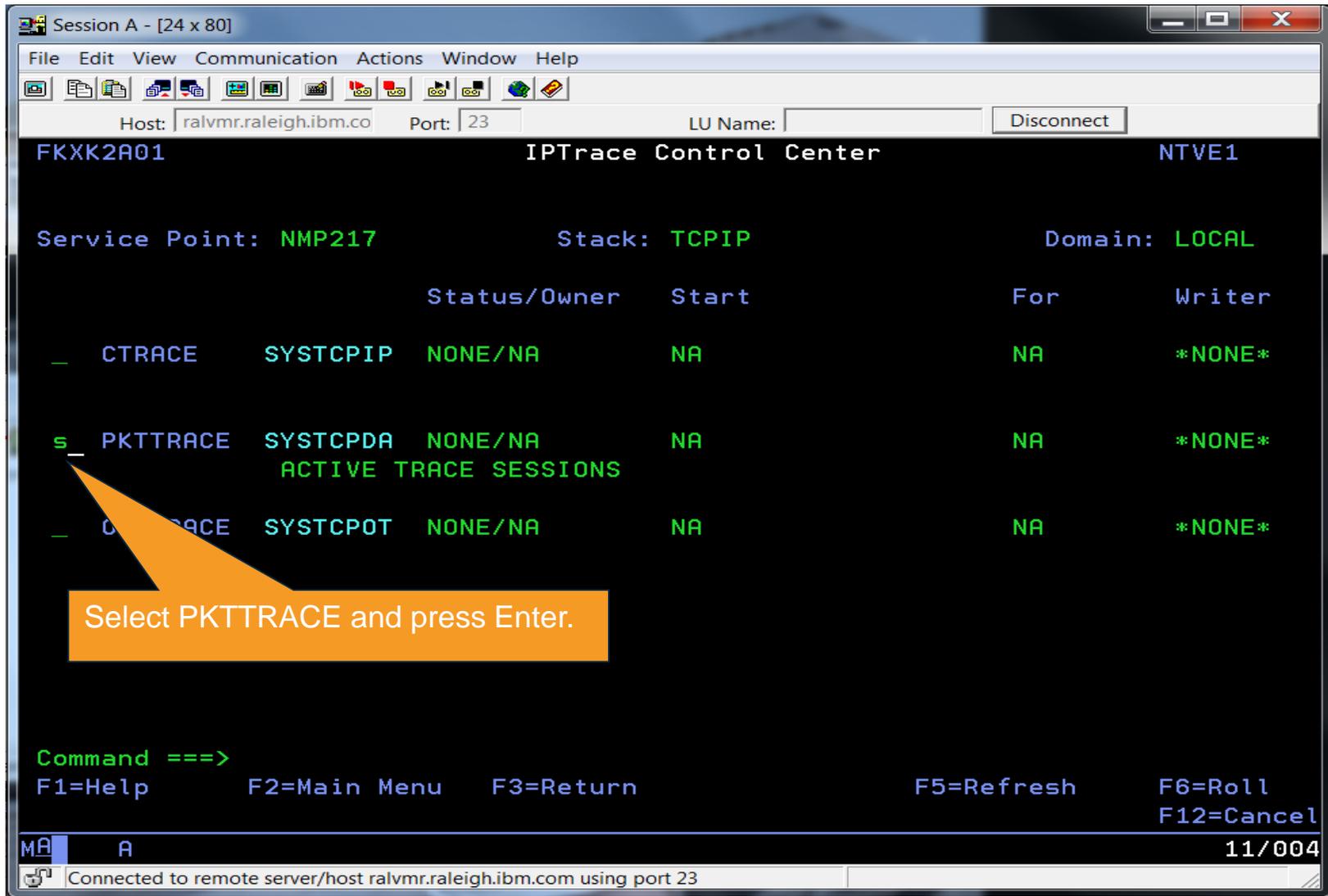
# Scenario: Packet Trace Connectivity



- 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



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2A01 IPTrace Control Center NTVE1

Service Point: NMP217 Stack: TCPIP Domain: LOCAL

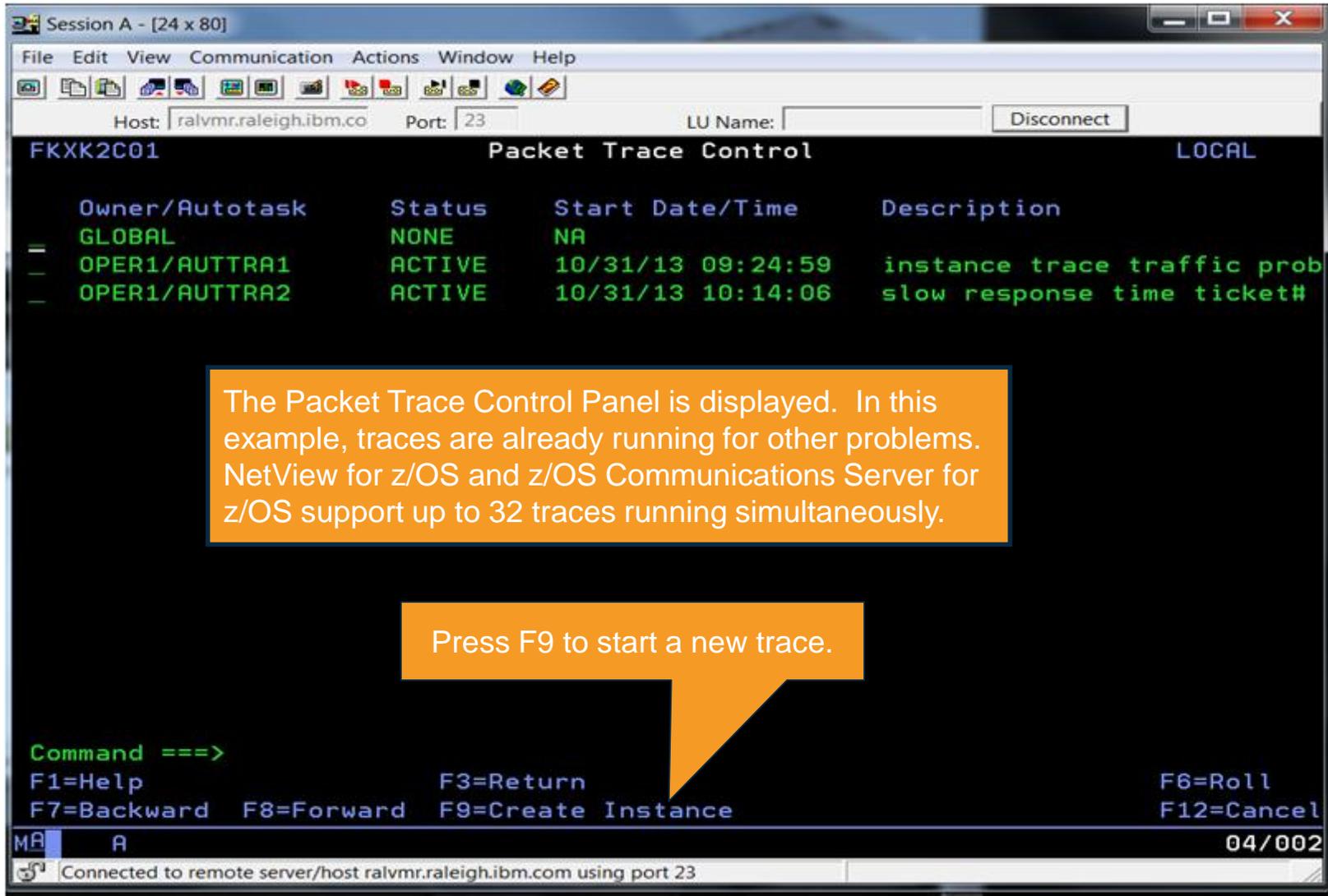
Status/Owner	Start	For	Writer
CTTRACE SYSTCPIP NONE/NA	NA	NA	*NONE*
<b>s</b> PKTRACE SYSTCPDA NONE/NA	NA	NA	*NONE*
ACTIVE TRACE SESSIONS			
CTTRACE SYSTCPIP NONE/NA	NA	NA	*NONE*

Command ==>  
F1=Help F2=Main Menu F3=Return F5=Refresh F6=Roll  
F12=Cancel

MA A 11/004

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

# Scenario 1: Packet Trace



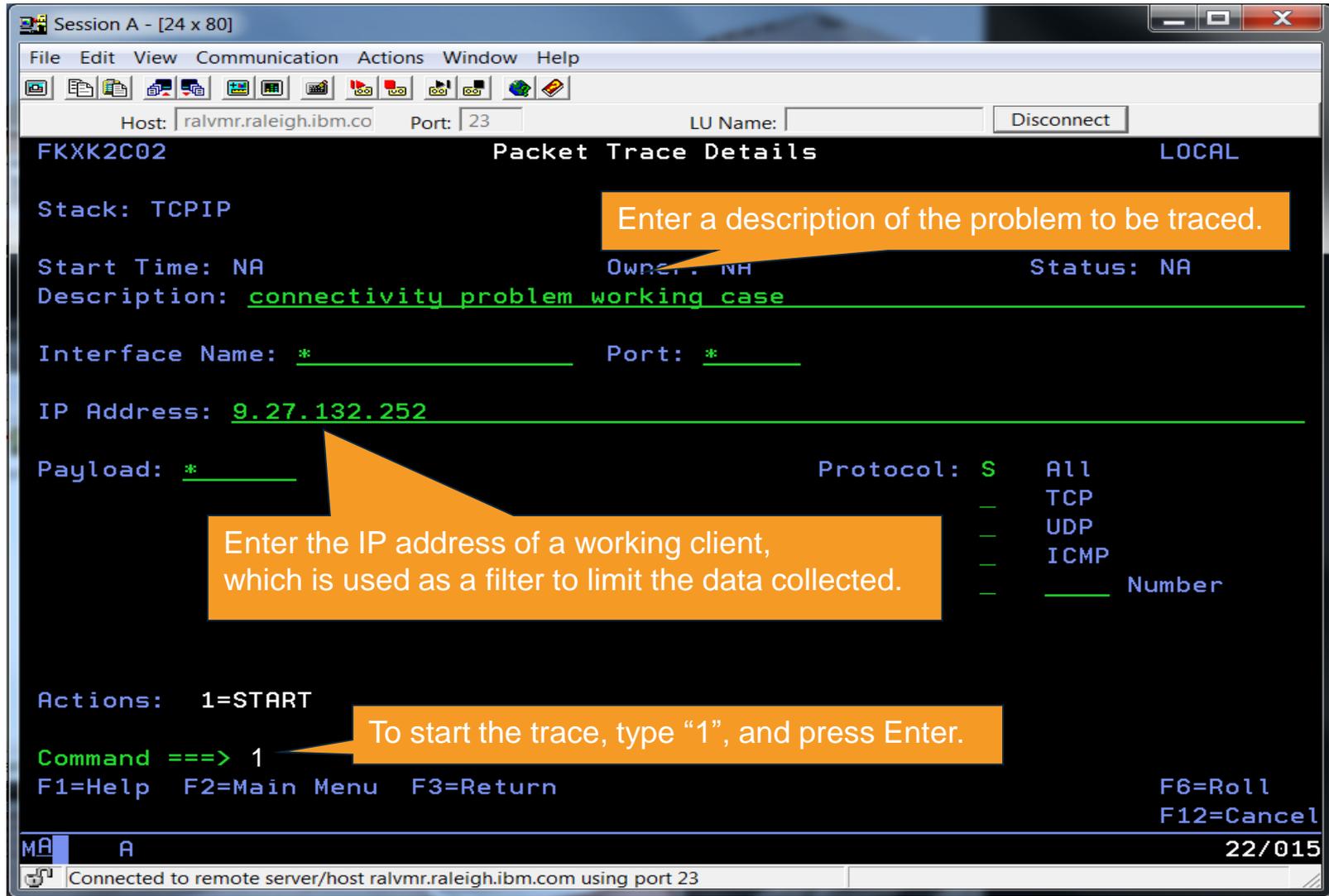
Owner/Autotask	Status	Start Date/Time	Description
GLOBAL	NONE	NA	
OPER1/AUTTRA1	ACTIVE	10/31/13 09:24:59	instance trace traffic prob
OPER1/AUTTRA2	ACTIVE	10/31/13 10:14:06	slow response time ticket#

Command ==>  
F1=Help                      F3=Return                      F6=Roll  
F7=Backward    F8=Forward    F9=Create Instance              F12=Cancel

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



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2C02 Packet Trace Details LOCAL

Stack: TCPIP

Start Time: NA Owner: NH Status: NA

Description: connectivity problem working case

Interface Name: \* Port: \*

IP Address: 9.27.132.252

Payload: \* Protocol: S All  
TCP  
UDP  
ICMP  
Number

Actions: 1=START

Command ==> 1

F1=Help F2=Main Menu F3=Return F6=Roll F12=Cancel

MA A 22/015

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

Enter a description of the problem to be traced.

Enter the IP address of a working client, which is used as a filter to limit the data collected.

To start the trace, type "1", and press Enter.

# Scenario 1: Packet Trace

```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect
FKXK2C01 Packet Trace Control LOCAL

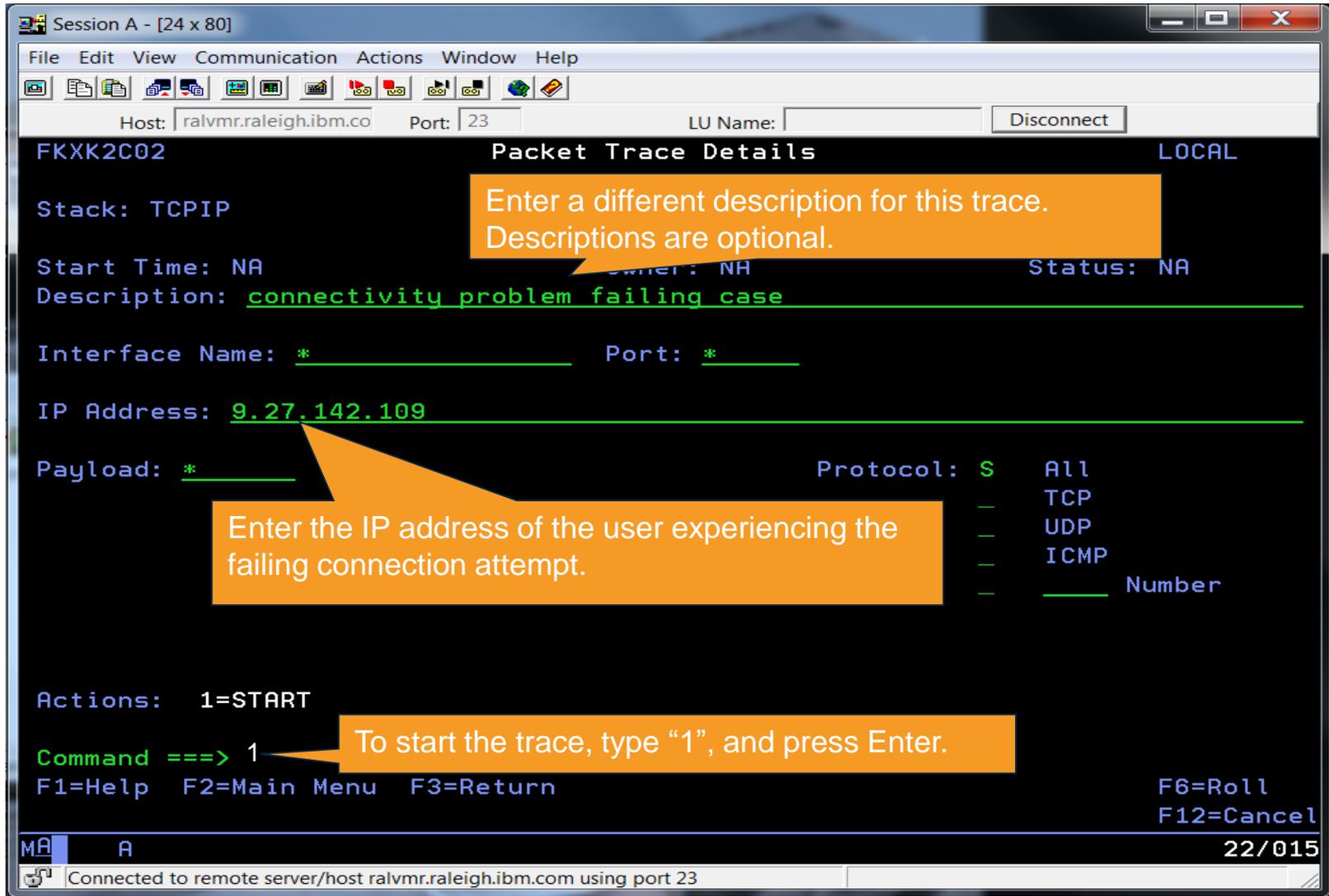
Owner/Autotask      Status      Start Date/Time      Description
- GLOBAL            NONE        NA
- OPER1/AUTTRA1     ACTIVE      10/31/13 09:24:59     instance trace traffic prob
- OPER1/AUTTRA2     ACTIVE      10/31/13 10:14:06     slow response time ticket#
- OPER1/AUTTRA3     ACTIVE      10/31/13 10:17:24     connectivity problem workin

DSI633I 'PKTS START' COMMAND SUCCESSFULLY COMPLETED
Command ==>
F1=Help              F3=Return           F6=Roll
F7=Backward          F8=Forward          F9=Create Instance  F12=Cancel

MA  A 04/002
Connected to remote server/host ralvmr.raleigh.ibm.com using port 23
```

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

# Scenario 1: Packet Trace



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2C02 Packet Trace Details LOCAL

Stack: TCPIP

Start Time: NA Owner: NA Status: NA

Description: connectivity problem failing case

Interface Name: \* Port: \*

IP Address: 9.27.142.109

Payload: \* Protocol: S All  
TCP  
UDP  
ICMP  
Number

Actions: 1=START

Command ==> 1

F1=Help F2=Main Menu F3=Return F6=Roll F12=Cancel

22/015

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

Enter a different description for this trace. Descriptions are optional.

Enter the IP address of the user experiencing the failing connection attempt.

To start the trace, type "1", and press Enter.

# Scenario 1: Packet Trace

```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect
FKXK2C01 Packet Trace Control LOCAL

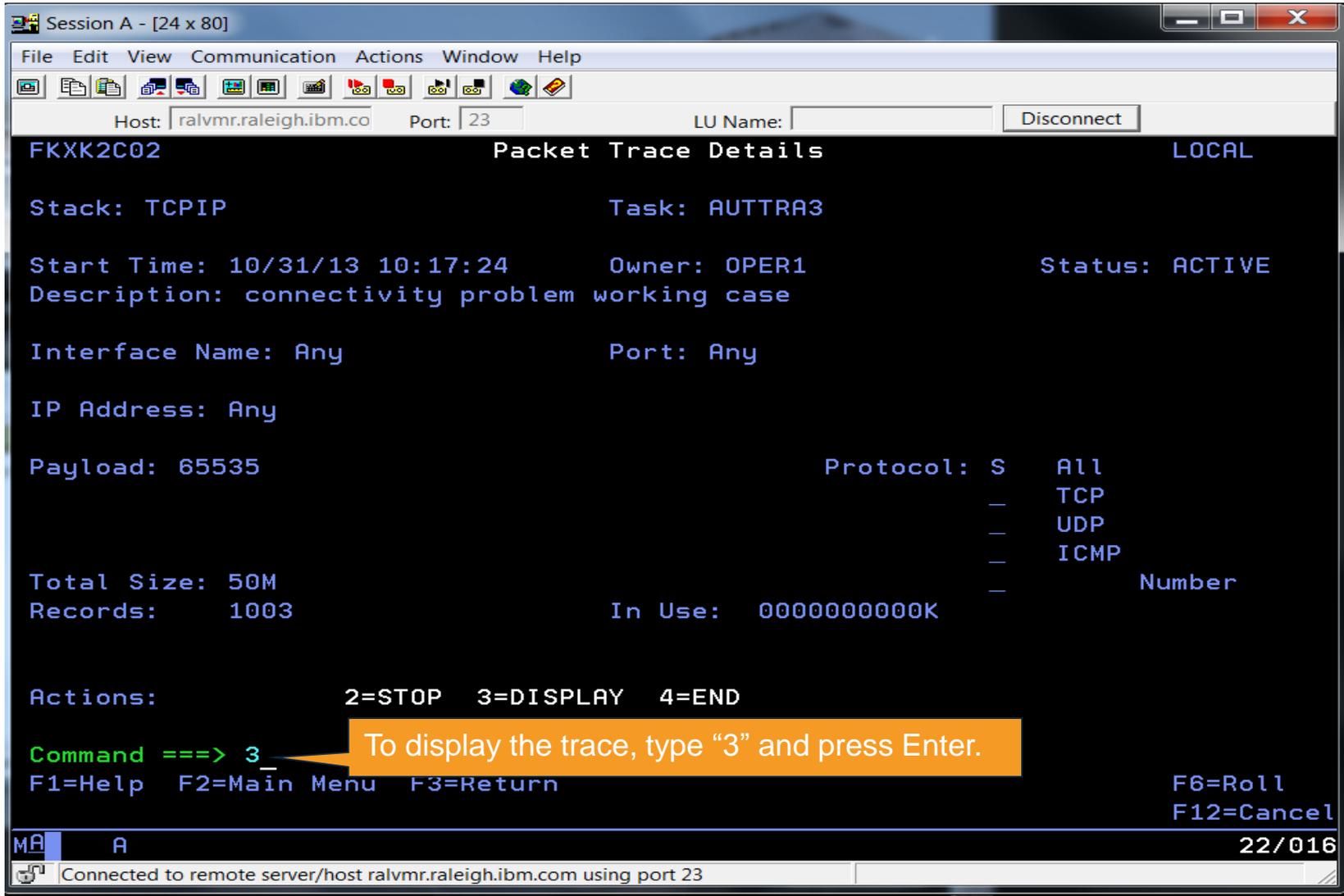
  Owner/Autotask      Status      Start Date/Time      Description
-  GLOBAL              NONE        NA
-  OPER1/AUTTRA1       ACTIVE      10/31/13 09:24:59     instance trace traffic prob
-  OPER1/AUTTRA2       ACTIVE      10/31/13 10:14:06     slow response time ticket#
-  OPER1/AUTTRA3       ACTIVE      10/31/13 10:17:24     connectivity problem workin
-  OPER1/AUTTRA4       ACTIVE      10/31/13 10:17:48     connectivity problem failin

DSI633I 'PKTS START' COMMAND SUCCESSFULLY COMPLETED
Command ==>
F1=Help           F3=Return          F6=Roll
F7=Backward      F8=Forward         F9=Create Instance F12=Cancel

MA  A 06/002
Connected to remote server/host ralvmr.raleigh.ibm.com using port 23
```

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



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXX2C02 Packet Trace Details LOCAL

Stack: TCPIP Task: AUTTRA3

Start Time: 10/31/13 10:17:24 Owner: OPER1 Status: ACTIVE  
Description: connectivity problem working case

Interface Name: Any Port: Any

IP Address: Any

Payload: 65535 Protocol: S All  
— TCP  
— UDP  
— ICMP  
— Number

Total Size: 50M  
Records: 1003 In Use: 0000000000K

Actions: 2=STOP 3=DISPLAY 4=END

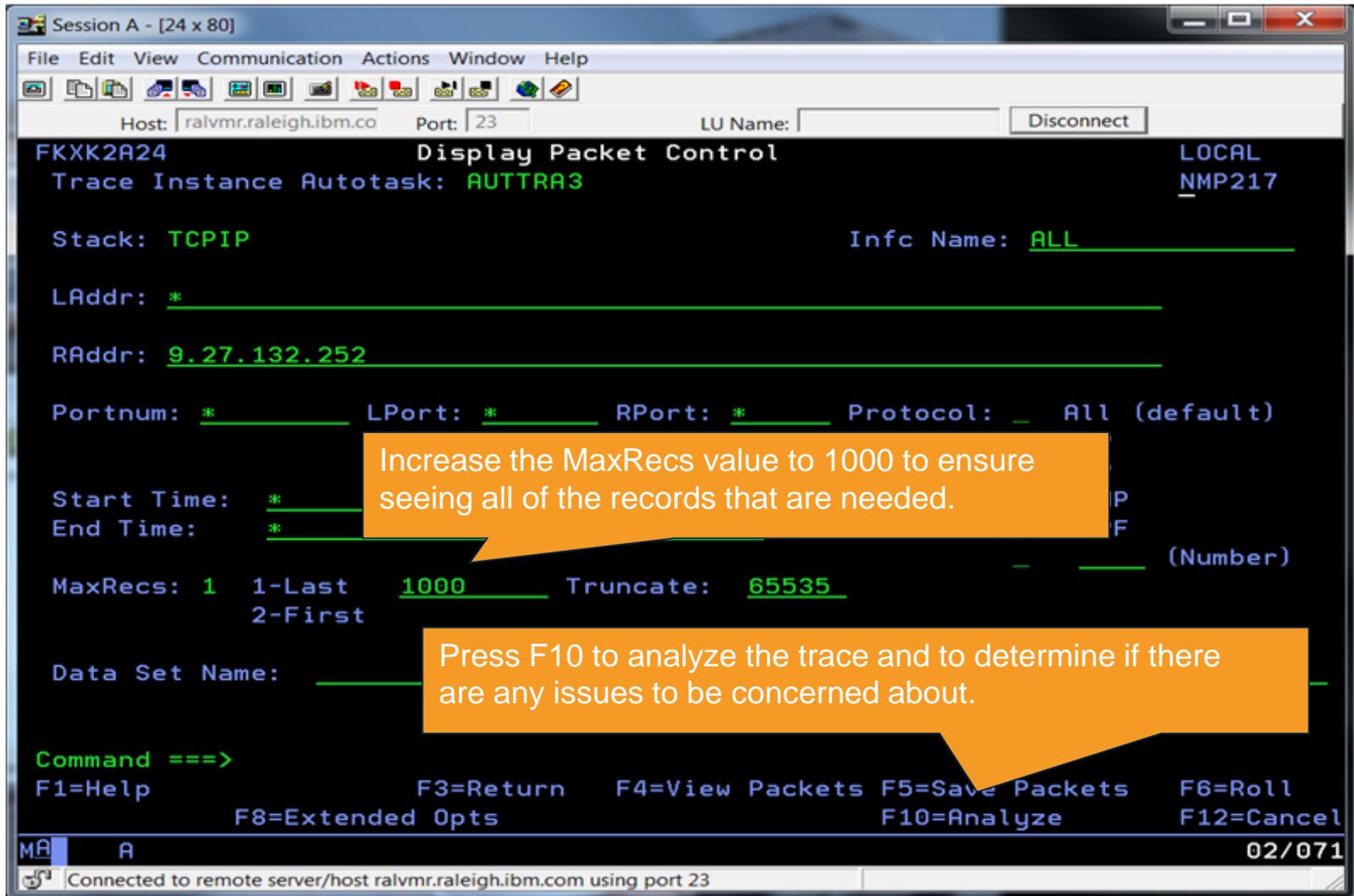
Command ==> 3 To display the trace, type "3" and press Enter.

F1=Help F2=Main Menu F3=Return F6=Roll F12=Cancel

MA A 22/016

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

# Scenario 1: Packet Trace



The screenshot shows a terminal window titled "Session A - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main content area is titled "Display Packet Control" and shows configuration for a trace instance named "AUTTRA3".

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2A24 Display Packet Control LOCAL NMP217

Trace Instance Autotask: AUTTRA3

Stack: TCPIP Infc Name: ALL

LAddr: \*

RAddr: 9.27.132.252

Portnum: \* LPort: \* RPort: \* Protocol: All (default)

Start Time: \* End Time: \* (Number)

MaxRecs: 1 1-Last 1000 Truncate: 65535 2-First

Data Set Name:

Command ==>

F1=Help F3=Return F4=View Packets F5=Save Packets F6=Roll  
F8=Extended Opts F10=Analyze F12=Cancel

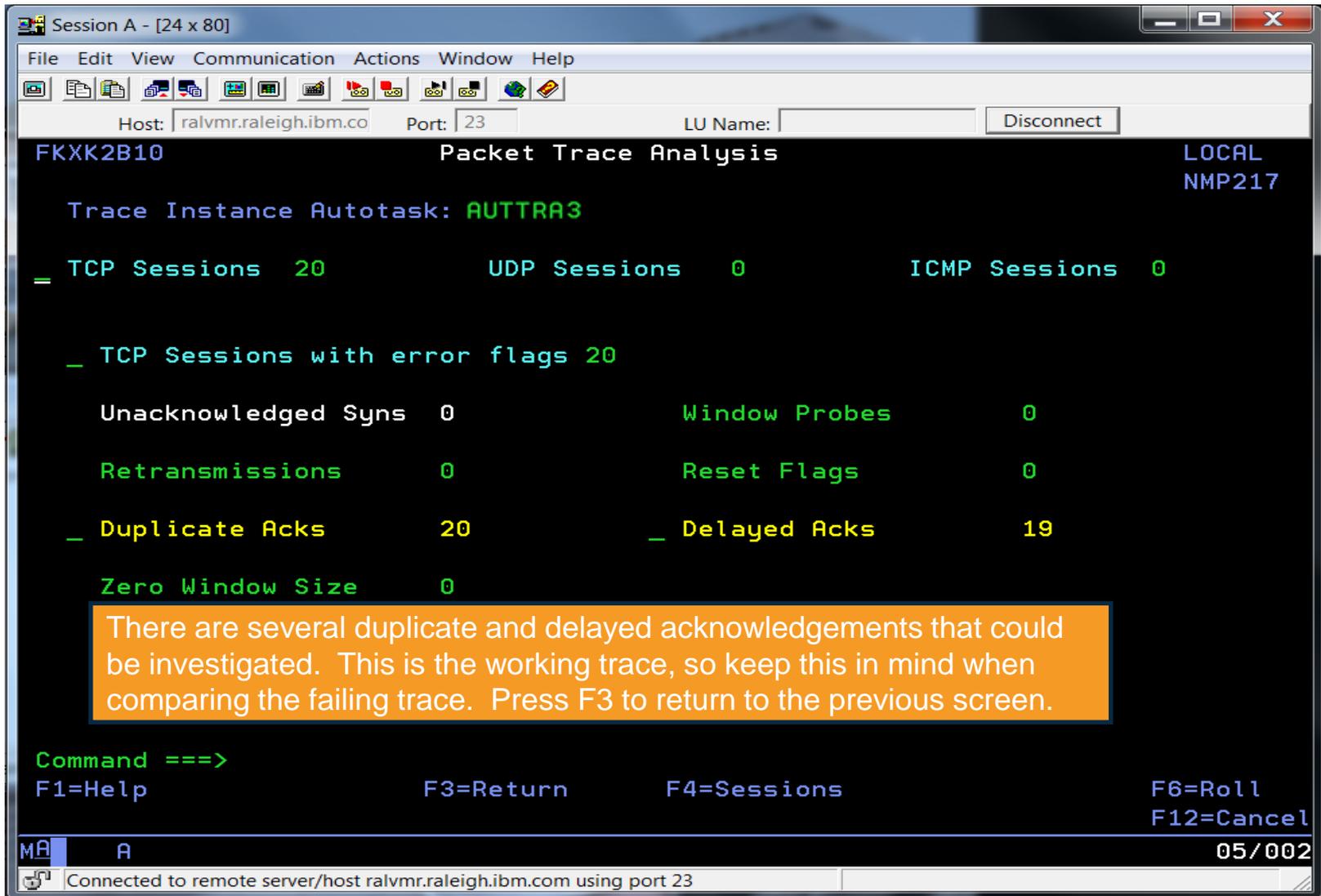
MR A 02/071

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

Two callout boxes are present:

- An orange callout box pointing to the "MaxRecs" field contains the text: "Increase the MaxRecs value to 1000 to ensure seeing all of the records that are needed."
- A larger orange callout box pointing to the "Data Set Name" field contains the text: "Press F10 to analyze the trace and to determine if there are any issues to be concerned about."

# Scenario 1: Packet Trace



The screenshot shows a terminal window titled "Session A - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main content area displays the following text:

```
Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect
FKXX2B10 Packet Trace Analysis LOCAL
NMP217
Trace Instance Autotask: AUTTRA3
TCP Sessions 20 UDP Sessions 0 ICMP Sessions 0
TCP Sessions with error flags 20
Unacknowledged Syms 0 Window Probes 0
Retransmissions 0 Reset Flags 0
Duplicate Acks 20 Delayed Acks 19
Zero Window Size 0
```

An orange callout box contains the text: "There are several duplicate and delayed acknowledgements that could be investigated. This is the working trace, so keep this in mind when comparing the failing trace. Press F3 to return to the previous screen."

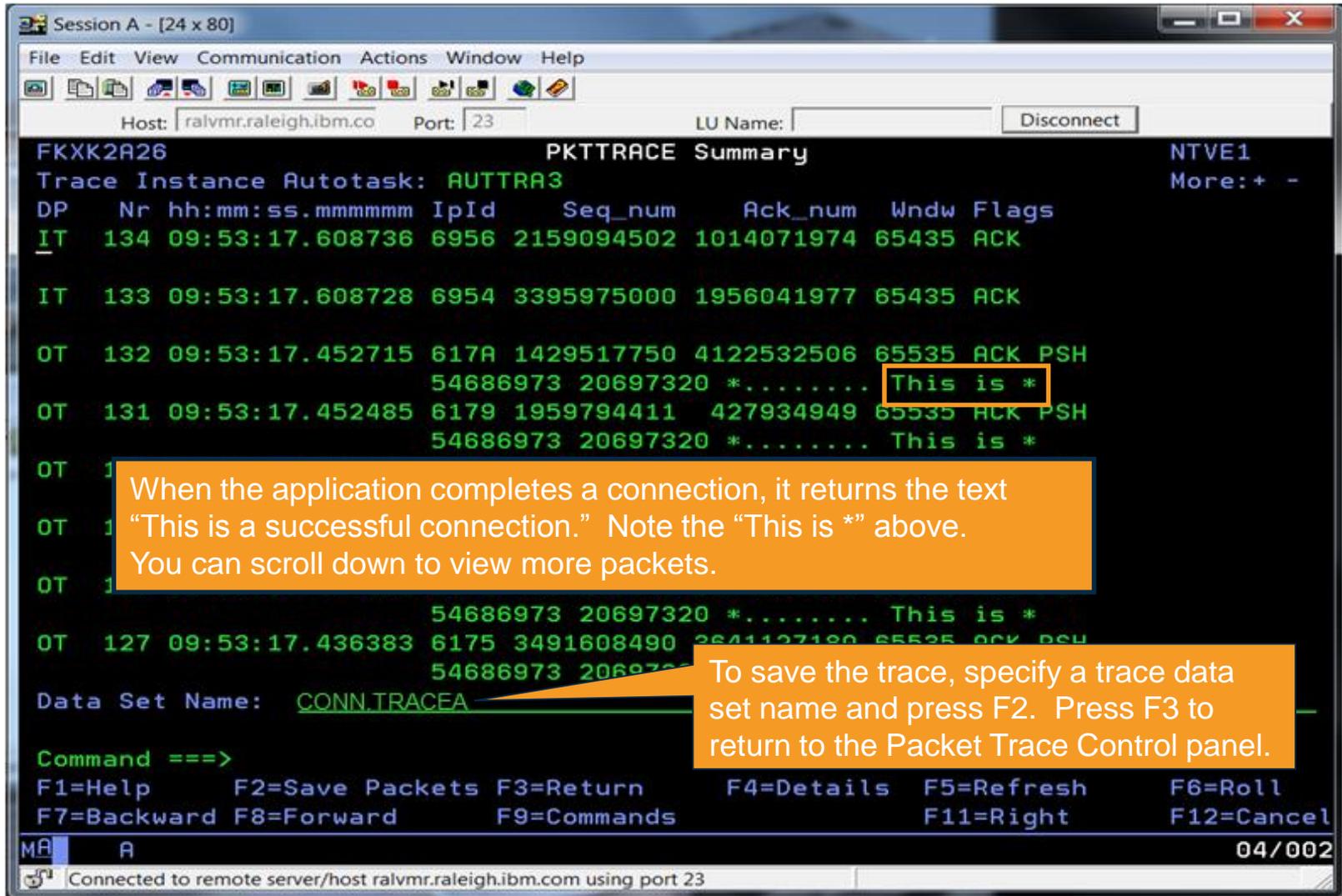
At the bottom, there is a command prompt "Command ==>" and a list of function key shortcuts: F1=Help, F3=Return, F4=Sessions, F6=Roll, F12=Cancel. The status bar at the very bottom shows "MA A" and "05/002".

# Scenario 1: Packet Trace



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

# Scenario 1: Packet Trace



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2A26 PKTTRACE Summary NTVE1

Trace Instance Autotask: AUTTRA3 More: + -

DP	Nr	hh:mm:ss.mmmmm	IpId	Seq_num	Ack_num	Wndw	Flags
IT	134	09:53:17.608736	6956	2159094502	1014071974	65435	ACK
IT	133	09:53:17.608728	6954	3395975000	1956041977	65435	ACK
OT	132	09:53:17.452715	617A	1429517750	4122532506	65535	ACK PSH
				54686973	20697320	*	..... This is *
OT	131	09:53:17.452485	6179	1959794411	427934949	65535	ACK PSH
				54686973	20697320	*	..... This is *
OT	1						
OT	1						
OT	1						
				54686973	20697320	*	..... This is *
OT	127	09:53:17.436383	6175	3491608490	2841127180	65535	ACK PSH
				54686973	20697320	*	..... This is *

Data Set Name: CONN.TRACEA

Command ==>

F1=Help F2=Save Packets F3=Return F4=Details F5=Refresh F6=Roll  
F7=Backward F8=Forward F9=Commands F11=Right F12=Cancel

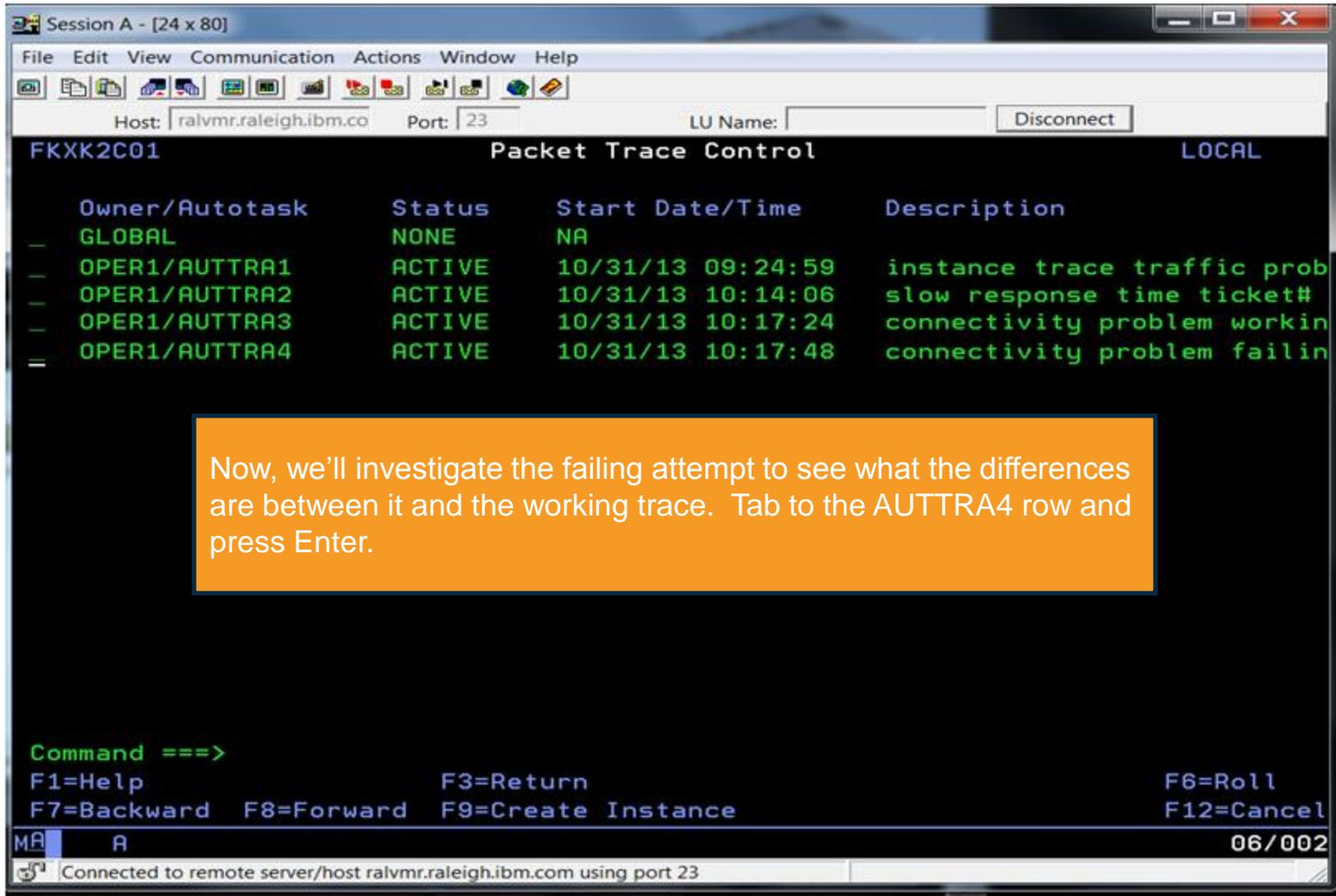
MA A 04/002

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

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



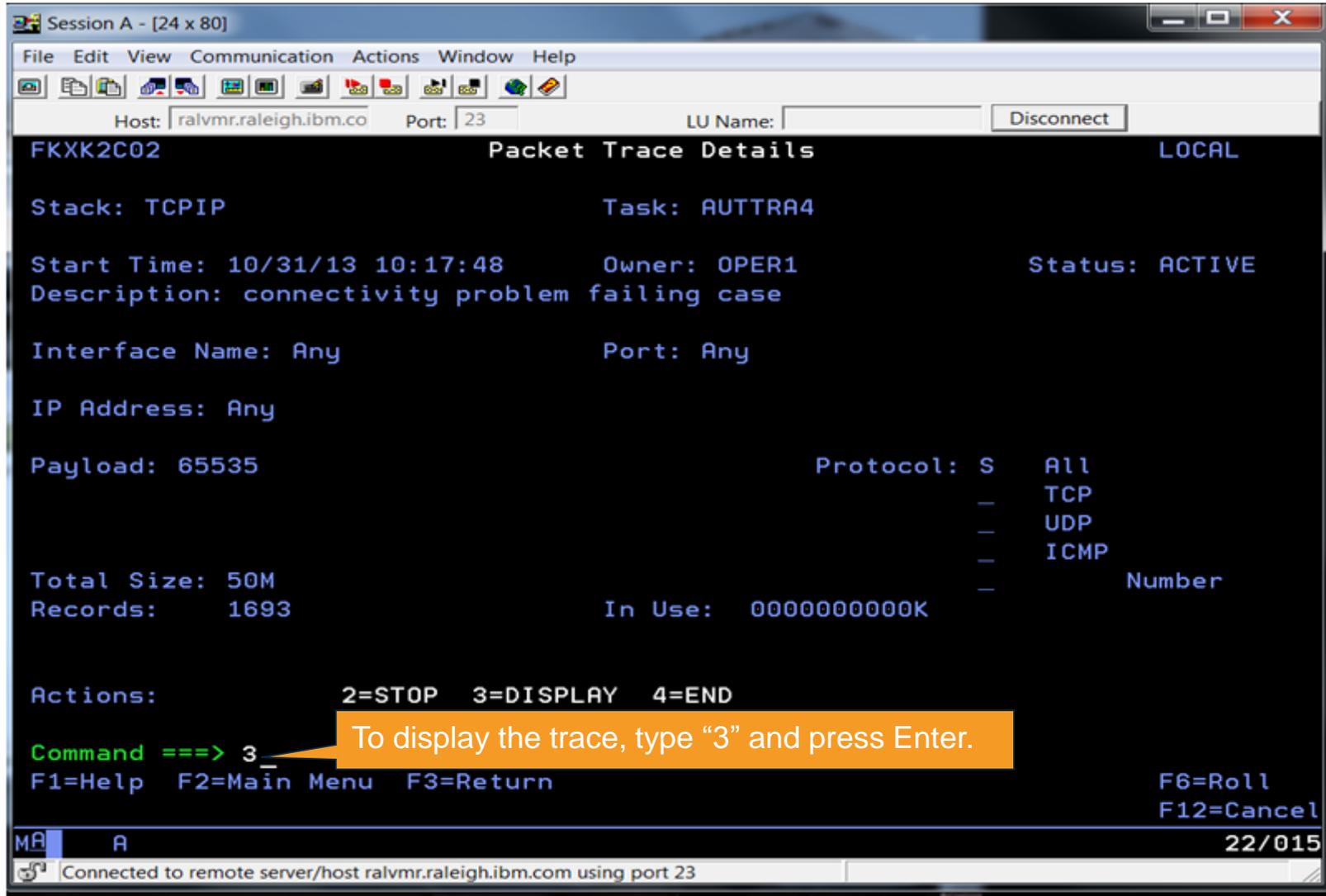
The screenshot shows a terminal window titled "Session A - [24 x 80]". The window has a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. Below the toolbar, there are fields for "Host: ralvmr.raleigh.ibm.co", "Port: 23", and "LU Name: ". A "Disconnect" button is visible. The main content area is titled "Packet Trace Control" and "LOCAL". It displays a table with the following columns: "Owner/Autotask", "Status", "Start Date/Time", and "Description".

Owner/Autotask	Status	Start Date/Time	Description
GLOBAL	NONE	NA	
OPER1/AUTTRA1	ACTIVE	10/31/13 09:24:59	instance trace traffic prob
OPER1/AUTTRA2	ACTIVE	10/31/13 10:14:06	slow response time ticket#
OPER1/AUTTRA3	ACTIVE	10/31/13 10:17:24	connectivity problem workin
OPER1/AUTTRA4	ACTIVE	10/31/13 10:17:48	connectivity problem failin

Below the table, there is a "Command ==>" prompt and a list of function key shortcuts: F1=Help, F3=Return, F6=Roll, F7=Backward, F8=Forward, F9=Create Instance, F12=Cancel. At the bottom, there is a status bar showing "MA A" and "06/002". A footer at the very bottom of the terminal window reads "Connected to remote server/host ralvmr.raleigh.ibm.com using port 23".

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



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2C02 Packet Trace Details LOCAL

Stack: TCPIP Task: AUTTRA4

Start Time: 10/31/13 10:17:48 Owner: OPER1 Status: ACTIVE

Description: connectivity problem failing case

Interface Name: Any Port: Any

IP Address: Any

Payload: 65535 Protocol: S All  
— TCP  
— UDP  
— ICMP

Total Size: 50M  
Records: 1693 In Use: 0000000000K Number

Actions: 2=STOP 3=DISPLAY 4=END

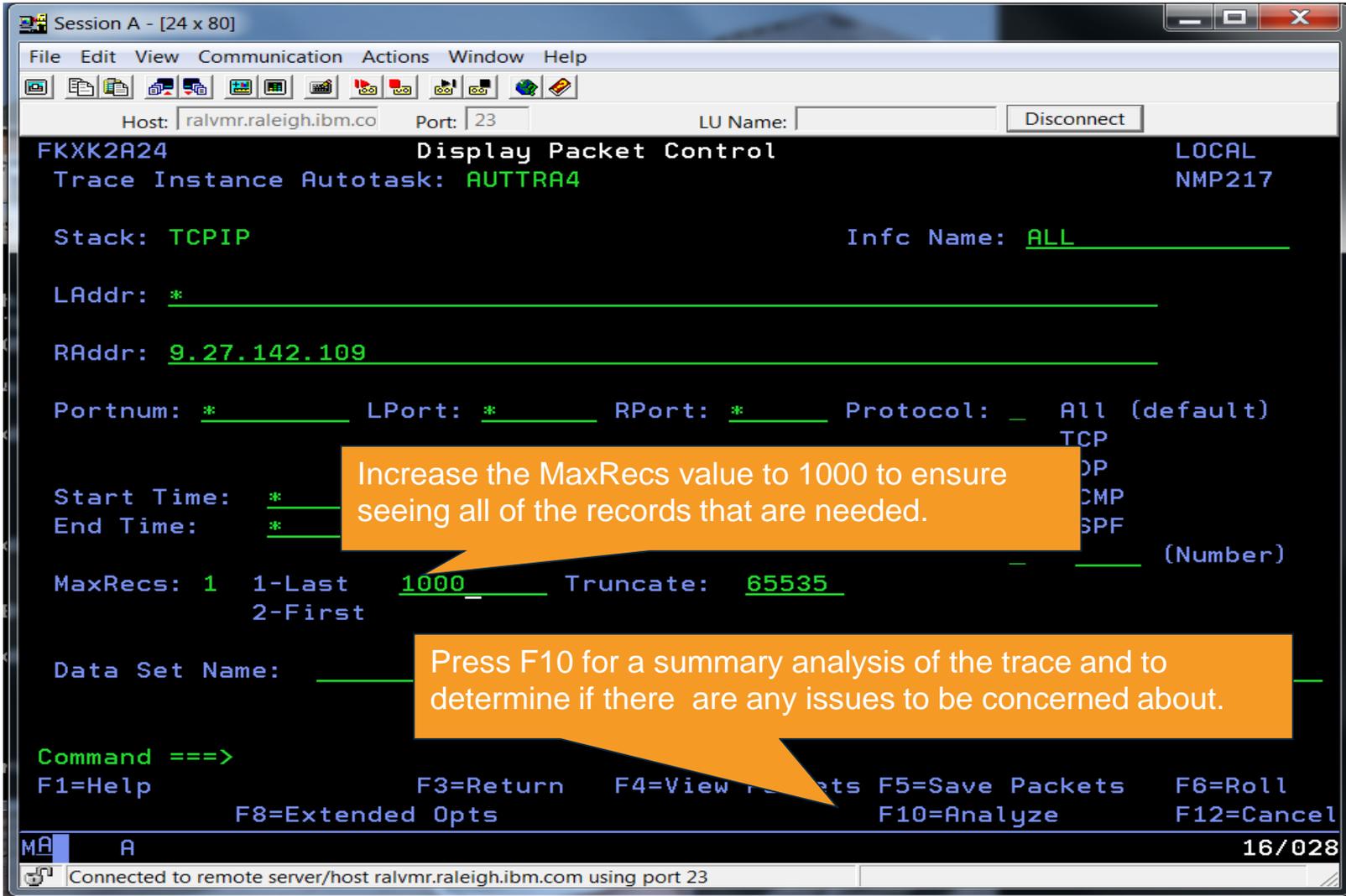
Command ==> 3

F1=Help F2=Main Menu F3=Return F6=Roll F12=Cancel

MR A 22/015

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

# Scenario 1: Packet Trace



Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXK2A24 Display Packet Control LOCAL  
Trace Instance Autotask: AUTTRA4 NMP217

Stack: TCPIP Infc Name: ALL

LAddr: \*

RAddr: 9.27.142.109

Portnum: \* LPort: \* RPort: \* Protocol: All (default)  
TCP  
DP  
CMP  
SPF

Start Time: \*  
End Time: \*

MaxRecs: 1 1-Last 1000 Truncate: 65535  
2-First (Number)

Data Set Name:

Command ==>  
F1=Help F3=Return F4=View Packets F5=Save Packets F6=Roll  
F8=Extended Opts F10=Analyze F12=Cancel

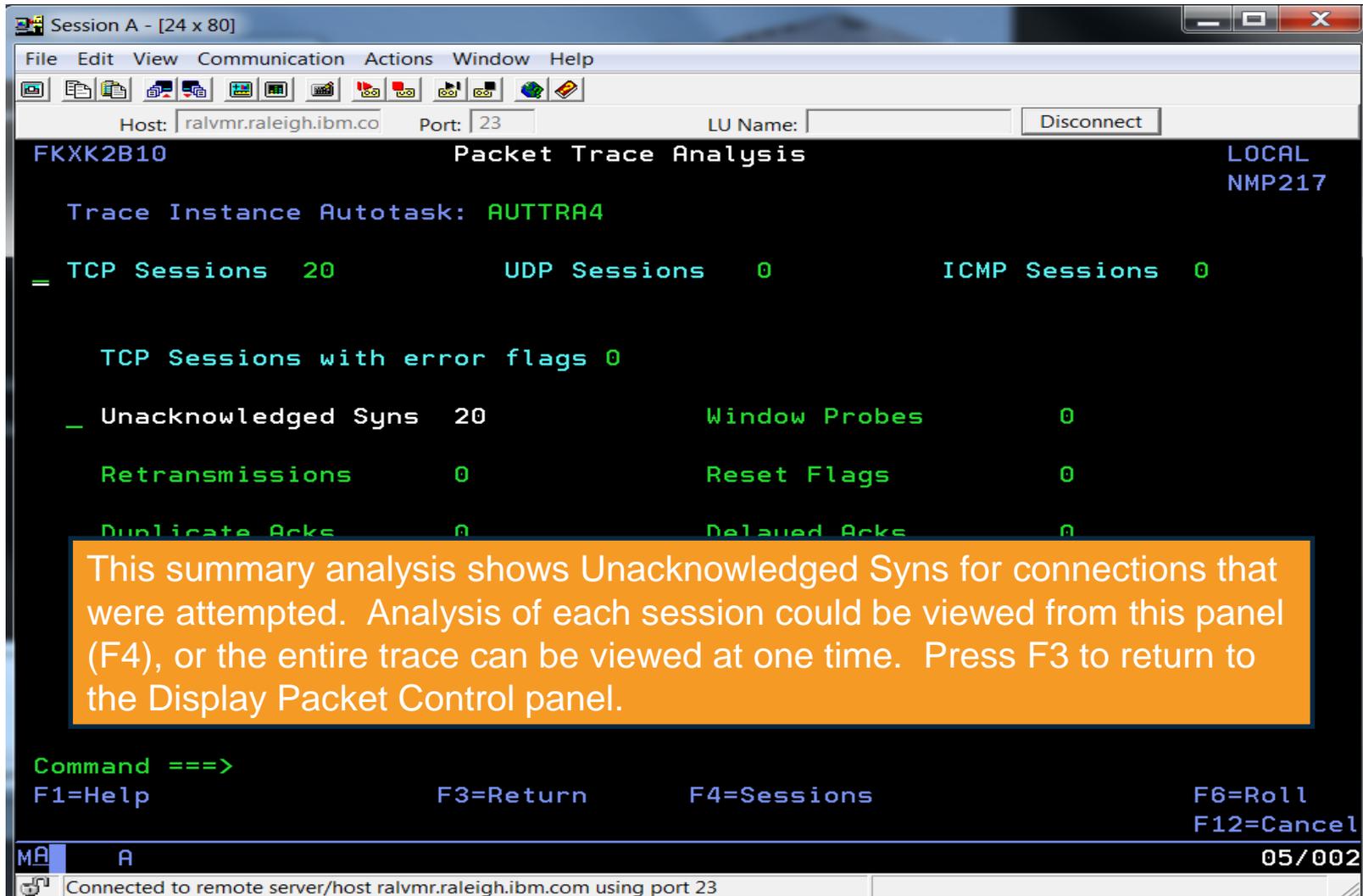
MA A 16/028

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

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

Press F10 for a summary analysis of the trace and to determine if there are any issues to be concerned about.

# Scenario 1: Packet Trace



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect

FKXXK2B10 Packet Trace Analysis LOCAL NMP217

Trace Instance Autotask: AUTTRA4

TCP Sessions 20 UDP Sessions 0 ICMP Sessions 0

TCP Sessions with error flags 0

Unacknowledged Syns 20 Window Probes 0

Retransmissions 0 Reset Flags 0

Duplicate Acks 0 Delayed Acks 0

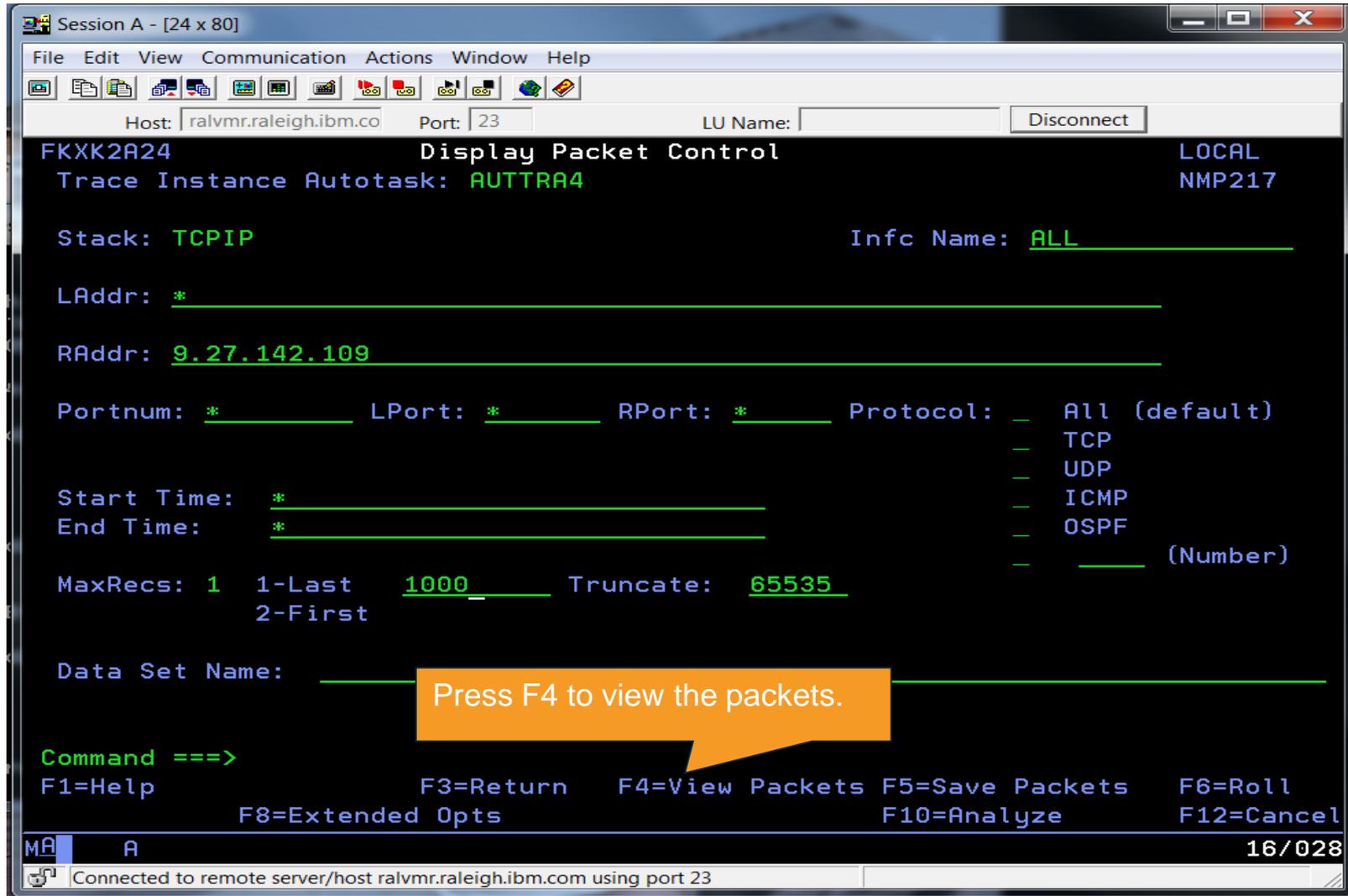
Command ==>  
F1=Help F3=Return F4=Sessions F6=Roll  
F12=Cancel

MA A 05/002

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

This summary analysis shows Unacknowledged Syns for connections that were attempted. Analysis of each session could be viewed from this panel (F4), or the entire trace can be viewed at one time. Press F3 to return to the Display Packet Control panel.

# Scenario 1: Packet Trace

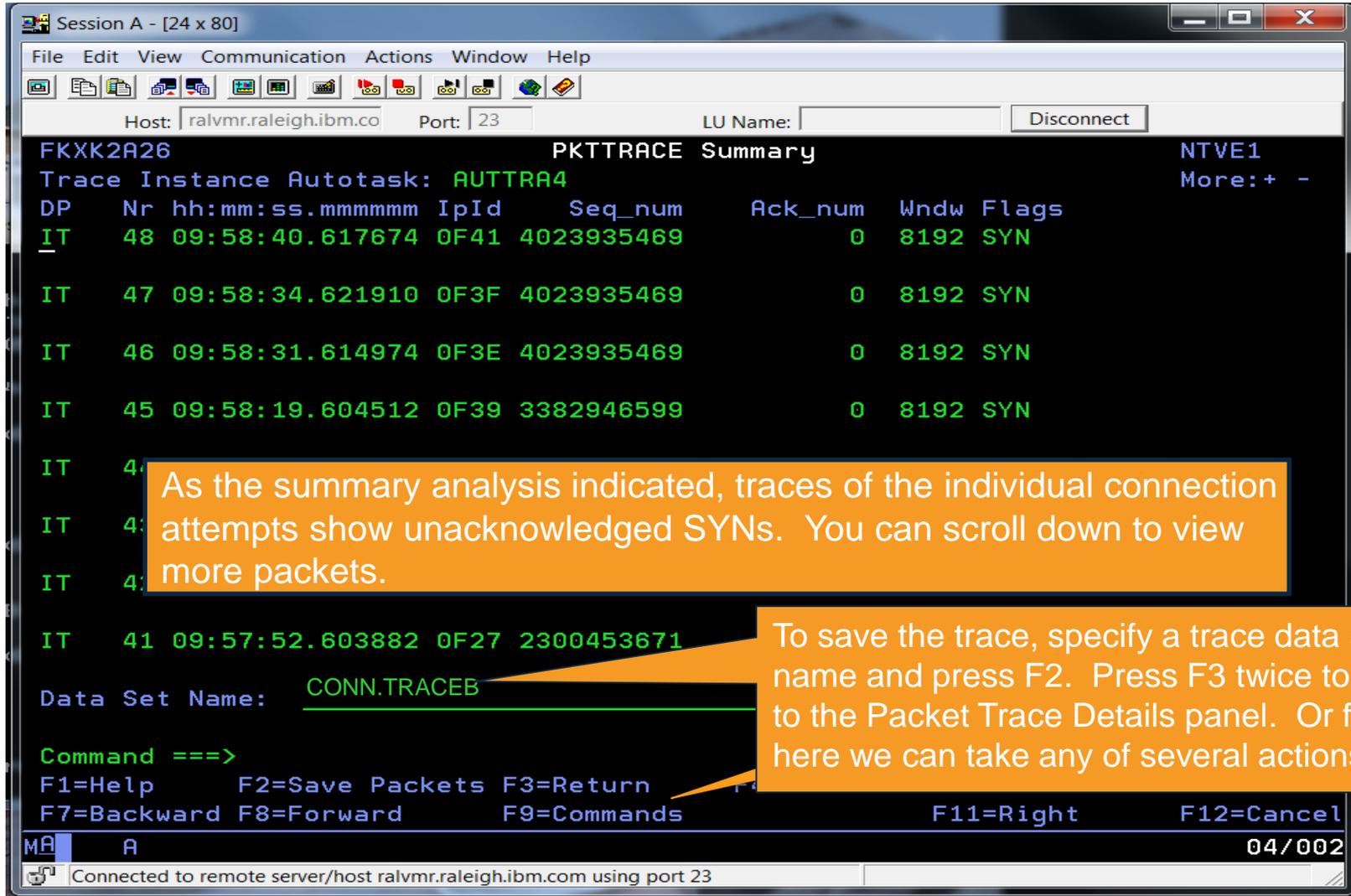


The screenshot shows a terminal window titled "Session A - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main content area is titled "Display Packet Control" and shows the following configuration options:

- Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect
- FKXK2A24 LOCAL
- Trace Instance Autotask: AUTTRA4 NMP217
- Stack: TCPIP Infc Name: ALL
- LAddr: \*
- RAddr: 9.27.142.109
- Portnum: \* LPort: \* RPort: \* Protocol: All (default), TCP, UDP, ICMP, OSPF (Number)
- Start Time: \* End Time: \*
- MaxRecs: 1 1-Last 1000 Truncate: 65535 2-First
- Data Set Name: \*

An orange callout box with the text "Press F4 to view the packets." is overlaid on the terminal. At the bottom, a command prompt shows "Command ==>" and a list of function key shortcuts: F1=Help, F3=Return, F4=View Packets, F5=Save Packets, F6=Roll, F8=Extended Opts, F10=Analyze, F12=Cancel. The status bar at the bottom indicates "Connected to remote server/host ralvmr.raleigh.ibm.com using port 23" and "16/028".

# Scenario 1: Packet Trace



FKXK2A26 PKTTRACE Summary NTVE1  
Trace Instance Autotask: AUTTRA4 More: + -

DP	Nr	hh:mm:ss.mmmmm	IpId	Seq_num	Ack_num	Wndw	Flags
IT	48	09:58:40.617674	0F41	4023935469	0	8192	SYN
IT	47	09:58:34.621910	0F3F	4023935469	0	8192	SYN
IT	46	09:58:31.614974	0F3E	4023935469	0	8192	SYN
IT	45	09:58:19.604512	0F39	3382946599	0	8192	SYN
IT	44	09:58:16.600274	0F38	3382946599	0	8192	SYN
IT	43	09:58:13.596036	0F37	3382946599	0	8192	SYN
IT	42	09:58:10.591798	0F36	3382946599	0	8192	SYN
IT	41	09:57:52.603882	0F27	2300453671	0	8192	SYN

Data Set Name: CONN.TRACEB

Command ==>  
F1=Help F2=Save Packets F3=Return F4=Forward  
F7=Backward F8=Forward F9=Commands F11=Right F12=Cancel

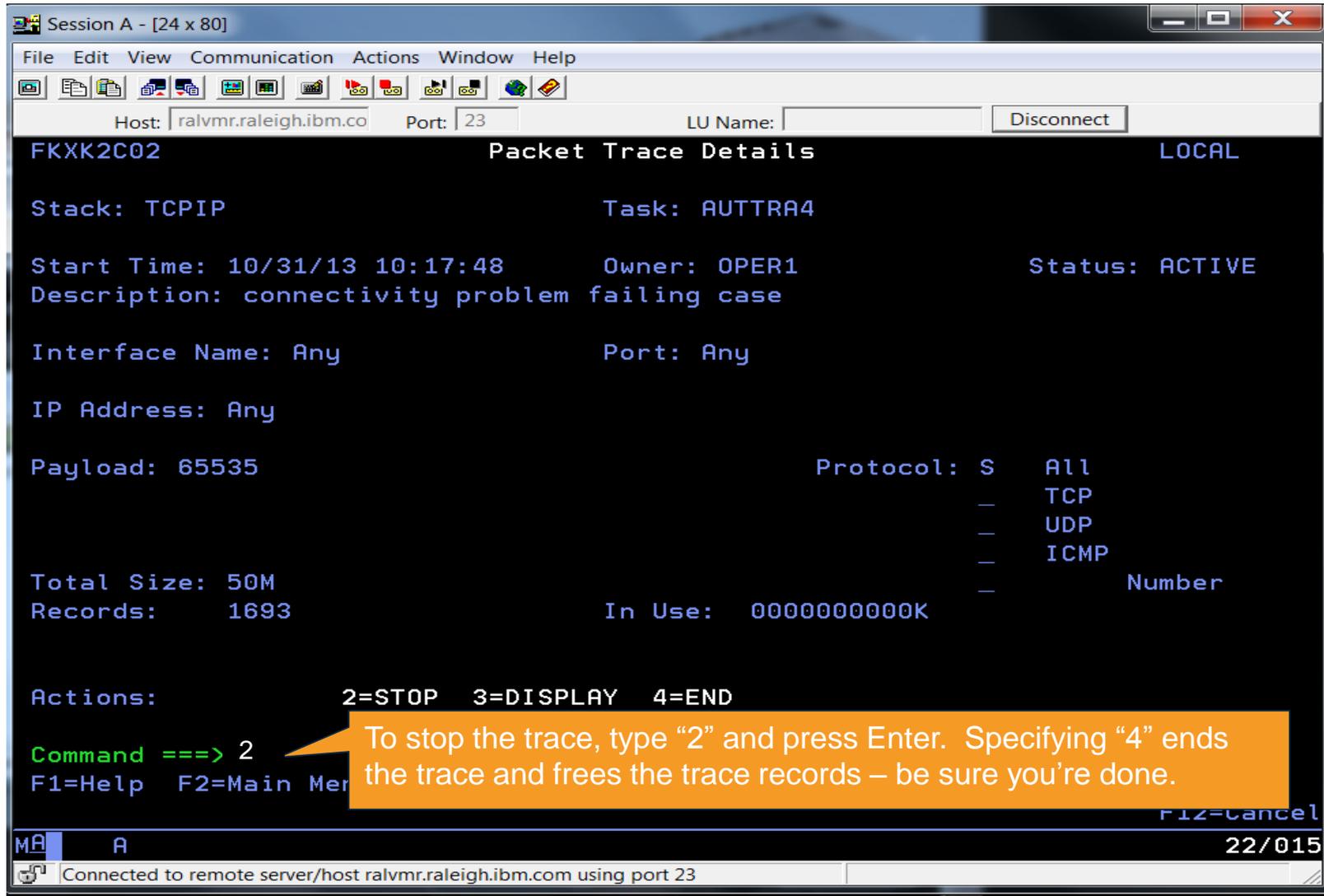
MA A 04/002

Connected to remote server/host ralvmr.raleigh.ibm.com using port 23

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

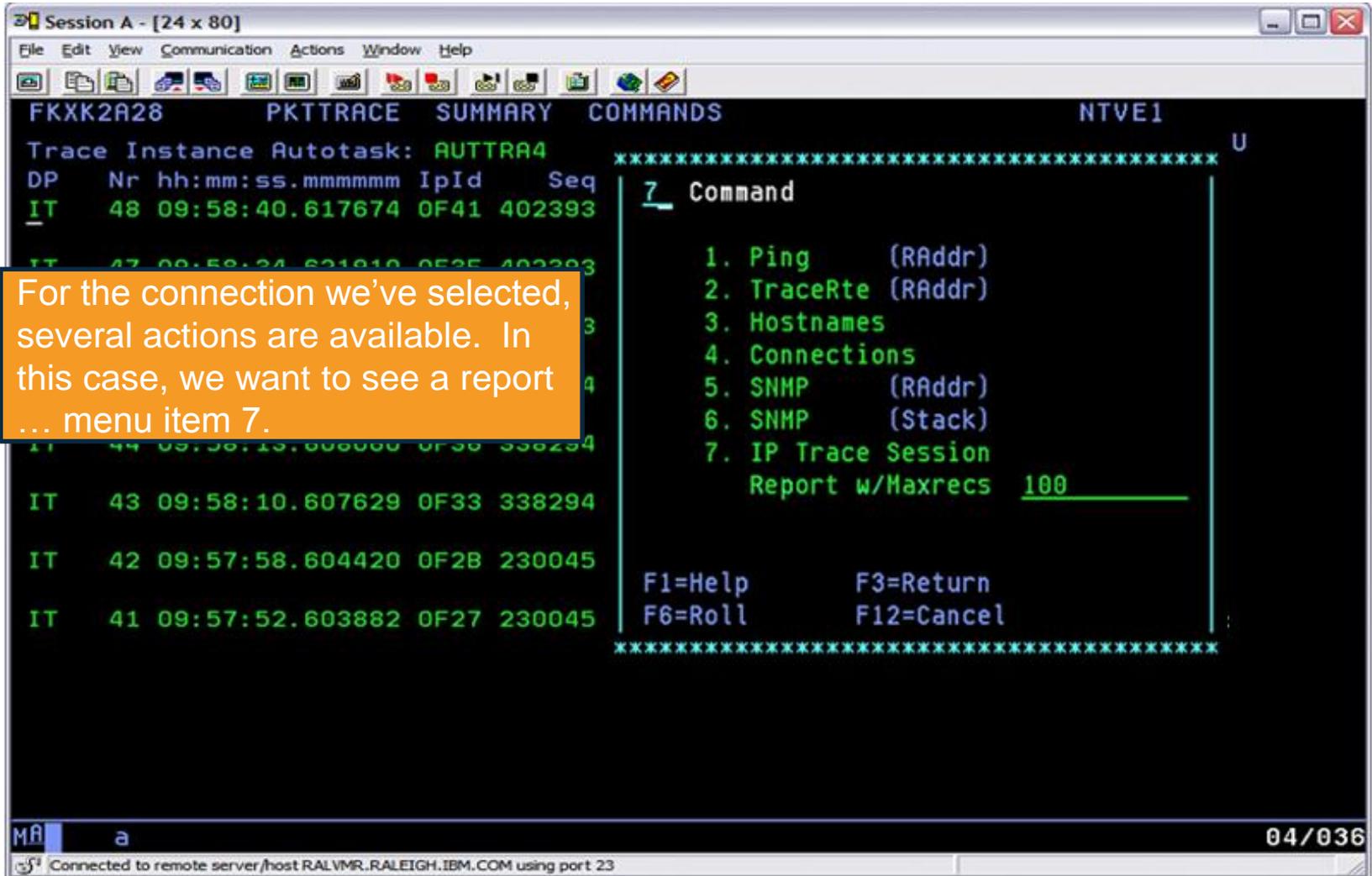


The screenshot shows a terminal window titled "Session A - [24 x 80]". The window contains the following text:

```
File Edit View Communication Actions Window Help
Host: ralvmr.raleigh.ibm.co Port: 23 LU Name: Disconnect
FKXK2C02 Packet Trace Details LOCAL
Stack: TCPIP Task: AUTTRA4
Start Time: 10/31/13 10:17:48 Owner: OPER1 Status: ACTIVE
Description: connectivity problem failing case
Interface Name: Any Port: Any
IP Address: Any
Payload: 65535 Protocol: S All
TCP
UDP
ICMP
Total Size: 50M
Records: 1693 In Use: 0000000000K
Actions: 2=STOP 3=DISPLAY 4=END
Command ==> 2
F1=Help F2=Main Mer F12=Cancel
22/015
Connected to remote server/host ralvmr.raleigh.ibm.com using port 23
```

An orange callout box points to the command prompt with the text: "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



Session A - [24 x 80]

File Edit View Communication Actions Window Help

FKXK2A28 PKTTRACE SUMMARY COMMANDS NTVE1

Trace Instance Autotask: AUTTRA4

DP	Nr	hh:mm:ss.mmmmm	IpId	Seq
IT	48	09:58:40.617674	0F41	402393
IT	47	09:58:34.621910	0E25	402393
IT	46	09:58:28.626146	0D09	402393
IT	45	09:58:22.630382	0B83	402394
IT	44	09:58:16.634618	0A67	338294
IT	43	09:58:10.607629	0F33	338294
IT	42	09:57:58.604420	0F2B	230045
IT	41	09:57:52.603882	0F27	230045

\*\*\*\*\*

7 Command

1. Ping (RAddr)
2. TraceRte (RAddr)
3. Hostnames
4. Connections
5. SNMP (RAddr)
6. SNMP (Stack)
7. IP Trace Session Report w/Maxrecs 100

F1=Help            F3=Return  
F6=Roll            F12=Cancel

\*\*\*\*\*

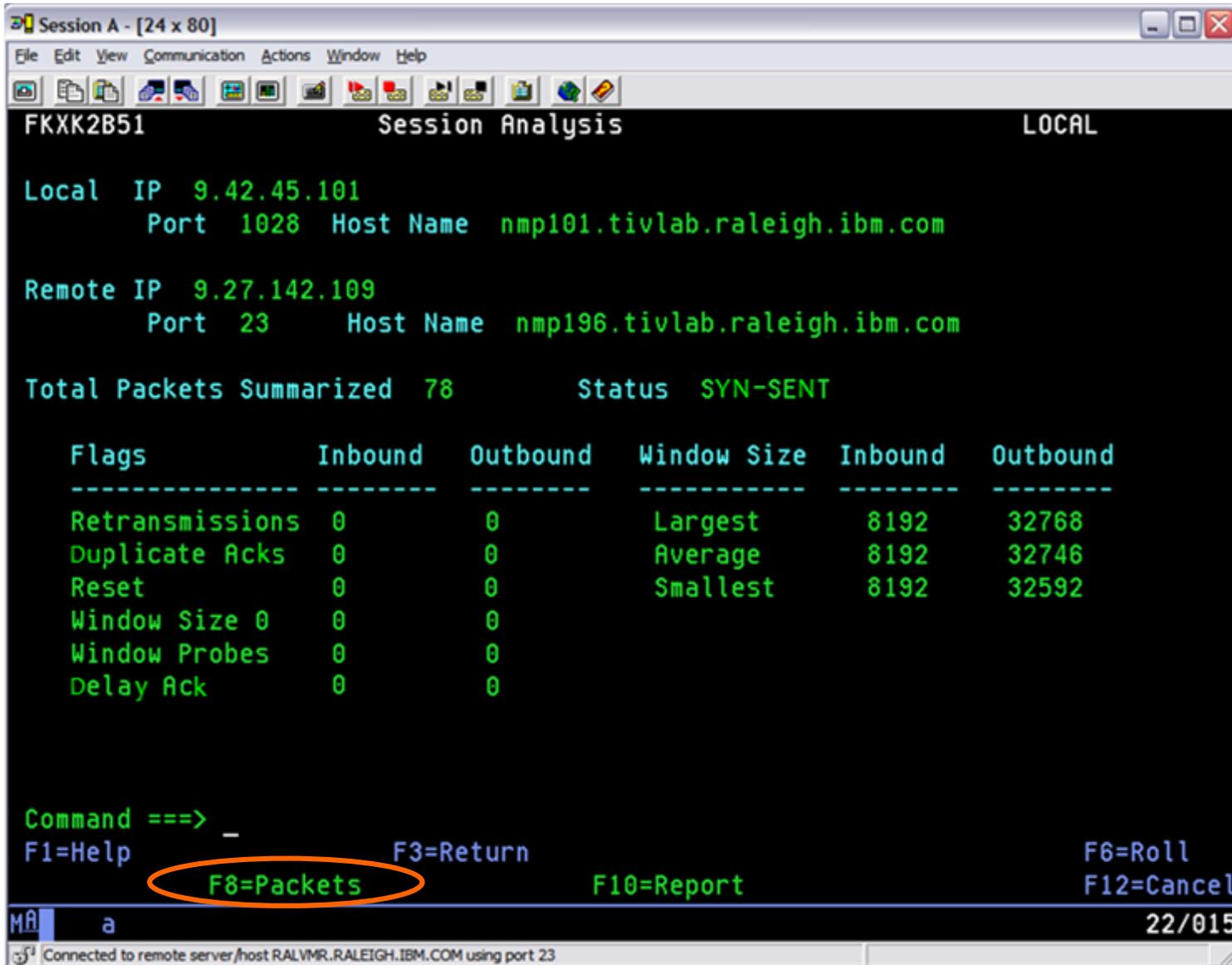
MR a

04/036

Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23

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



FKXK2B51 Session Analysis LOCAL

Local IP 9.42.45.101  
Port 1028 Host Name nmp101.tivlab.raleigh.ibm.com

Remote IP 9.27.142.109  
Port 23 Host Name nmp196.tivlab.raleigh.ibm.com

Total Packets Summarized 78 Status SYN-SENT

Flags	Inbound	Outbound	Window Size	Inbound	Outbound
Retransmissions	0	0	Largest	8192	32768
Duplicate Acks	0	0	Average	8192	32746
Reset	0	0	Smallest	8192	32592
Window Size 0	0	0			
Window Probes	0	0			
Delay Ack	0	0			

Command ==> \_  
F1=Help F3=Return F6=Roll  
F8=Packets F10=Report F12=Cancel

MA a 22/015

Connected to remote server /host RALVMR.RALEIGH.IBM.COM using port 23

# Scenario 1: Individual packets for the session

Session A - [24 x 80]

File Edit View Communication Actions Window Help

FKXK2B53 Session Analysis Packets LOCAL  
More:+

Packet Summary

TcpHdr	IO	F	Seq	Ack	RcvWnd	Data	Delta	Time	TimeStamp
S	0	.	709065838	0	32768	0	0.000000	08:48:32.554268	
S	I	.	1516924025	709065839	32768	0	0.000793	08:48:32.555061	
H	U	.	709065839	1516924026	32768	0	0.000044	08:48:32.555105	
AP	I	.	1516924026	709065839	32768	3	0.001814	08:48:32.556919	
A	0	d	709065839	1516924029	32765	0	0.236337	08:48:32.793256	
AP	0	.	709065839	1516924029	32765	3	0.630173	08:48:33.423429	
AP	0	.	709065842	1516924029	32765	3	0.000363	08:48:33.423792	
AP	I	+	1516924029	709065842	32765	3	0.000590	08:48:33.424382	
A	0	d	709065845	1516924032	32765	0	0.270321	08:48:33.694703	
AP	I	+	1516924032	709065845	32765	6	0.000804	08:48:33.695507	
AP	0	+	709065845	1516924038	32762	18	0.000195	08:48:33.695702	
AP	I	+	1516924038	709065863	32750	3	0.000683	08:48:33.696385	
AP	0	+	709065863	1516924041	32765	3	0.000065	08:48:33.696450	
AP	0	.	709065866	1516924041	32765	3	0.000073	08:48:33.696523	
AP	I	+	1516924041	709065869	32762	9	0.000502	08:48:33.697025	
AP	0	+	709065869	1516924050	32759	3	0.000093	08:48:33.697118	

Command ==>

F1=Help F3=Return F4=Packet Detail F6=Roll  
F7=Backward F8=Forward F11=Right F12=Cancel

Complete y MA a 05/002

Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23

duplicate  
ack

delayed  
ack

F4=Packet Detail

# Scenario 1: Packet Details

```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
CNMKWIND OUTPUT FROM Packet Detail LINE 0 OF 48
*----- Top of Data -----*
z/OS TCP/IP Packet Trace Formatter, Copyright IBM Corp. 2000, 2009; 2009.028

**** 2013/10/31
RcdNr Sysname Mnemonic Entry Id Time Stamp Description
-----
48 NMP101 PACKET 00000004 09:58:40.617674 Packet Trace
To Interface : TCPIPLINK Device: QDIO Ethernet Full=52
Tod Clock : 2013/10/31 09:58:40.617674 Intfx: 5
Segment # : 0 Flags: Out
Source : 9.27.142.109
Destination : 9.42.45.101
Source Port : 23 Dest Port: 1028 Asid: 002F TCB: 006B59D0
IpHeader: Version : 4 Header Length: 20
Tos : 00 QOS: Routine Normal Service
Packet Length : 52 ID Number: 0F41
Fragment : Offset: 0
TTL : 64 Protocol: TCP CheckSum: 097F F
Source : 9.27.142.109
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==> _
MA a 24/009
```

# Scenario 1: Analysis for selected session

Session A - [24 x 80]

File Edit View Communication Actions Window Help

FKXX2B51 Session Analysis LOCAL

Local IP 9.42.45.101  
Port 1028 Host Name nmp101.tivlab.raleigh.ibm.com

Remote IP 9.27.142.109  
Port 23 Host Name nmp196.tivlab.raleigh.ibm.com

Total Packets Summarized 78 Status SYN-SENT

Flags	Inbound	Outbound	Window Size	Inbound	Outbound
Retransmissions	0	0	Largest	8192	32768
Duplicate Acks	0	2	Average	8192	32746
Reset	0	1	Smallest	8192	32592
Window Size 0	0	0			
Window Probes	0	0			
Delay Ack	1	14			

Command ==> \_

F1=Help F3=Return F6=Roll  
F8=Packets F9=Actions F10=Report F12=Cancel

MA a 22/015

Connected to remote server /host RALVMR.RALEIGH.IBM.COM using port 23

Complete

# Scenario 1: Session Report

```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
CNMKWIND OUTPUT FROM Session Report LINE 0 OF 213
*----- Top of Data -----*
BNH773I NUMBER OF PACKETS: 78 , MISSED BUFFERS: 0 , TCPNAME: TCPIP
z/OS TCP/IP Packet Trace Formatter, Copyright IBM Corp. 2000, 2009; 2009.028

**** 2013/10/31
      No packets required reassembly

=====
Interface Table Report
Index Count Link          Address
   5     78 TCPIPLINK      9.42.45.101
=====

Tcp Sessions Report
   1 sessions found

-----
78 packets summarized

Local Ip Address:          9.42.45.101
Remote Ip Address:        9.27.142.109

TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==> _

MA a 24/009
Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23
```

Complete

# Scenario 1: Session Report (cont.)

```

Session A - [24 x 80]
File Edit View Communication Actions Window Help
CNMKWIND OUTPUT FROM Session Report LINE 20 OF 213

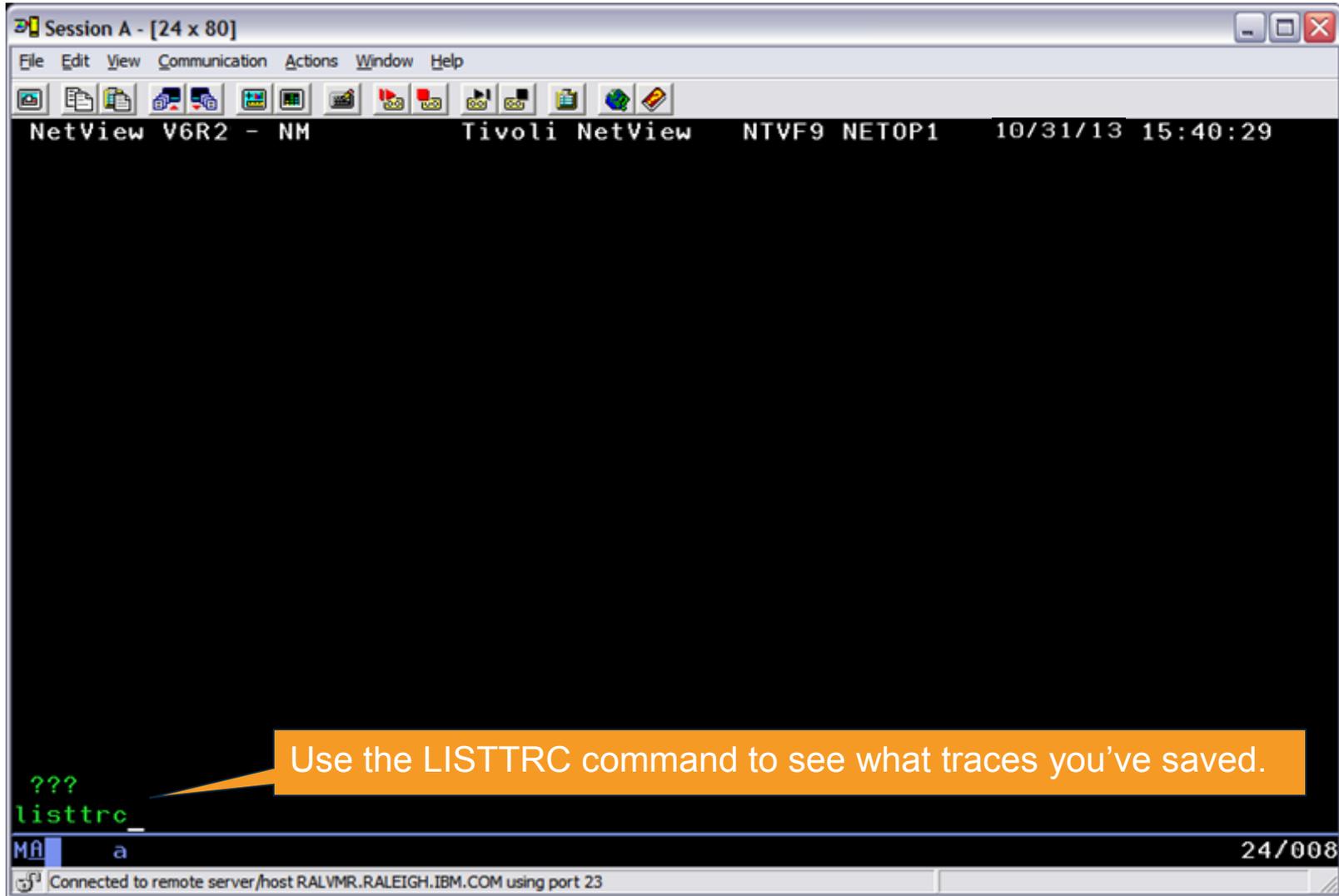
Host:                Local,          Remote
Client or Server:    SERVER,         CLIENT
Port:                1028,          23
Application:         ,             telnet
Link speed (parm):   10,             10 Megabits/s

Connection:
First timestamp:     2013/10/31 08:48:32.554268
Last timestamp:      2013/10/31 08:49:16.053717
Duration:            00:00:43.499449
Average Round-Trip-Time: 0.042 sec
Final Round-Trip-Time: 0.627 sec
Final state:         CLOSED (ACTIVE RESET)
Out-of-order timestamps: 0

Data Quantity & Throughput:    Inbound,          Outbound
Application data bytes:        8293,             245
Sequence number delta:         8294,             247
Total bytes Sent:              8293,             246
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==>
M[A] a 24/009
Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23
  
```

Complete

# Scenario 1: Packet Trace



Session A - [24 x 80]

File Edit View Communication Actions Window Help

NetView V6R2 - NM Tivoli NetView NTVF9 NETOP1 10/31/13 15:40:29

listtrc

MA a

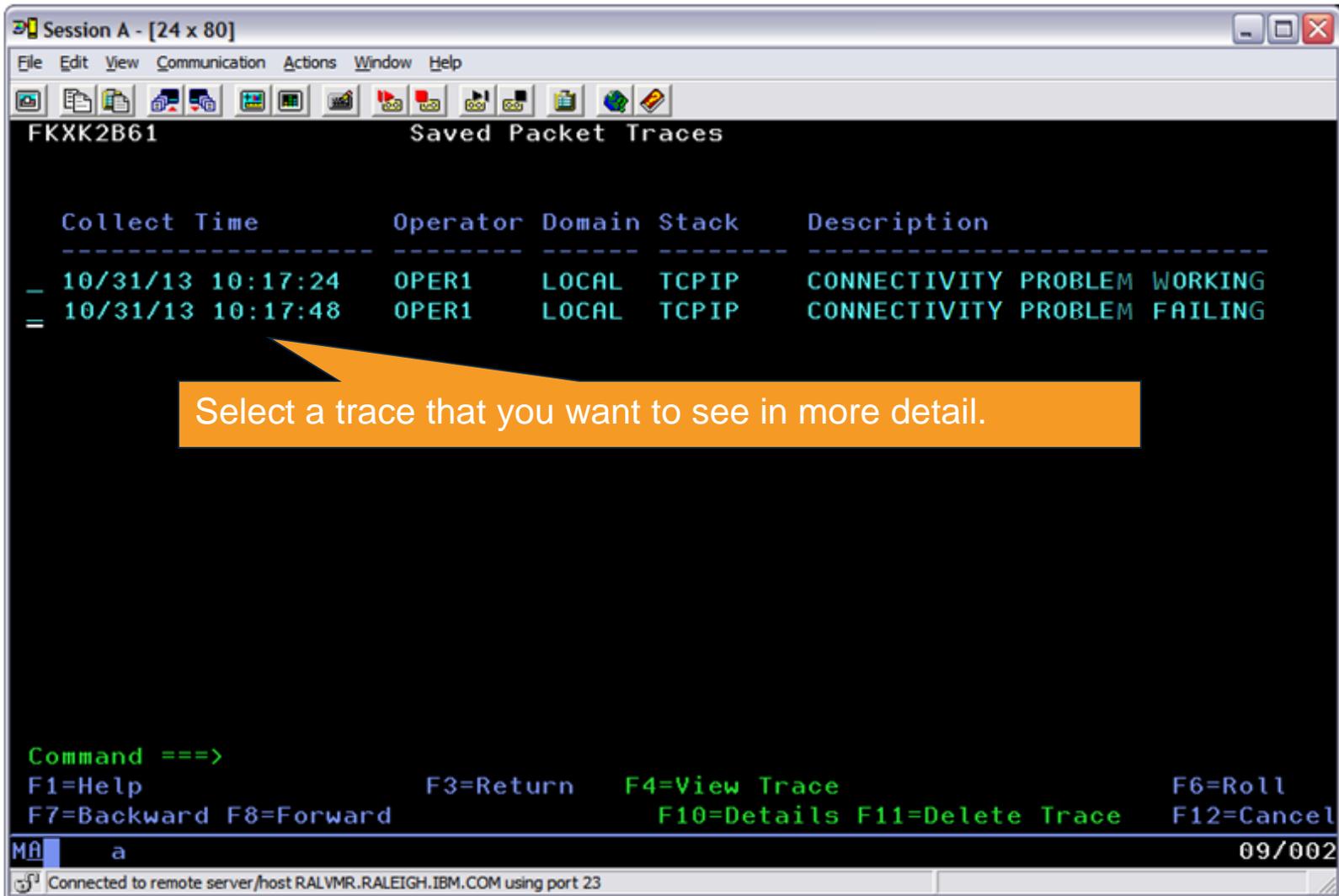
24/008

Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23

Use the LISTTRC command to see what traces you've saved.

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# Scenario 1: Packet Trace



Collect	Time	Operator	Domain	Stack	Description
_	10/31/13 10:17:24	OPER1	LOCAL	TCPIP	CONNECTIVITY PROBLEM WORKING
=	10/31/13 10:17:48	OPER1	LOCAL	TCPIP	CONNECTIVITY PROBLEM FAILING

Command ==>  
F1=Help                      F3=Return      F4=View Trace                      F6=Roll  
F7=Backward F8=Forward                      F10=Details F11=Delete Trace                      F12=Cancel

MA a 09/002

Connected to remote server/host RALVMR.RALEIGH.IBM.COM using port 23

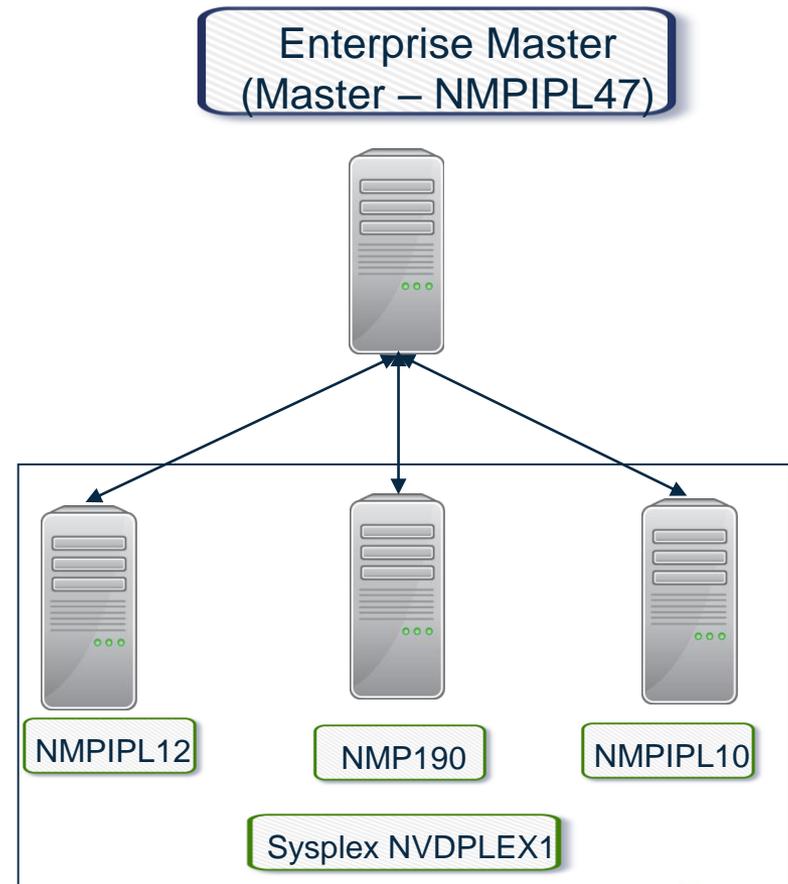
Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# Packet Trace Summary

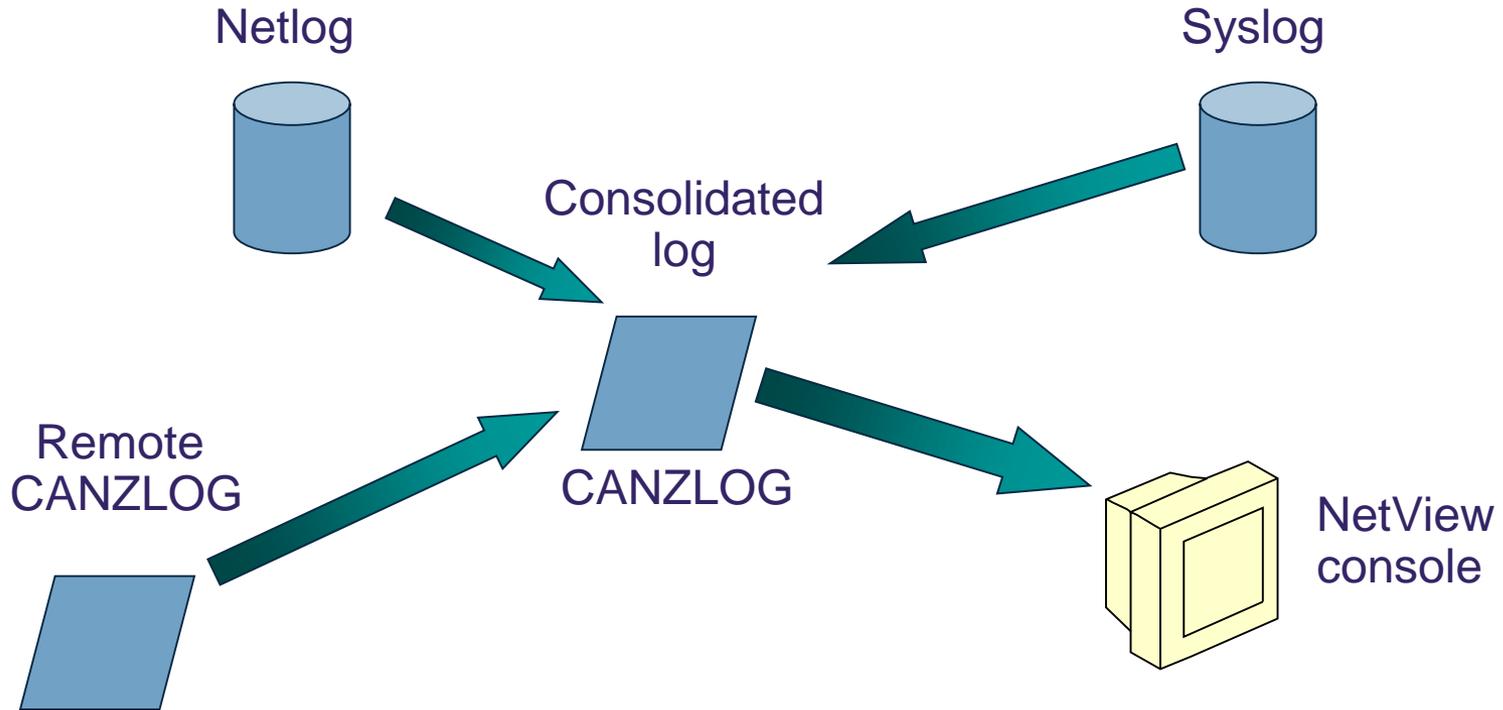
- Packet trace can be controlled through the global trace or multiple instance traces
  - “Global” trace: only 1 per stack
  - “Instance” traces: up to 32 per stack
- Multi-trace function requires z/OS Communications Server V2.1 and NetView for z/OS V6.2 or later.
- Multiple traces can be useful for 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 **L**OG

# 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.NTV66 = NMPIPL30.TIVLAB.RALEIGH.IBM.COM/4022 ON USIBMNT
RMTALIAS.NTV66TST = IP.NTV66
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

```

CNMKCZLG          Specify Canzlog Filters

From: _____ To: '03/11/14 23:16:00'
For: 0D 0H 1M
Tag: _____
Jobname: _____
ASID: _____
Console: _____
Domain: _____
AutoTok: _____
AuthUser: _____
Opid: _____
CHKey: _____
Text - case sensitive; faster search: _____
Text - case insensitive; slower search: _____
Target: plex1
Name: _____ Remark: _____

TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD-->
  
```

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

```

Canzlog Target=PLEX1 T0='03/11/14 23:16:00' 03/11/14 23:15:00 -- 23:15:09
NMPIPL10 TCPIP 23:15:00 EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,OBEYFILE,USER.PARMLIB(DDVIPADD)
NMPIPL10 TCPIP 23:15:00 EZZ0300I OPENED OBEYFILE FILE 'USER.PARMLIB(DDVIPADD)'
NMP190 T620EENV 23:15:00 IEA630I OPERATOR NETO2NM NOW ACTIVE, SYSTEM=NMP190 , LU=NT74L701
NMPIPL10 TCPIP 23:15:00 EZZ0309I PROFILE PROCESSING BEGINNING FOR 'USER.PARMLIB(DDVIPADD)'
NMP190 T620EENV 23:15:00 V TCPIP,TCPIP,OBEYFILE,USER.PARMLIB(DDVIPADD)
NMPIPL10 TCPIP 23:15:00 EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'USER.PARMLIB(DDVIPADD)'
NMPIPL10 TCPIP 23:15:00 EZZ0053I COMMAND VARY OBEY COMPLETED SUCCESSFULLY
NMPIPL10 TCPIP 23:15:00 EZZ0312I VIPA 201.2.10.10 MAY NOT BE CHANGED WITH VIPADEFINE
NMP190 TCPIP 23:15:00 EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,OBEYFILE,USER.PARMLIB(DDVIPADD)
NMP190 TCPIP 23:15:00 EZZ0300I OPENED OBEYFILE FILE 'USER.PARMLIB(DDVIPADD)'
NMP190 TCPIP 23:15:00 EZZ0309I PROFILE PROCESSING BEGINNING FOR 'USER.PARMLIB(DDVIPADD)'
NMP190 TCPIP 23:15:00 EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'USER.PARMLIB(DDVIPADD)'
NMP190 TCPIP 23:15:00 EZZ0331I NO HOME ADDRESS ASSIGNED TO
NMP190 TCPIP 23:15:00 EZZ0331I NO HOME ADDRESS ASSIGNED TO
NMP190 TCPIP 23:15:00 EZZ0053I COMMAND VARY OBEY COMPLETED SUCCESSFULLY
NMPIPL12 T620EENV 23:15:00 IEA630I OPERATOR NETO1NM1 NOW ACTIVE, SYSTEM=NMP190 , LU=NT74L701
NMPIPL12 T620EENV 23:15:00 V TCPIP,TCPIP,OBEYFILE,USER.PARMLIB(DDVIPADD)
NMPIPL12 TCPIP 23:15:00 EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,OBEYFILE,USER.PARMLIB(DDVIPADD)
NMPIPL12 TCPIP 23:15:00 EZZ0300I OPENED OBEYFILE FILE 'USER.PARMLIB(DDVIPADD)'
NMPIPL12 TCPIP 23:15:00 EZZ0309I PROFILE PROCESSING BEGINNING FOR 'USER.PARMLIB(DDVIPADD)'
NMPIPL12 TCPIP 23:15:00 EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'USER.PARMLIB(DDVIPADD)'
NMPIPL12 TCPIP 23:15:00 EZZ0053I COMMAND VARY OBEY COMPLETED SUCCESSFULLY
NMPIPL12 TCPIP 23:15:00 EZZ0312I VIPA 201.2.10.203 MAY NOT BE CHANGED WITH VIPADEFINE
NTV74 AUTOTCPS 23:15:09 CNM493I CNMSDVCG : #0000030 : CNM8265 AUTO
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==> _
  
```

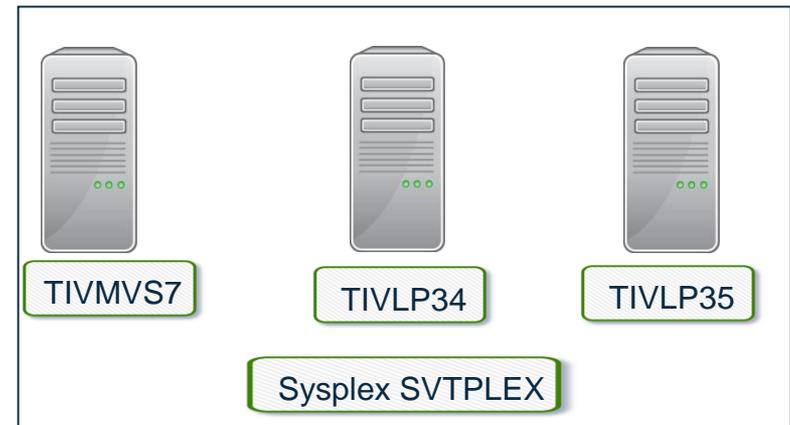
Indicates the DVIPA address is already defined on the current stacks.

# 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



Distributed DVIPA Server Health

Tivoli Enterprise Portal Welcome SYSADMIN Log out IBM

File Edit View Help

Navigator View: Physical

- CNM01
  - DDVIPA Server Health
  - DVIPA Application-Instance
  - DVIPA Connections
  - DVIPA Definition and Status
  - DVIPA Distributor Targets
  - DVIPA Stack-Defined
  - DVIPA Sysplex Distributors
  - HiperSockets
  - NetView Audit Log
  - NetView Command Response
  - NetView Health
  - NetView Log
  - OSA
  - Session Data
  - Stack Configuration and Status
  - TCPIP Connection Data
  - Telnet Server Configuration and Status

LP34

Physical

### WLM Weight

DVIPA and DVIPA Port

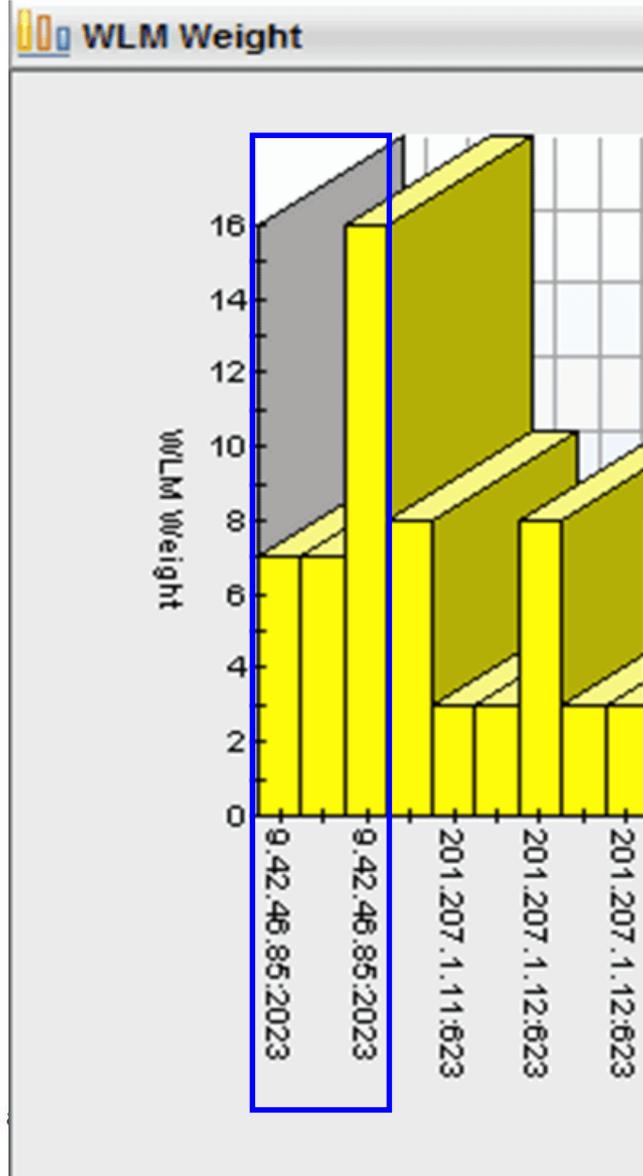
### Distributed DVIPA Server Health Summary

Update Time	Application Server Name	DVIPA	DVIPA Port	Dynamic XCF IP Address	ZOS Image Name	Port Health Percent	WLM Weight	Abnormal Transaction Percent	Target Server Responsiveness Rate	Target Connectivity Success Rate	Server Accept Efficiency Fraction	Connection Establishment Rate	Raw Composite Weight	Raw CP Weight	Raw zAAP Weight	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

Hub Time: Thu, 08/08/2013 01:46 PM Server Available Distributed DVIPA Server Health - nc058026.tivlab.raleigh.ibm.com - SYSADMIN

# Scenario 3: WLM Weight Bar Chart

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



Complete your session evaluations online

# 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](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](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](http://www.SHARE.org/Seattle-Eval)

© Copyright IBM Corporation 2014