# CA NetMaster® Network Management for TCP/IP

## Overview Guide

### Release 12.1

# CA Technologies Product References

This document references the following CA Technologies products:

- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA Network and Systems Management (CA NSM)
- CA Network and Systems Management NetMaster® Option (CA NSM NetMaster Option)
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS)

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Contents

# Chapter 1: Introduction

This section contains the following topics:



## Product Overview

CA NetMaster NM for TCP/IP addresses day-to-day network operations, availability, and performance management challenges, letting you unify and simplify the management of your IT environment for greater business results. The product empowers your organization to resolve problems proactively with IP network access to mainframe-hosted applications, helping to ensure that service-level goals are met.

CA NetMaster NM for TCP/IP lets you display information about z/OS mainframe IP network activity and provides a diagnostic interface to mainframe IP network resources. The product pinpoints network slow-downs or failures and monitors the availability and use of TCP/IP connections to mainframe applications such as CICS, DB2, or WebSphere. You can watch and look after the IP networks of multiple MVS systems (LPARs) from its consolidated, enterprise-wide 3270 and web browser displays.

Using CA NetMaster NM for TCP/IP, you can find out the following information about your networks:

- Status of network resources and alerts on network problems through various monitor displays
- List of connections that satisfy criteria (such as round-trip time (RTT) and user IDs) specified by you
- Events (such as connections and FTP failures) that can help you manage your networks
- Real-time and long-term performance data about your mainframe-connected networks
- Packet traces, which can help you diagnose network problems

# Fast and Efficient Problem Diagnosis

This product supports highly efficient problem resolution functionality that enables the early detection and resolution of connection problems. Network availability is improved by swift automated responses to IP network events such as stack errors, and logging of IP-related events for faster problem diagnosis and accountability.

By using these tools, you can reduce the time to recover from a network problem, thus increasing network availability. The ability to highlight a problem, diagnose it, and monitor it from the same application can help you identify the cause of the problem quicker, implement the resolution faster, and reduce the impact on the network and the business.

## Dynamic Packet Tracing

This product supports the timely tracing of network connections using a real-time tracing function named SmartTrace (see page 39). You can perform the following tasks with SmartTrace:

- Run multiple traces simultaneously with varying criteria.
- Create and save trace definitions.
- Initiate traces from the various monitors, or automatically trigger them.
- View trace results immediately, or save them for later viewing.
- Secure the packet data to specific users.

## Network Baselines

CA NetMaster NM for TCP/IP uses automated network learning techniques to establish your network's baseline or normal operating characteristics and usage patterns. You can set thresholds to allow CA NetMaster NM for TCP/IP to report and alert on deviations or deltas from the baseline associated with normal operation.

# Network Resources Discovery

Network discovery makes the process of identifying and setting up your TCP/IP resources for monitoring easy and quick. CA NetMaster NM for TCP/IP provides a code-free, menu-driven method of defining the resources on your network—you do not have to build or write procedures to learn and discover your network.

Network discovery happens when you start a region for the first time and invokes Express Setup. The process discovers resources based on criteria such as number of hops and the IP starting address. These resources are added to the database, with details about how to manage and monitor them.

## Network Performance Monitoring

Intelligent performance management helps you make informed decisions about the use and growth of your network infrastructure. CA NetMaster NM for TCP/IP collects network traffic and usage information in real time, establishes network baselines, and monitors the network for degradation.

Performance information is also saved to provide historical performance reporting so that you can evaluate long-term patterns in response time, data rates, and resource availability. You can also identify potential device path or session response problems that affect connectivity and the availability of z/OS-based applications. This information enables you to take immediate action to address current problems.

Early detection of potential resource problems that affect users and applications increases network reliability and application availability. Problem resolution time is decreased because technical staff have visibility of mission-critical resources and detailed information about the availability and performance of the network.

## Network Usage and Trends Reporting

ReportCenter (see page 61) provides web-based historical and trend reporting of collected data. This component combines the familiarity and stability of the enterprise environment with the usability of the web, providing integrated mainframe-to-browser presentation of your TCP/IP network performance data from multiple regions.

## WebCenter

WebCenter is a browser-based user interface that you can use for the day-to-day management of your environment. WebCenter includes standard monitoring functions such as the Resource Monitor and Alert Monitor.

WebCenter lets technical staff view consolidated alert information and perform diagnostics on enterprise-wide connections. WebCenter helps you in the following ways:

- Decrease problem resolution time.
- Increase ease of use.
- Enhance accessibility to information because anyone with a PC, network connection, and a web browser can access the product.

Being able to monitor the network without the need to acquire mainframe knowledge decreases the training requirements for technical staff.

WebCenter resides entirely in the z/OS operating environment. The web server runs within the CA NetMaster NM for TCP/IP address space and requires no third-party components. From WebCenter, you can access the performance, diagnostics, and reporting functions of the product.

## CA NSM NetMaster Option

You can use the CA NSM NetMaster Option to monitor this product's resources from CA NSM. This component lets you monitor these resources at an enterprise layer and incorporate them into business process views. Simple point and click commands let you branch from CA NSM to WebCenter facilities for performing diagnostics and control, within context.

# Who Uses the Product

The product helps the following people to perform their tasks:

- Network operators can perform the following tasks:
  - Respond to proactive alerts before problems occur.
  - Diagnose connection problems in response to end-user problems.
  - Diagnose problems using real-time packet tracing
- Network administrators can use performance data to help them manage the IP network infrastructure.
- System programmers can diagnose software problems using real-time packet tracing.
- Application programmers can diagnose application problems using real-time packet tracing.
- DB2 staff can use the DB2 Network Information Center to find out about DB2 network activities.

# What You Can Manage

You can manage the following components in your IP network:

**Connections**

You can diagnose the following connections from connection lists:

- Telnet connections
- FTP connections
- General connections

You can use event detector to alert you on specific connection events.

**IP resources**

You can monitor and diagnose the following IP resources:

**z/OS IP stacks**

The product supports CA TCPaccess CS and IBM's Communications Server. You can monitor the stacks through the following views:

- Business view of connections by applications
- Hardware view of network interfaces
- Network view of IP, TCP, and UDP activity

These resources are defined under the STACK resource class.

**Open Systems Adapters (OSAs)**

The product supports OSA-2, OSA-Express, OSA-Express2, and OSA-Express3.

These resources are defined under the OSA resource class.

**Address Spaces**

You can monitor the IP activity for address spaces (for example, connections and throughput by ports).

These resources are defined under the ASMON resource class.

**Enterprise Extender (EE)**

You can monitor the IP activity on EE (for example, throughput by UDP ports and traffic statistics by remote control points (CPs)).

These resources are defined under the EE resource class.

**Advanced Peer to Peer Networking/High Performance Routing (APPN/HPR)**

The resource represents the Rapid Transport Protocol (RTP) pipes on a system. You can monitor the activity on and the status of the pipes.

These resources are defined under the APPNHPR resource class.

**Virtual IP Addresses (VIPAs)**

You can monitor the IP activity for dynamic VIPAs (for example, distributed bytes and connections).

These resources are defined under the VIPA resource class.

**Cisco Channel Cards**

You can monitor attributes such as channel loading, Common Link Access for Workstation (CLAW) activity, and TN3270 response time.

These resources are defined under the CIP resource class.

**Communications Storage Manager (CSM)**

You can display CSM usage, and monitor attributes such as data space buffer and ECSA storage.

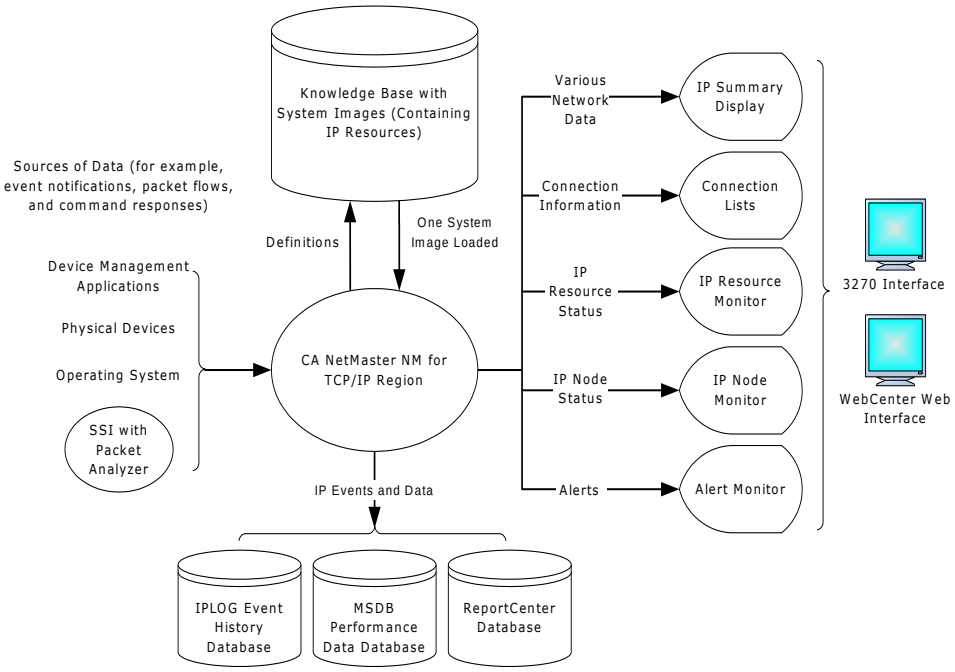
These resources are defined under the CSM resource class.

**IP nodes**

You can monitor and diagnose IP nodes. An IP node is any host that is reachable using IP from the z/OS system. The nodes can include routers, servers, workstations, other systems, and interfaces. Nodes are defined under the IPNODE resource class.

# How the Product Works

CA NetMaster NM for TCP/IP is a VTAM application program that runs as a started task on a z/OS system. A running instance (an MVS address space) is known as a region (TCP/IP management region). The region performs IP network management functions, 3270 and web user interface processing, and has internal interfaces to MVS, VTAM, and stack facilities and data. The following illustration shows the main product components and the flow of data:



The following process shows how the product works:

1. The product region gets data from various sources, for example:
   - Device management applications such as OSA/SF
   - Physical devices through Simple Network Management Protocol (SNMP)
   - Operating system through the following facilities:
     - Stack, network, and system internal application program interfaces (APIs)
     - MVS, VTAM, and UNIX System Services commands
     - System management facilities (SMF) and Resource Measurement Facility (RMF)
   - Packet Analyzer, which maintains a dynamic database of the activity on z/OS TCP/IP stacks

     Packet Analyzer is a feature of the SOLVE Subsystem Interface (SSI), which is an address space that runs on the same system as the region. The SSI communicates with the region using cross-memory services.
2. When the region receives the data, it acts on them according to the definitions in the loaded system image and defined event detectors.
   - A system image contains definitions for resources such as address spaces, stacks, and nodes. The definitions provide monitoring for various attributes to gauge the health of the resources and optionally act when a problem is detected. The Express Setup facility helps you build the initial system image.
   - An event detector contains criteria to detect specific network or system events. Initially, no event detectors are active.
3. Based on the data, the region presents the health of your network on various displays. You can define filters to select what you want to display.
   - The IP Summary Display provides a single place from where you view a snapshot of the most useful information about your network environment. Data on this display is sourced from the Packet Analyzer.
   - The connection lists show information about connections such as fragmentation, retransmissions, and round-trip time (RTT). You can diagnose a connection by performing tasks such as pinging the remote host, tracing the route, and tracing packets.
   - The IP Resource Monitor and the IP Node Monitor show the status of managed resources and nodes. In addition to various diagnostic tasks, you can review the performance of a resource or node through monitored attributes.
   - The Alert Monitor shows alerts that warn you of any problems or critical activities (for example, an alert indicating that the RTT to a node is excessive).

4. The region stores data in the following databases:
   - Start, completion, and failure event records in a history database
   - Performance data in the MSDB database and, if ReportCenter is configured, in the ReportCenter database.

   These databases let you report on network activities, which can help you plan your network. You can use WebCenter to produce these reports, which provide a rich presentation with graphs.

**More information:**

How You Learn About Your Network (see page 19)
How You Diagnose Connections (see page 26)
How You Manage IP Resources (see page 32)
How You Manage IP Nodes (see page 33)
How You Use Historical Performance for Planning (see page 59)

## Multisystem Support

Multisystem support provides you with a single point of visibility for IP network activity and managed resources on multiple systems. You can link regions together to provide an enterprise view of the managed network.

In a multisystem environment where each region manages the resources defined to its own loaded system image, failure of one region does not affect the visibility of resources on the other systems. You can still have an enterprise view of the resources managed on those systems.

A multisystem environment can consist of the following types of regions:

- Focal point regions—you have visibility of all the managed resources.
- Subordinate regions—you have visibility of the locally managed resources only. By using subordinates, you reduce the amount of traffic in the multisystem environment.

**Note:** For more information about multisystem support, see the *Administration Guide*.

# Chapter 2: Understanding the Overall Health of Your IP Network

This section contains the following topics:



## How You Learn About Your Network

To gain an initial understanding of your network, you can use the IP Summary Display. After the region is active for a while, the display becomes populated with data. You can use the display as your starting point to monitor the health of your network.

The IP Summary Display provides a single place from where you view a snapshot of the most useful information about your network environment. Data on this display is sourced from the Packet Analyzer. The display provides the following complementary perspectives:

**Condition Summary**

Provides an exception-based perspective of your network environment. The summary compares a set of monitored IP characteristics with alert threshold conditions. It charts the values of those conditions and reflects their values through the following statuses: OK, WARNING, and PROBLEM.

**IP Traffic Summary**

Provides an activity-based perspective of your IP environment. The summary provides traffic throughput statistics and identifies the most active application, port, and addresses.

**EE Traffic Explorer**

Provides information about the recent and cumulative (Enterprise Extender) EE traffic throughput.

**Alert Summary**

Provides a graphical representation of how many alerts are outstanding for each alert severity. On focal point regions, alerts from linked regions are included.

Typically, the display appears at the bottom of the primary menu when you log on to the region. If the display is not there, enter the /IPSUM shortcut at the Command prompt to access the display.

# Condition Summary

The Condition Summary shows the status of a product-defined set of conditions. A *condition* is a characteristic that is being monitored based on the underlying performance attributes of monitored IP resources.

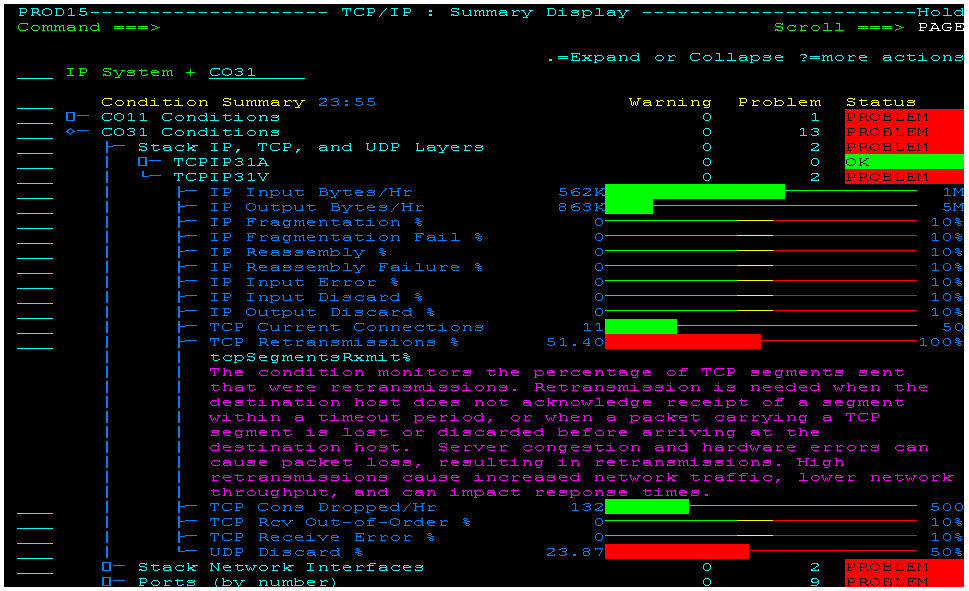
From the IP Summary Display, you can view the conditions of the following resources:

- Stack IP, TCP, and UDP layers
- Stack network interfaces
- Ports by port number or address space
- EE
- APPN/HPR

### Example: Condition of Stack IP, TCP, and UDP Layers Across Multiple Systems

This example shows a partially expanded display in multisystem mode. The display lists the systems monitored by the linked regions. Each system then expands to the condition summaries.

For the TCP Retransmissions % condition, it identifies the attribute and shows the brief explanation about the condition (through the I (Information) action). You can enter the HLP action next to a problematic attribute to review the recommended actions.



# IP Traffic Summary

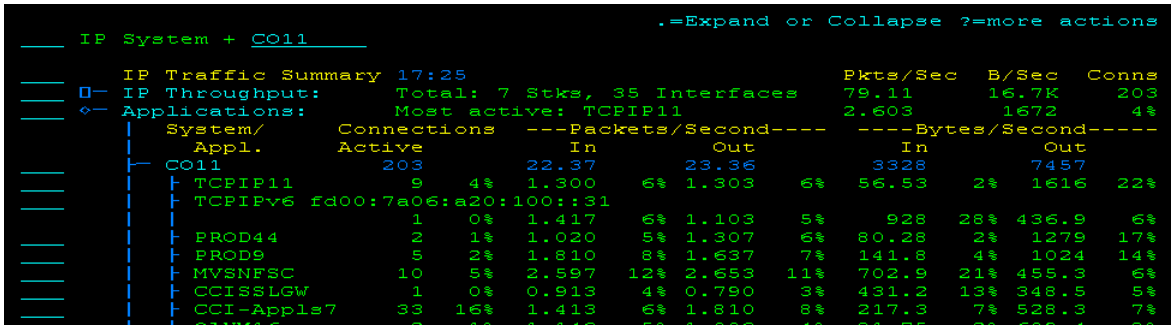
The IP Traffic Summary summarizes your IP network traffic.

From the IP Summary Display, you can access the following IP traffic summaries (when sorted by system). You can also sort the summaries by stacks.

- IP Throughput
- Applications
- TCP Server Ports
- Home Addresses
- Remote Networks
- IP Protocols
- Subsystems

### Example: IP Traffic for Defined Business Applications

This example shows a partially expanded display. The display lists the defined business applications that have IP traffic on the system.




During Express Setup, you can request that business applications be defined for the discovered address spaces. You can also define applications manually through the Maintain Application Name Definitions menu option. The shortcut is **/IPAPPLS**.

**Note:** For more information about business applications, see the *Implementation Guide*.

# EE Traffic Explorer

The EE Traffic Explorer uses data collected from the Packet Analyzer to graph EE traffic throughput.

You can use the TIME command to graph traffic for the following time frames:

- The last full clock hour
- The last full calendar day
- Cumulative (from the time the Packet Analyzer started monitoring)

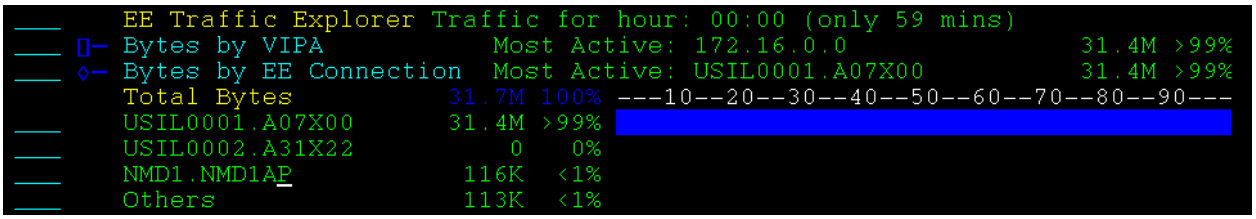
The relative size of each bar in the graphs indicates a proportion or percentage of all cumulative traffic.

You can perform various functions from the EE Traffic Explorer, for example:

- Use the F5 function key to switch between the graphical mode and the detail mode.
- Use the HLP action to find out about other features that can give you more information.

### Example: Bytes by EE Connection

This example shows an expanded display listing the remote CP names that identify the connections.



# Alert Summary

The Alert Summary summarizes the alerts in this region. A different color bar represents the alerts at a different severity level. You can enter the S action next to the summary to jump to the Alert Monitor.

# Chapter 3: Monitoring and Diagnosing Connections

This section contains the following topics:

# How You Diagnose Connections

CA NetMaster NM for TCP/IP enables you to list connections to IP stacks based on a set of criteria. For example, you can produce lists for the following connections:

- Telnet connections—For example, you can list connections by IP address, LU name, or Telnet application name. You can list connections using a Cisco channel card TN3270 server in the same way as connections to the stack's Telnet server.
- (IBM stacks on systems with at least z/OS V1R10.0) FTP connections—For example, you can list connections by IP address or user ID.
- General connections—For example, you can list connections with a particular task name or local port number.

You can use relational operator expressions to search for pertinent criteria. For example, you can search for connections that have exceeded a specified idle time, a specified byte count, or a specified idle time and byte count.

Depending on the type of connections, a connection list contains details such as host, port, byte counts, and stack.

You can select a connection from a list of connections and perform various diagnostic functions:

- Initiate packet tracing using SmartTrace.
- Perform transaction path analysis to investigate the response times for a connection.
- Display a graphical representation of connections to the node, and issue ping, traceroute and name server lookup commands.
- Drop a connection if you have sufficient authority.
- Display the SNA information for a Telnet connection.

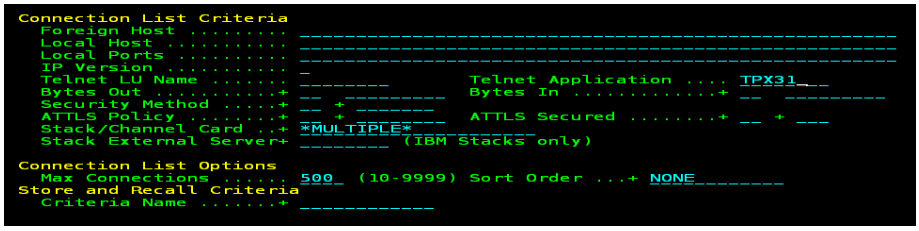
Connection events are also stored in a database for a specified period to provide a historical record. The retention period is specified in the IPFILES parameter group.

You can list connections from the Connections menu. To access the menu, enter the /IPCON shortcut.

## Connection List Example

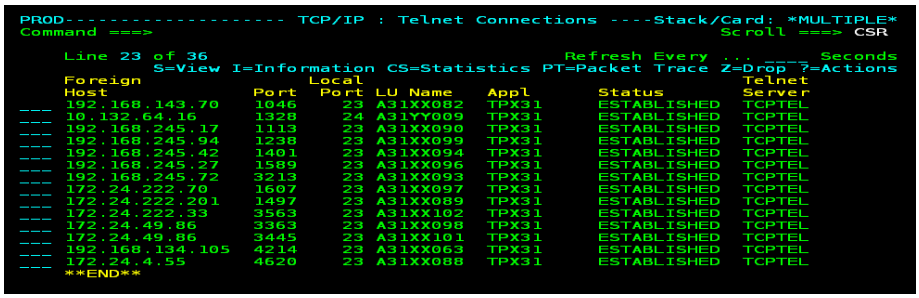
This example shows a list of Telnet connections with the TPX31 primary LU of a VTAM application. The following process shows you how to list the connections:

1. From the Connections menu, enter **T** (List Telnet Connections) and specify TPX31 as a criteria:




   The criteria lists the Telnet connections with TPX31on all monitored stacks and channel cards.

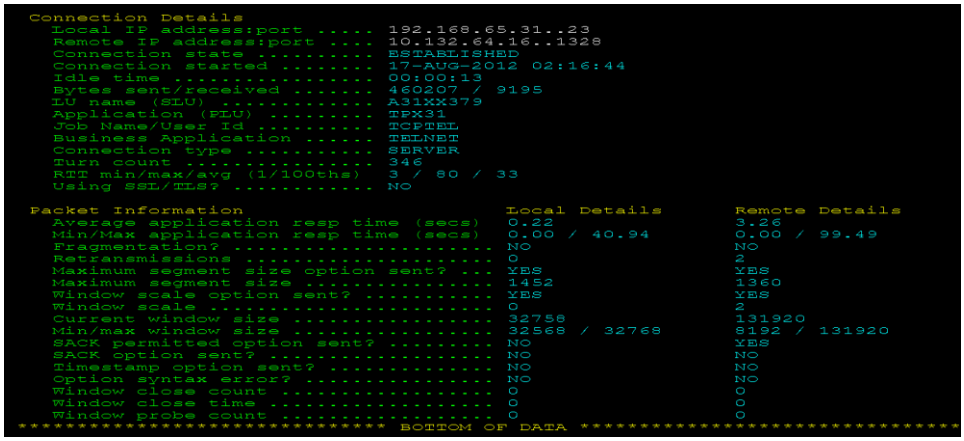
2. Press F6 (Action) to list the connections.




   You can press F11 (Right) to display more connection information. You can enter a question mark (?) next to a connection to list the actions you can perform. For example, you can use TPA (Transaction Path Analyzer) to view response times or PT (Activate Packet Trace) to trace packets.

## Connection Information Example

You can enter the I (Information) action next to a connection to display information in addition to what is available on the connection list. This example displays information about a connection with the following address: 10.132.64.16 Port 1328.




This display includes additional connection details such as RTTs, and packet information such as fragmentation and retransmissions.

# How You Detect Connection Events

The connection lists tell you about the connections. The lists do not alert you automatically to specific conditions that you want to know about (for example, termination of a critical connection). To be warned of these specific conditions, you can define event detectors.

An *event detector* defines the network and systems events that you want to monitor, and what to do when the event occurs.

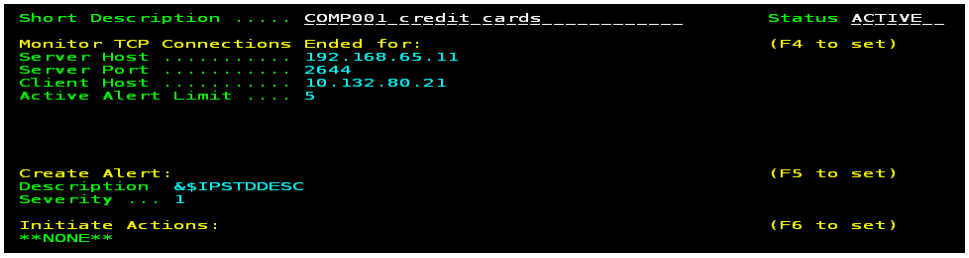
You can define an alert to raise, and you can define the wording of the alert. You can also define an automatic action to run.

Sample event detector definitions are supplied. Each type of event is represented in the samples. Use these definitions as examples when you create your own event detectors.

You can define detectors from the Event Detector Controls List. You can enter the /EDETECT shortcut to access the list.

### Example: Event Detector That Alerts on a Terminated Connection

This example shows an event detector that generates an alert when a critical connection is terminated.



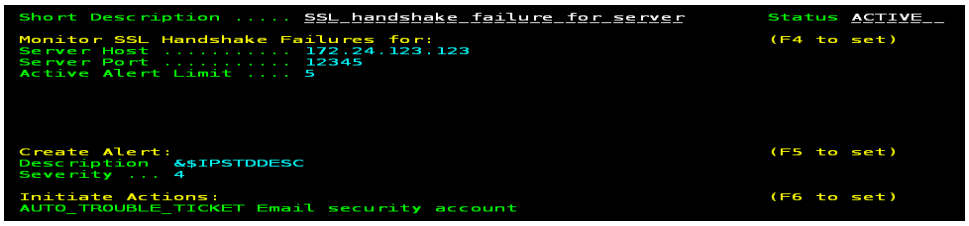

The definition monitors a connection between the CICS region that processes credit card transactions and the customer (COMP001) device that requests the transactions. If a requested transaction cannot be processed, the customer is entitled to financial penalties. The connection is critical to the business. If the connection is terminated, the event detector raises a severity one alert.

The following process shows you how to define the detector:

1. From the Event Detector Controls List, press F4 (Add) to add a detector of the TCPEND type, or copy an existing TCPEND type detector and modify the definition.
2. Provide a short description and use the function keys to specify the detection criteria and action to take:
   - Press F4 (Criteria) to specify the criteria.
   - Press F5 (Alert) to specify the alert. To see the variables that you can use, press F1 (Help).

### Example: Event Detector That Alerts on Secure Sockets Layer Handshake Failures

This example shows an event detector that sends an email to a security account when Secure Sockets Layer (SSL) handshake failures occur for a particular server. This condition can indicate that an unauthorized client is attempting to access a secure server or that an authorized client is having difficulties accessing the server. When the event is detected, an email is sent to notify interested parties of the condition.




In the definition, 172.24.123.123 is the IP address and 12345 is the port number of the secure server. If a connection is established with this server by any client and the SSL handshake negotiations fail, then an alert is raised and an email notification is sent. The automatically generated alert text is used, for example:

```
SSL handshake failure: TCP server 172.24.123.123:12345 client 10.0.0.100 stack TCPIPA
```

**Note:** The email feature relies on the definition of the email trouble ticket interface. Depending on the definition, you can specify that emails be sent to one or more addresses. You can enter the /ALTTI shortcut to define the interface.

The following process shows you how to define the detector:

1. From the Event Detector Controls List, press F4 (Add) to add a detector of the SSLHFAIL type, or copy an existing SSLHFAIL type detector and modify the definition.
2. Provide a short description, and use the function keys to specify the detection criteria and action to take:
   - Press F4 (Criteria) to specify the criteria. Identify the server and optionally the client.
   - Press F5 (Alert) to specify the alert. To see the variables that you can use, press F1 (Help).
   - Press F6 (Action), and select AUTO_TROUBLE_TICKET to specify the notification details and a short description to make the action easier to identify when the definition is viewed.

# Chapter 4: Monitoring and Diagnosing IP Resources and Nodes

This section contains the following topics:

# How You Manage IP Resources

When you first start the region, Express Setup discovers and defines the IP resources available on your system at that time in a system image. You can monitor and act on these resources from the IP Resource Monitor. You can enter the /IPMON shortcut to access the monitor. As you learn more about the IP network, you can refine the existing resources or add resources to provide more targeted monitoring.

Typically, an IP resource definition has the following features that you can use:

- You can monitor the performance attributes of individual resources. For example, the ConTotalActive attribute of a STACK resource gives the total number of active connections for the stack. Some of these attributes are also monitored on the Condition Summary.

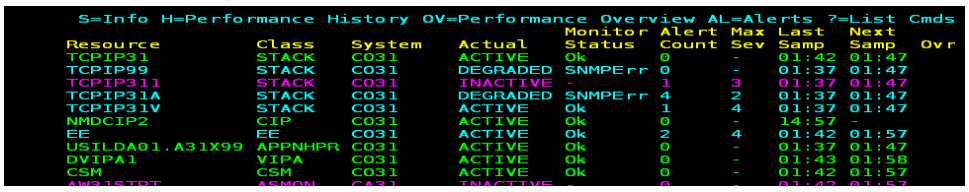
  Attributes enable you to test the performance of a resource against a value or a calculated baseline to trigger alerts and actions.
- You can monitor specific messages and specify actions to respond to those messages.
- Monitoring uses system resources. Monitoring maps enable you to monitor specific resources at the required times.

From the IP Resource Monitor, you can use the DB line command to refine resources or the F4 (Add) function key to add resources. The following process shows you how to add a resource from the IP Resource Monitor:

1. Press F4 to add a resource.
2. Select the system image to which you want to add the resource. In a multisystem environment, the image is the one on the system where the resource operates.
3. Select the class of resource you want to add.
4. Complete the definition of the resource.

### Example: IP Resource Monitor

This example shows monitored IP resources. The color reflects the status of a resource.




You can enter a question mark (?) next to a resource to list the commands you can issue. For example, you can use the IC (List IP Connections) command on a STACK resource to list connections.

# How You Manage IP Nodes

When you first start the region, Express Setup discovers and defines the IP nodes known to your system at that time in a system image. You can monitor and act on these nodes from the IP Node Monitor. You can enter the /IPNODE shortcut to access the monitor. As you learn more about the IP network, you can refine the existing nodes or add nodes to provide more targeted monitoring.

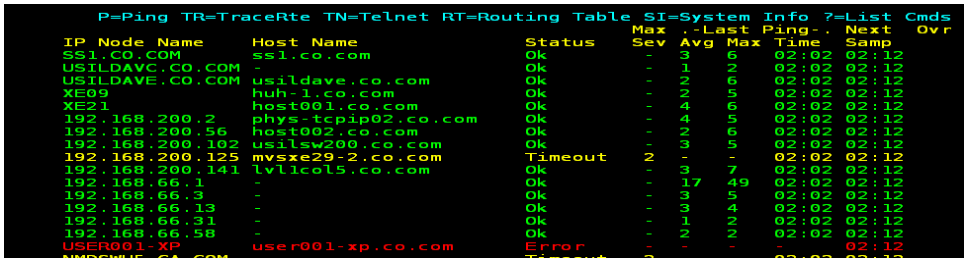
An IP node definition belongs to a monitor group that specifies the performance attributes to monitor. You can refine the monitoring for a node by attaching it to a different monitor group or modifying the existing group definition (which affects all nodes belongs to the group). As with IP resources, you can restrict the monitoring of an IP node to specific times.

From the IP Node Monitor, you can use the DB line command to refine nodes or the F4 (Add) function key to add nodes.

You can add or modify monitor groups from the IP Node Monitor Group List. You can enter the /IPMONG shortcut to access the menu. You can also modify an attached group directly from the node definition.

### Example: IP Node Monitor

This example shows monitored IP nodes. The color reflects the status of a node.




You can press F11 (Right) to display more node information. You can enter a question mark (?) next to a node to list the commands you can issue. For example, you can use PT (Activate Packet Trace) to trace packets.

# Chapter 5: Monitoring and Diagnosing the Enterprise Extender

This section contains the following topics:



## How You Manage the EE Resource

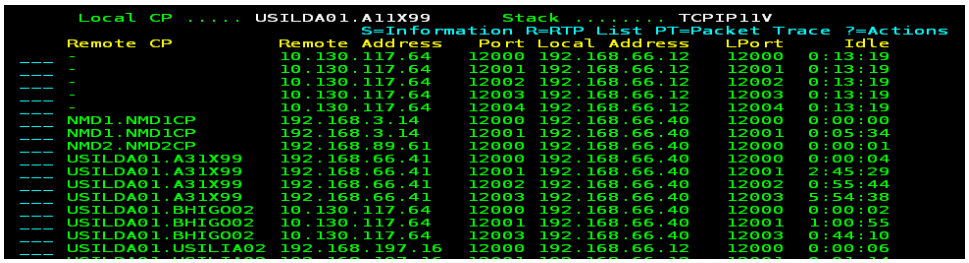
You can explore EE using the EE Traffic Explorer (see page 22).

Also, when you first start the region, Express Setup discovers and defines an EE resource on your system in a system image. You can monitor and act on the resource from the IP Resource Monitor. As you learn more about the resource, you can refine the resource to provide more targeted monitoring. For example, by default, an EE resource monitors all remote CPs. You can restrict the monitoring to specific CPs by specifying a filter in the resource definition.

From the monitor, you can issue various commands to find out more about the resource. Some of these commands are also available from the Enterprise Extender Management menu, which you can access using the /EE shortcut.

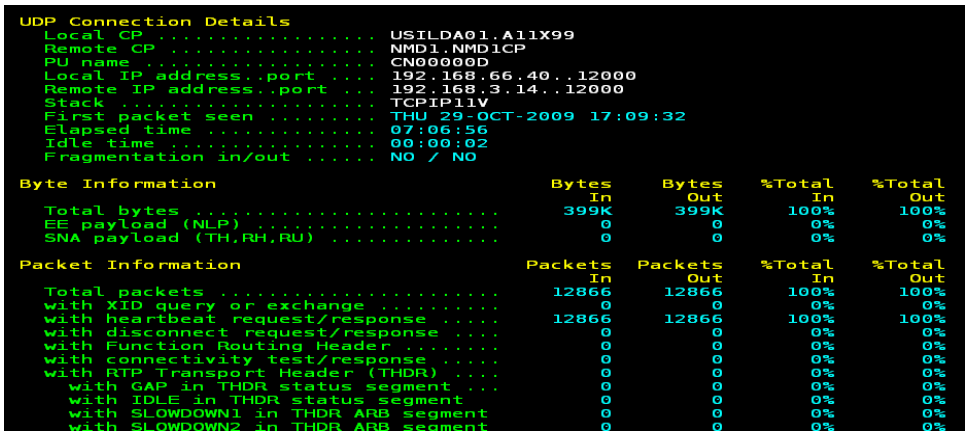
## UDP Connections Example

You can enter the UC (Display UDP Connections) command next to an EE resource to list the UDP connections by the name of the remote CP.



```
      Local CP ..... USILDA01.A11X99       Stack ........ TCPIP11V
                                 S=Information R=RTP List PT=Packet Trace ?=Actions
     Remote CP          Remote Address    Port Local Address    LPort     Idle
___  -                  10.130.117.64    12000 192.168.66.12    12000   0:13:19
___  -                  10.130.117.64    12001 192.168.66.12    12001   0:13:19
___  -                  10.130.117.64    12002 192.168.66.12    12002   0:13:19
___  -                  10.130.117.64    12003 192.168.66.12    12003   0:13:19
___  -                  10.130.117.64    12004 192.168.66.12    12004   0:13:19
___  NMD1.NMD1CP        192.168.3.14     12000 192.168.66.40    12000   0:00:00
___  NMD1.NMD1CP        192.168.3.14     12001 192.168.66.40    12001   0:05:34
___  NMD2.NMD2CP        192.168.89.61    12000 192.168.66.40    12000   0:00:01
___  USILDA01.A31X99    192.168.66.41    12000 192.168.66.40    12000   0:00:04
___  USILDA01.A31X99    192.168.66.41    12001 192.168.66.40    12001   2:45:29
___  USILDA01.A31X99    192.168.66.41    12002 192.168.66.40    12002   0:55:44
___  USILDA01.A31X99    192.168.66.41    12003 192.168.66.40    12003   5:54:38
___  USILDA01.BHIGO02   10.130.117.64    12000 192.168.66.40    12000   0:00:02
___  USILDA01.BHIGO02   10.130.117.64    12001 192.168.66.40    12001   1:00:55
___  USILDA01.BHIGO02   10.130.117.64    12003 192.168.66.40    12003   0:44:10
___  USILDA01.USILIA02  192.168.197.16   12000 192.168.66.12    12000   0:00:06
```

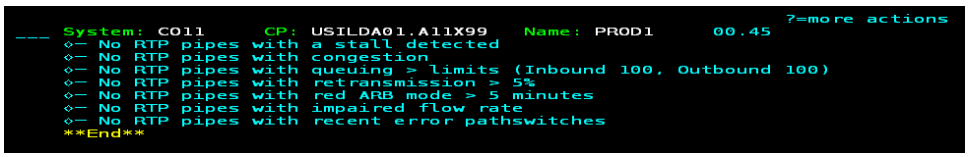
You can press F11 (Right) to display more information. You can enter a question mark (?) next to a CP name to list the actions you can perform. For example, you can enter S next to the NMD1.NMD1CP CP to display information in addition to what is available on the list.



```
UDP Connection Details
  Local CP ................... USILDA01.A11X99
  Remote CP .................. NMD1.NMD1CP
  PU name .................... CN00000D
  Local IP address..port .... 192.168.66.40..12000
  Remote IP address..port ... 192.168.3.14..12000
  Stack ...................... TCPIP11V
  First packet seen .......... THU 29-OCT-2009 17:09:32
  Elapsed time ............... 07:06:56
  Idle time .................. 00:00:02
  Fragmentation in/out ....... NO / NO

Byte Information                                Bytes     Bytes    %Total    %Total
                                                  In       Out        In       Out
  Total bytes ..........................        399K      399K      100%      100%
  EE payload (NLP) .....................           0         0        0%        0%
  SNA payload (TH,RH,RU) ...............           0         0        0%        0%

Packet Information                            Packets   Packets    %Total    %Total
                                                  In       Out        In       Out
  Total packets ........................       12866     12866      100%      100%
  with XID query or exchange ...........           0         0        0%        0%
  with heartbeat request/response .....        12866     12866      100%      100%
  with disconnect request/response ....           0         0        0%        0%
  with Function Routing Header ........           0         0        0%        0%
  with connectivity test/response .....           0         0        0%        0%
  with RTP Transport Header (THDR) ....           0         0        0%        0%
    with GAP in THDR status segment ...           0         0        0%        0%
    with IDLE in THDR status segment ..           0         0        0%        0%
    with SLOWDOWN1 in THDR ARB segment ..         0         0        0%        0%
    with SLOWDOWN2 in THDR ARB segment ..         0         0        0%        0%
```

## RTP Pipes Example

You can enter the RH (RTP Health Check) command next to an EE resource to check the health of the EE RTP pipes. This example shows that all pipes are healthy.



```
                                                                  ?=more actions
___  System: C011      CP: USILDA01.A11X99   Name: PROD1      00.45
     ◇— No RTP pipes with a stall detected
     ◇— No RTP pipes with congestion
     ◇— No RTP pipes with queuing > limits (Inbound 100, Outbound 100)
     ◇— No RTP pipes with retransmission > 5%
     ◇— No RTP pipes with red ARB mode > 5 minutes
     ◇— No RTP pipes with impaired flow rate
     ◇— No RTP pipes with recent error pathswitches
     **End**
```

If the list shows an unhealthy RTP pipe, you can enter a question mark (?) next to the pipe to list the actions you can perform. For example, you can use S (Formatted Display of the RTP) to view details about the pipe or PT (Activate Packet Trace) to trace packets.

# How You Diagnose EE Using SmartTrace

EE traces have summary information that indicates the characteristics of the SNA information contained within the trace.

Although you can trace packets through the various lists from the IP Resource Monitor, the EE SmartTrace Menu puts these trace functions in one place for easy access. You can use the /EETRACE shortcut to access the menu. From the menu, you can trace packets through the following EE components:

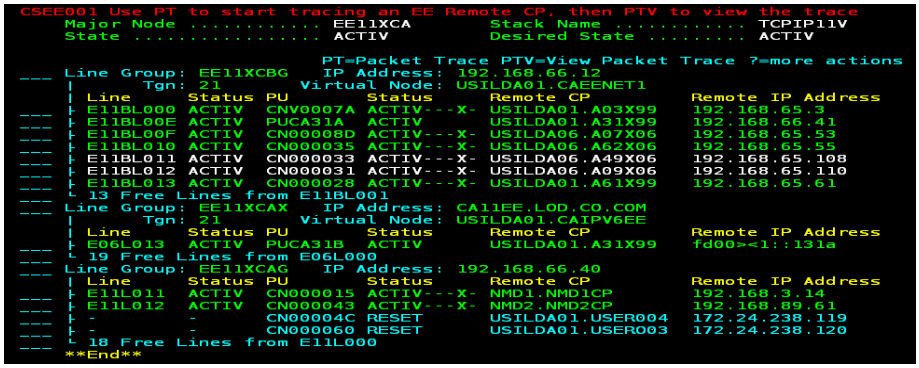
- Remote CPs
- RTP pipes
- UDP connections
- UDP ports
- VIPAs

### Example: Trace an RTP Pipe

This example shows the trace of an RTP pipe that is using a line within the EE. The following process shows you how to perform the trace:

1. From the EE SmartTrace menu, select **C** (Trace EE Remote CP).

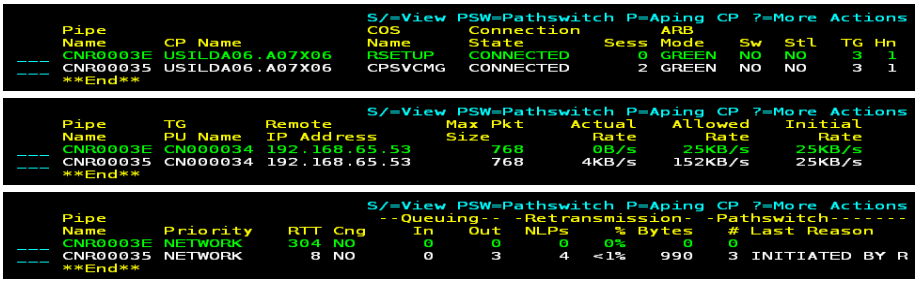
   The lines within the EE are listed, for example:




   Lines with RTP pipes are in green.

2. Enter **R** next to the E11BL00F line.

   The RTP pipes using the line are listed. The following example shows the displayed information over several screens using the F11 (Right) function key:



```
                                    S/-View PSW=Pathswitch P=Aping CP ?=More Actions
    Pipe                            COS       Connection          ARB
    Name      CP Name               Name      State         Sess Mode    Sw  Stl   TG Hn
___ CNR0003E USILDA06.A07X06        RSETUP    CONNECTED        0 GREEN   NO  NO     3  1
___ CNR00035 USILDA06.A07X06        CPSVCMG   CONNECTED        2 GREEN   NO  NO     3  1
    **End**
```

```
                                    S/-View PSW=Pathswitch P=Aping CP ?=More Actions
    Pipe      TG        Remote           Max Pkt     Actual    Allowed    Initial
    Name      PU Name   IP Address       Size          Rate       Rate       Rate
___ CNR0003E CN000034 192.168.65.53         768        0B/s     25KB/s     25KB/s
___ CNR00035 CN000034 192.168.65.53         768       4KB/s    152KB/s     25KB/s
    **End**
```

```
                                    S/-View PSW=Pathswitch P=Aping CP ?=More Actions
    Pipe                              --Queuing--  -Retransmission-  -Pathswitch-------
    Name      Priority    RTT Cng     In    Out  NLPs    % Bytes    # Last Reason
___ CNR0003E NETWORK     304 NO       0      0     0     0%      0    0
___ CNR00035 NETWORK       8 NO       0      3     4    <1%    990    3 INITIATED BY R
    **End**
```

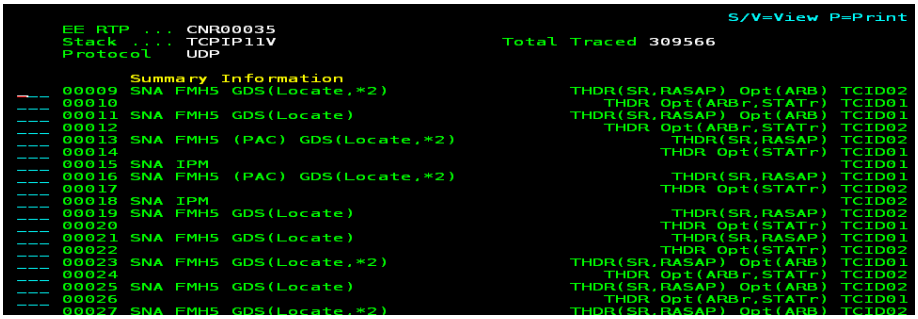
3. You want to trace the CNR00035 pipe. Enter **PT** next to the pipe.

   You are prompted whether you want to include packets with SNA data only. By default, the trace includes all packets.

4. Press F6 (Action) to start the trace.

5. Enter **PTV** next to the traced line group to view the trace.

   The following example shows the summary information for the packets:



```
                                                                    S/V=View P=Print
    EE RTP ... CNR00035
    Stack  ... TCPIP11V                          Total Traced 309566
    Protocol   UDP

          Summary Information
___ 00009 SNA FMH5 GDS(Locate,*2)                THDR(SR,RASAP) Opt(ARB) TCID02
___ 00010                                          THDR Opt(ARBr,STATr) TCID01
___ 00011 SNA FMH5 GDS(Locate)                   THDR(SR,RASAP) Opt(ARB) TCID01
___ 00012                                          THDR Opt(ARBr,STATr) TCID02
___ 00013 SNA FMH5 (PAC) GDS(Locate,*2)                 THDR(SR,RASAP) TCID02
___ 00014                                             THDR Opt(STATr) TCID01
___ 00015 SNA IPM                                                     TCID01
___ 00016 SNA FMH5 (PAC) GDS(Locate,*2)                 THDR(SR,RASAP) TCID01
___ 00017                                             THDR Opt(STATr) TCID02
___ 00018 SNA IPM                                                     TCID02
___ 00019 SNA FMH5 GDS(Locate)                          THDR(SR,RASAP) TCID02
___ 00020                                             THDR Opt(STATr) TCID01
___ 00021 SNA FMH5 GDS(Locate)                          THDR(SR,RASAP) TCID01
___ 00022                                             THDR Opt(STATr) TCID02
___ 00023 SNA FMH5 GDS(Locate,*2)                THDR(SR,RASAP) Opt(ARB) TCID01
___ 00024                                          THDR Opt(ARBr,STATr) TCID02
___ 00025 SNA FMH5 GDS(Locate)                   THDR(SR,RASAP) Opt(ARB) TCID02
___ 00026                                          THDR Opt(ARBr,STATr) TCID01
___ 00027 SNA FMH5 GDS(Locate,*2)                THDR(SR,RASAP) Opt(ARB) TCID02
```

6. Press F10 (Left) or F11 (Right) to display other packet information. Enter **S** next to a packet to display the details and contents of the packet.

# Chapter 6: Tracing Packets

This section contains the following topics:



## How You Trace Packets

Packet tracing is a valuable tool for troubleshooting network connectivity problems. CA NetMaster NM for TCP/IP provides the following packet tracing facilities:

**SmartTrace**

Is the integrated real-time packet tracing facility for CA NetMaster NM for TCP/IP. SmartTrace lets you do the following:

- Initiate a trace, and view the results in real time.
- Define trace criteria using a panel interface.
- Export trace data to libpcap or CTRACE format, enabling you to use the trace data with other packet tracing viewers.

**CTRACE**

Is a menu-assisted facility for starting and stopping IBM's component trace (SYSTCPDA) to obtain and view traces of IP packets. Using this facility, you can initiate a trace without having to know the commands required to start CTRACE.

Packet tracing has several access points:

- The Packet Tracing Menu enables you to maintain SmartTrace definitions and records. The menu also provides an option to access CTRACE. You can enter the /SMART shortcut to access the menu.
- For SmartTrace, the following access points are available:
  - You can initiate a trace by using a line command from the IP Node Monitor, IP Resource Monitor, or a connection list.
  - You can initiate a trace from resource management menus (for example, the Stack Management menu, which you access using the /STACK shortcut).

# Packet Data Decoding

Decoding interprets the packet contents according to the specific protocol and application. When a packet is decoded, its data is broken down into individual elements (for example, commands and flags). Whenever possible, the meaning of each element is displayed in readable text. When a packet is not decoded, its data is displayed in hexadecimal dump format with the corresponding EBCDIC and ASCII translations.

TCP packets on the ports specified in the SMARTTRACE parameter group are decoded. The following protocols are decoded:

- Distributed Relational Database Architecture (DRDA)
- FTP
- HTTP
- Simple Object Access Protocol (SOAP) (through HTTP ports)
- Telnet

In addition to this decoding, you can enter the DECODE command on a Packet List panel to decode TCP packet data for other DRDA, FTP, HTTP, and Telnet ports. Decoding applies to the current session. If you exit the panel and then reenter it, enter the command again to perform specific decoding.

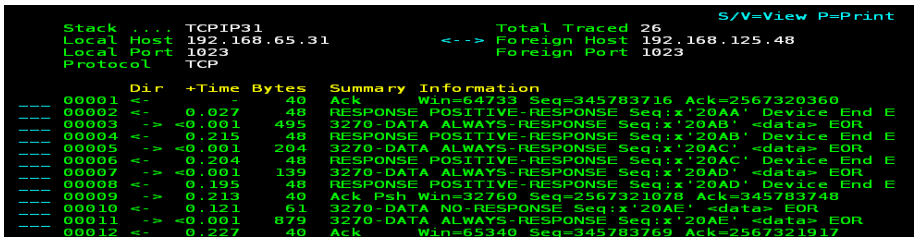
Packets that use the following protocols are also decoded by default:

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Generic Routing Encapsulation (GRE)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- IPSec
- Open Shortest Path First Interior Gateway Protocol (OSPFIGP)
- Transport Layer Security (TLS) and Secure Sockets Layer (SSL) handshake
- User Datagram Protocol (UDP) (for Enterprise Extender data only)

# Packet Trace Example

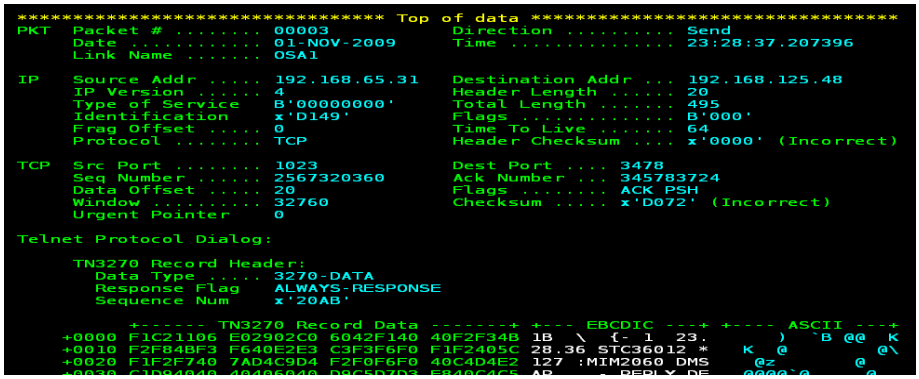
This example shows the packet trace for a Telnet connection. The following process shows you how to trace the packets:

1. Enter **/CONNT**, and specify the criteria for the Telnet connections you want to list.
2. Enter **PT** next to a connection to start a trace.
3. Enter **PTV** next to the traced connection to view the trace. Depending on the traffic, you may need to wait for packets to be collected.




You can press F11 (Right) to display more packet information. As shown in the trace, some packets are decoded.

4. Enter **S** next to a packet to display the details and contents of the packet.




**More information:**

How You Diagnose EE Using SmartTrace (see page 37)
How You Diagnose DDF Using SmartTrace (see page 50)

# SmartTrace Definitions

SmartTrace definitions provide more targeted tracing than is available through the PT command. You can add and activate these definitions from the All Traces panel, which you can access from the Packet Tracing Menu or using the /TRALL shortcut.

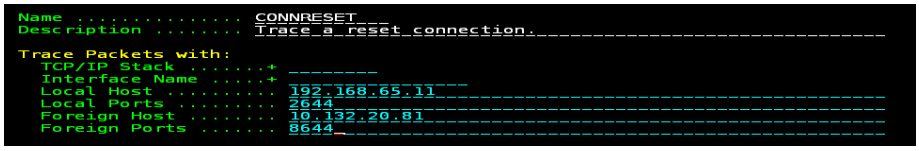
CA NetMaster NM for TCP/IP provides a number of definition types that you can use. A definition type provides various criteria that you can specify. For example, a TCP trace provides the following criteria:

- Stack and interface names, and addresses
- TCP flags and packet data
- Criteria that causes the trace to stop and actions to take when the trace stops

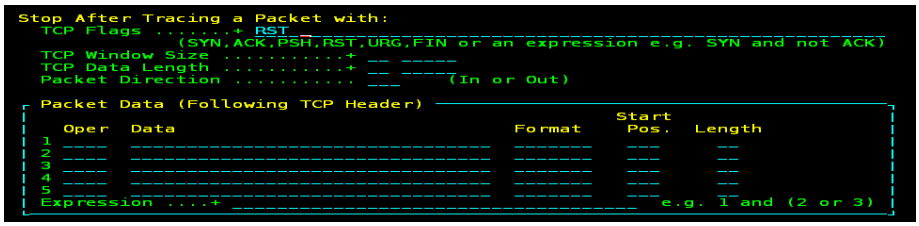
### Example: Trace Packets in an Intermittent TCP Connection

Resets are occurring in a TCP connection intermittently. You want to find out the packet activity before a reset. You decide to create a SmartTrace definition to capture this activity. You want the trace to stop when a TCP RST packet is received and capture the packets up to that point. The following process shows you how to create the definition:

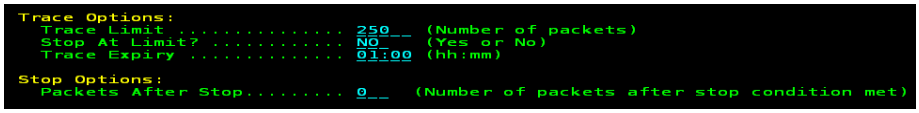
1. From the All Traces panel, press F4 (Add) to add a new TCP trace.
2. Name and provide a short description for the trace, and specify the local and foreign hosts that are having intermittent TCP connections, for example:




3. Press F8 (Forward) twice to display Page 3 of the definition, and specify the RST flag as the criteria for the trace to stop:




4. Press F8 (Forward), and accept the values on Page 4. The trace keeps up to 250 packets before a TCP RST packet is received.



# Chapter 7: Monitoring and Diagnosing IP Applications

This section contains the following topics:

# How You Use Business Application Names

The primary goal of a mainframe-based network is to provide reliable access to critical data and applications that reside on z/OS systems. This data and these applications underpin many of your business applications and services. Being able to view network activity and workload in terms of your key business applications and services enables you to better understand their well-being, prioritize network events, and assure service to the business.

You can define application names to group connections to specific business applications. During Express Setup, you can request that business applications be defined for the discovered address spaces. You can also define applications manually from the Application Definition Name List. The shortcut is **/IPAPPLS**. You can set connection alerts for defined applications through Connection Workload Monitoring in STACK resources.

You can define application names to group connections to specific business applications. During Express Setup, you can specify whether you want to define applications names automatically for discovered address spaces. You can also set connection alerts by application through Connection Workload Monitoring in STACK resources.

After monitoring has been active for some time, you can view the traffic for these applications by various means, for example:

- From the IP Traffic Summary
- Using the TRS (Display IP Traffic Statistics) or WC (Display Connection Workload Performance) line command on a STACK resource
  - The TRS command displays application traffic by bytes and packets.
  - The WC command enables you to display the data collected for monitored attributes such as ConActive, which gives the total number of connections by applications.

The following process shows you how to implement business application monitoring:

1. Enter **/IPAPPLS**, and refine or add application name definitions.
2. Wait for data to be collected for the applications.
3. Set connection alerts. Enter **/IPMON** and then **UM** next to a STACK resource on the current system. Set alerts for the Connection Workload Monitoring attributes as required. You can qualify the attributes by the different applications that have data and set different alerts for the qualified attributes. The relevant attributes are ConActive, ConBytes, and ConConnects.

### Examples: Application Names

The following examples show some possible application names:

- FOREX as an application name for all connections between local port 12345 and remote addresses *x* through *y*
- HTTPS as an application name for all connections to local ports 443 and 8443
- WebSphereMQ as an application name for all connections to local port 1414

## How You Monitor and Diagnose FTP and Telnet Traffic

You can set up suitable FTP and Telnet business application names, and use a STACK resource's FTP workload monitoring and Telnet workload monitoring to gather data for the monitored attributes. Include the attributes you want to monitor in the STACK resource definition. Use the WF and WT line commands to view the monitored attributes.

You can define event detectors to provide alerts for specific events.

You can list FTP and Telnet connections from the Connections menu. Using the CF (List Connections (Advanced)) or CH (List Connections (with History)) option, you can list connections using application names as criteria.

# Chapter 8: Monitoring and Diagnosing DB2 Network

This section contains the following topics:



## DB2 Network Information Center

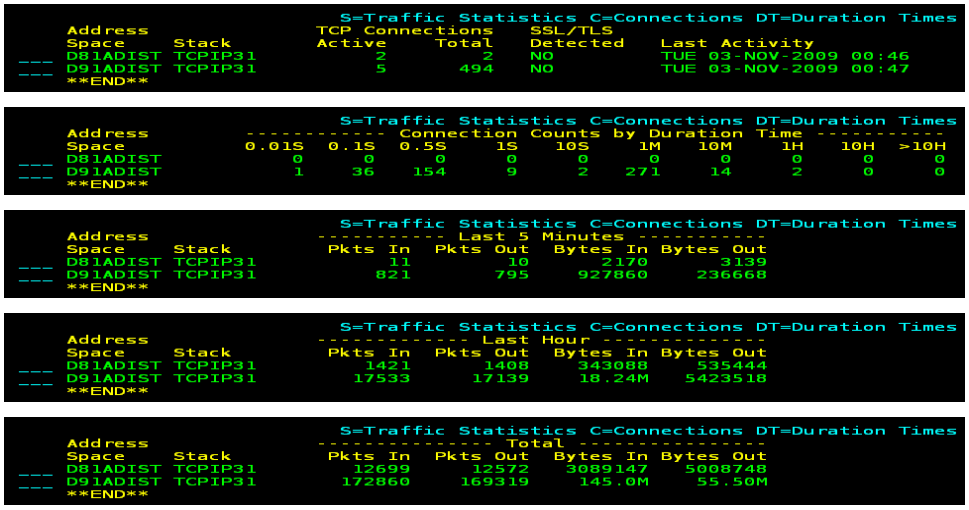
The DB2 Network Information Center provides a single point of access for DB2 staff to find out about DB2 network activities:

- You can find out about and diagnose Distributed Data Facility (DDF) connections.
- You can display statistics on DB2 address space activities.
- You can trace packets for defined ASMON resources of Type DB2.

You can access the menu for the DB2 Network Information Center using the /DB2 panel shortcut, or the D option on the Address Space and Port Management menu. To learn more about the center, see the tutorial on the menu.

# How You Display DDF Address Space Activities

To display statistics on DDF address spaces, select the TC (DB2 DDF TCP Application Activity) option from DB2 for z/OS Network Information Center menu. Only address spaces that have TCP packet activities are listed. The following example shows the displayed information over several screens using the F11 (Right) function key.



```
                                S=Traffic Statistics C=Connections DT=Duration Times
     Address                  TCP Connections    SSL/TLS
     Space      Stack         Active     Total   Detected    Last Activity
___  D81ADIST  TCPIP31             2         2   NO          TUE 03-NOV-2009 00:46
___  D91ADIST  TCPIP31             5       494   NO          TUE 03-NOV-2009 00:47
     **END**
```

```
                                S=Traffic Statistics C=Connections DT=Duration Times
     Address                  ------------ Connection Counts by Duration Time ------------
     Space          0.01S  0.1S   0.5S     1S     10S     1M     10M     1H     10H   >10H
___  D81ADIST           0     0      0      0       0      0       0      0       0      0
___  D91ADIST           1    36    154      9       2    271      14      2       0      0
     **END**
```

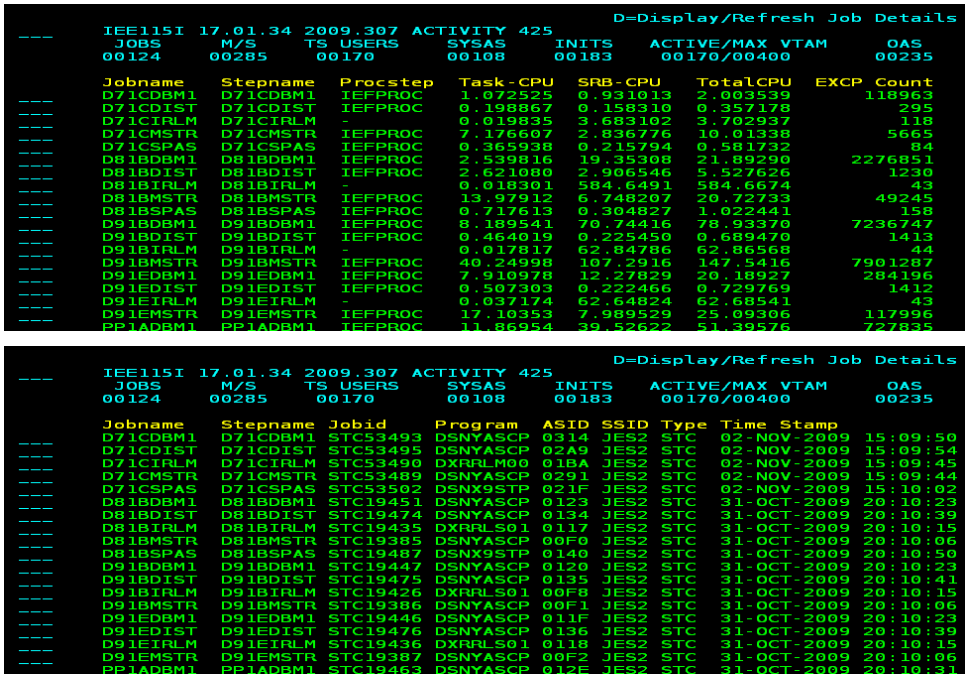
```
                                S=Traffic Statistics C=Connections DT=Duration Times
     Address                  ----------- Last 5 Minutes -----------
     Space      Stack         Pkts In  Pkts Out  Bytes In Bytes Out
___  D81ADIST  TCPIP31             11        10      2170      3139
___  D91ADIST  TCPIP31            821       795    927860    236668
     **END**
```

```
                                S=Traffic Statistics C=Connections DT=Duration Times
     Address                  ------------- Last Hour -------------
     Space      Stack         Pkts In  Pkts Out  Bytes In Bytes Out
___  D81ADIST  TCPIP31           1421      1408    343088    535444
___  D91ADIST  TCPIP31          17533     17139     18.24M   5423518
     **END**
```

```
                                S=Traffic Statistics C=Connections DT=Duration Times
     Address                  --------------- Total ---------------
     Space      Stack         Pkts In  Pkts Out  Bytes In Bytes Out
___  D81ADIST  TCPIP31          12699     12572   3089147   5008748
___  D91ADIST  TCPIP31         172860    169319    145.0M    55.50M
     **END**
```

# How You Display DB2 Address Space Information

To display information about all DB2 address spaces on the system, select the AS (DB2 Address Space Information) option from DB2 for z/OS Network Information Center menu. The following example shows the displayed information over several screens using the F11 (Right) function key.



```
                                                    D=Display/Refresh Job Details
___     IEE115I 17.01.34 2009.307 ACTIVITY 425
          JOBS      M/S     TS USERS     SYSAS     INITS    ACTIVE/MAX VTAM      OAS
         00124    00285     00170        00108     00183     00170/00400        00235

         Jobname   Stepname  Procstep  Task-CPU   SRB-CPU    TotalCPU  EXCP Count
___      D71CDBM1  D71CDBM1  IEFPROC   1.072525   0.931013   2.003539      118963
___      D71CDIST  D71CDIST  IEFPROC   0.198867   0.158310   0.357178         295
___      D71CIRLM  D71CIRLM  -         0.019835   3.683102   3.702937         118
___      D71CMSTR  D71CMSTR  IEFPROC   7.176607   2.836776  10.01338         5665
___      D71CSPAS  D71CSPAS  IEFPROC   0.365938   0.215794   0.581732          84
___      D81BDBM1  D81BDBM1  IEFPROC   2.539816  19.35308   21.89290      2276851
___      D81BDIST  D81BDIST  IEFPROC   2.621080   2.906546   5.527626         1230
___      D81BIRLM  D81BIRLM  -         0.018301   584.6491   584.6674           43
___      D81BMSTR  D81BMSTR  IEFPROC   13.97912   6.748207   20.72733        49245
___      D81BSPAS  D81BSPAS  IEFPROC   0.717613   0.304827   1.022441          158
___      D91BDBM1  D91BDBM1  IEFPROC   8.189541   70.74416   78.93370      7236747
___      D91BDIST  D91BDIST  IEFPROC   0.464019   0.225450   0.689470         1413
___      D91BIRLM  D91BIRLM  -         0.017817   62.84786   62.86568           44
___      D91BMSTR  D91BMSTR  IEFPROC   40.24998   107.2916   147.5416      7901287
___      D91EDBM1  D91EDBM1  IEFPROC   7.910978   12.27829   20.18927       284196
___      D91EDIST  D91EDIST  IEFPROC   0.507303   0.222466   0.729769         1412
___      D91EIRLM  D91EIRLM  -         0.037174   62.64824   62.68541           43
___      D91EMSTR  D91EMSTR  IEFPROC   17.10353   7.985529   25.09306       117996
___      PP1ADBM1  PP1ADBM1  IEFPROC   11.86954   39.52622   51.39576       727835
```



```
                                                    D=Display/Refresh Job Details
___     IEE115I 17.01.34 2009.307 ACTIVITY 425
          JOBS      M/S     TS USERS     SYSAS     INITS    ACTIVE/MAX VTAM      OAS
         00124    00285     00170        00108     00183     00170/00400        00235

         Jobname   Stepname  Jobid     Program   ASID SSID Type Time Stamp
___      D71CDBM1  D71CDBM1 STC53493  DSNYASCP  0314 JES2 STC  02-NOV-2009 15:09:50
___      D71CDIST  D71CDIST STC53495  DSNYASCP  02A9 JES2 STC  02-NOV-2009 15:09:54
___      D71CIRLM  D71CIRLM STC53490  DXRRLM00 01BA JES2 STC  02-NOV-2009 15:09:45
___      D71CMSTR  D71CMSTR STC53489  DSNYASCP  0291 JES2 STC  02-NOV-2009 15:09:44
___      D71CSPAS  D71CSPAS STC53502  DSNX9STP 021F JES2 STC  02-NOV-2009 15:10:02
___      D81BDBM1  D81BDBM1 STC19451  DSNYASCP  0123 JES2 STC  31-OCT-2009 20:10:23
___      D81BDIST  D81BDIST STC19474  DSNYASCP  0134 JES2 STC  31-OCT-2009 20:10:39
___      D81BIRLM  D81BIRLM STC19435  DXRRLS01 0117 JES2 STC  31-OCT-2009 20:10:15
___      D81BMSTR  D81BMSTR STC19385  DSNYASCP  00F0 JES2 STC  31-OCT-2009 20:10:06
___      D81BSPAS  D81BSPAS STC19487  DSNX9STP 0140 JES2 STC  31-OCT-2009 20:10:50
___      D91BDBM1  D91BDBM1 STC19447  DSNYASCP  0120 JES2 STC  31-OCT-2009 20:10:23
___      D91BDIST  D91BDIST STC19475  DSNYASCP  0135 JES2 STC  31-OCT-2009 20:10:41
___      D91BIRLM  D91BIRLM STC19426  DXRRLS01 00F8 JES2 STC  31-OCT-2009 20:10:15
___      D91BMSTR  D91BMSTR STC19386  DSNYASCP  00F1 JES2 STC  31-OCT-2009 20:10:06
___      D91EDBM1  D91EDBM1 STC19446  DSNYASCP  011F JES2 STC  31-OCT-2009 20:10:23
___      D91EDIST  D91EDIST STC19476  DSNYASCP  0136 JES2 STC  31-OCT-2009 20:10:39
___      D91EIRLM  D91EIRLM STC19436  DXRRLS01 0118 JES2 STC  31-OCT-2009 20:10:15
___      D91EMSTR  D91EMSTR STC19387  DSNYASCP  00F2 JES2 STC  31-OCT-2009 20:10:06
___      PP1ADBM1  PP1ADBM1 STC19463  DSNYASCP  012E JES2 STC  31-OCT-2009 20:10:31
```

# How You Diagnose DDF Using SmartTrace

To access SmartTrace functions, use the ST (DB2 DDF SmartTrace) option to open the Address Space SmartTrace Menu. From the menu, you can select the DDF address space you want to trace. Only address spaces defined as ASMON resources of Type DB2 are available.

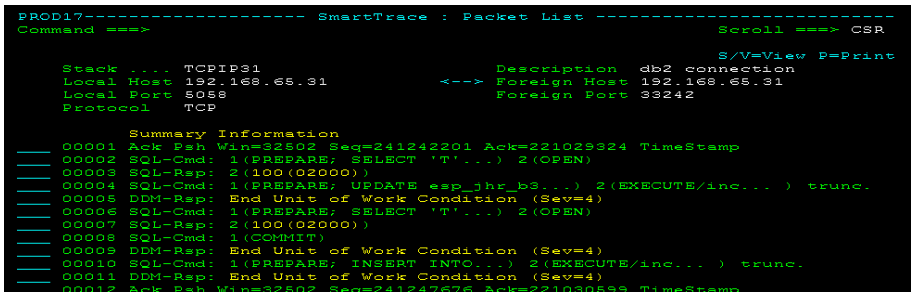
IBM's DB2 distributed database functionality is based on DRDA. Decoded DRDA packets help application programmers and network analysts who have limited knowledge of DB2 to diagnose problems.

The SMARTTRACE parameter group specifies the ports to decode. You can also use the DECODE command to specify ports on demand.

On the 3270 interface, you can use the following primary commands to change the contents in the Summary Information column:

**SQLVIEW**

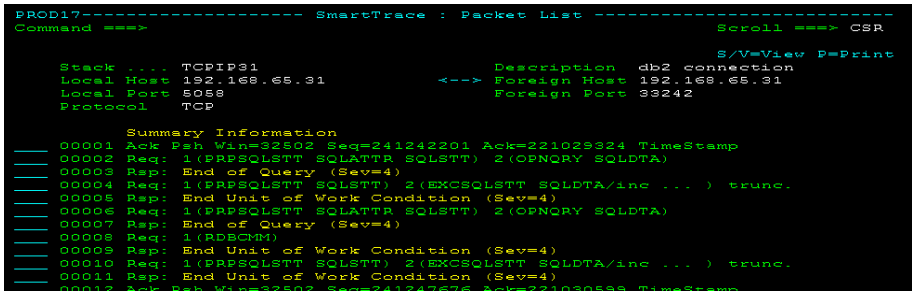
(Default view) Displays the SQL commands and responses in a DRDA packet. If there is no SQL information, the Distributed Data Management (DDM) commands and responses are shown.




This view is useful for troubleshooting SQL application issues. When a response shows an SQL status code, you can display an explanation of the code using the SQL line command.

**DDMVIEW**

Displays only the DDM commands and responses in a DRDA packet. This view requires knowledge of the DRDA command set. The following panel shows the previous example in DDM view:



# Chapter 9: Understanding IP Network Security

This section contains the following topics:



## IP Network Security Center

The IP Network Security Center provides a single point of access for you to find out about and manage the security of your IP network:

- You can find out about and diagnose problems for secured connections.
- You can find out about IPSec configuration and manage tunnels.

You can access these functions from the IP Security menu, using the /SECURE panel shortcut or the SEC option on the Stack Management menu.

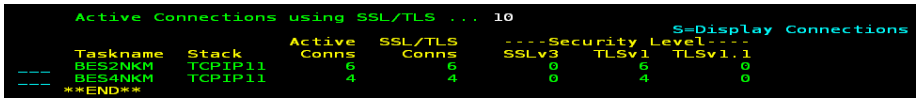
# How You Diagnose Secured Connections

To target your diagnosis on connections that are secured, use the Summary options on the IP Security menu. From the summary, you can drill down to a connection list. This list is the same as what you can display from the Connections menu, but with predefined criteria.

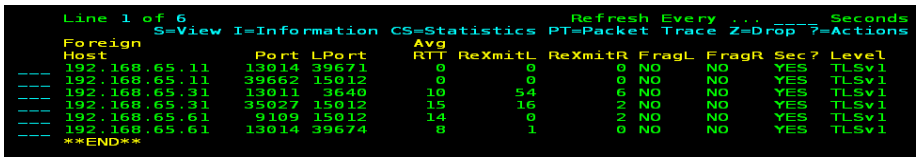
### Example: Connections Secured by SSL/TLS

This example shows you how to list connections secured by Secure Socket Layer/Transport Layer Security (SSL/TLS).

1. From the IP Security menu, enter **S** (SSL/TLS Summary) to list the tasks that have active connections secured by SSL/TLS.




2. Enter **S** next to a task to list the connections. The following example includes information about the security status:




# How You Manage IPSec

The IPSec menu that contains IPSec management functions. To access this menu, use the I (IPSec) option .

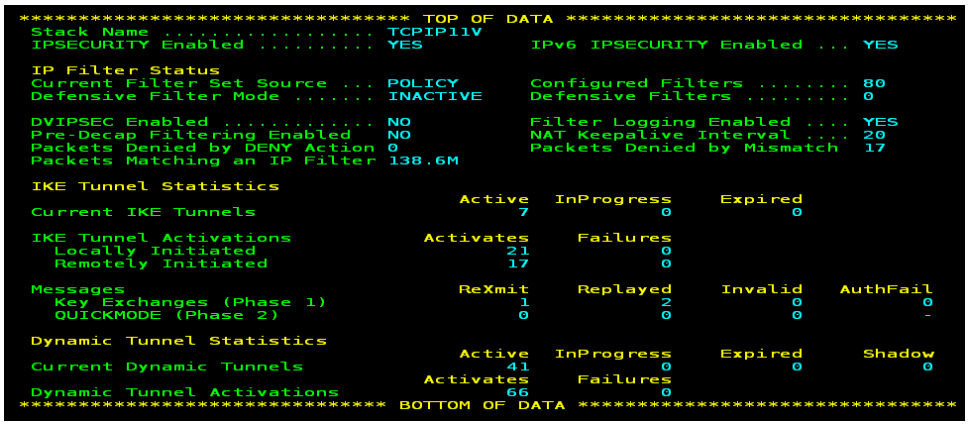
The following tools are available to help you manage IPSec in IBM's Communications Server:

- Reactive management tools provide a set of diagnostic displays, including concise selection lists of filters and tunnels. These displays make it easy to check the configuration and status of filters and tunnels.
- Proactive management tools enable the monitoring of IPSec status at the stack level, which provides the basis for alerting on problem scenarios such as tunnel activation failures and failed key exchanges.

Some of these tools require you to have authority to use the ipsec z/OS UNIX command.

## IPSec Summary Example

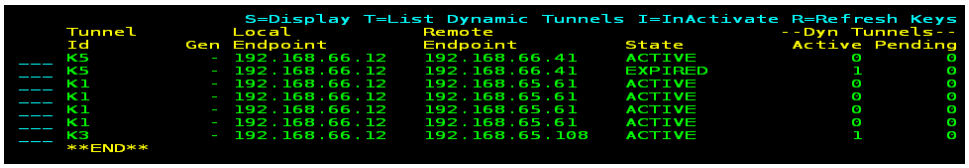
To display information about IPSec, including IP filter status and tunnel statistics, select the S (IPSec Summary) option on the IPSec menu.



## Tunnel Example

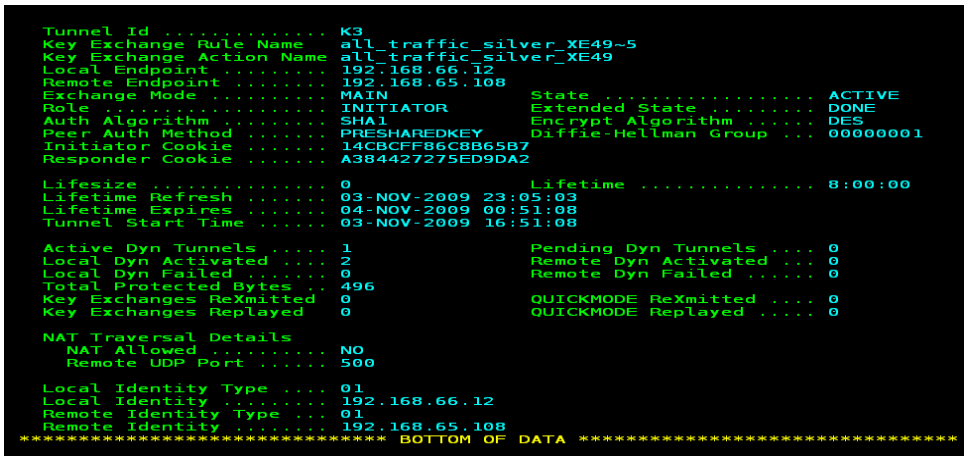
To view the details of the different types of tunnels, use the Tunnels options on the IPSec menu.

From the IPSec menu, select the K (List IKE Tunnels) option to list the tunnels for a specified stack.



```
                  S=Display T=List Dynamic Tunnels I=InActivate R=Refresh Keys
     Tunnel       Local          Remote                        --Dyn Tunnels--
     Id       Gen Endpoint       Endpoint         State         Active Pending
___  K5         - 192.168.66.12  192.168.66.41    ACTIVE             0       0
___  K5         - 192.168.66.12  192.168.66.41    EXPIRED            1       0
___  K1         - 192.168.66.12  192.168.65.61    ACTIVE             0       0
___  K1         - 192.168.66.12  192.168.65.61    ACTIVE             0       0
___  K1         - 192.168.66.12  192.168.65.61    ACTIVE             0       0
___  K1         - 192.168.66.12  192.168.65.61    ACTIVE             0       0
___  K3         - 192.168.66.12  192.168.65.108   ACTIVE             1       0
___  **END**
```

From the list, you can perform various functions such as displaying the details of a tunnel, deactivating a tunnel, or refreshing the cryptographic keys for a tunnel. This example shows the details of an IKE tunnel.



```
  Tunnel Id ..............  K3
  Key Exchange Rule Name     all_traffic_silver_XE49~5
  Key Exchange Action Name   all_traffic_silver_XE49
  Local Endpoint .........   192.168.66.12
  Remote Endpoint ........   192.168.65.108
  Exchange Mode ..........   MAIN                 State ................... ACTIVE
  Role ...................   INITIATOR            Extended State ......... DONE
  Auth Algorithm .........   SHA1                 Encrypt Algorithm ...... DES
  Peer Auth Method .......   PRESHAREDKEY         Diffie-Hellman Group ... 00000001
  Initiator Cookie .......   14CBCFF86C8B65B7
  Responder Cookie .......   A384427275ED9DA2

  Lifesize ...............   0                    Lifetime ............... 8:00:00
  Lifetime Refresh .......   03-NOV-2009 23:05:03
  Lifetime Expires .......   04-NOV-2009 00:51:08
  Tunnel Start Time ......   03-NOV-2009 16:51:08

  Active Dyn Tunnels .....   1                    Pending Dyn Tunnels .... 0
  Local Dyn Activated ....   2                    Remote Dyn Activated ... 0
  Local Dyn Failed .......   0                    Remote Dyn Failed ...... 0
  Total Protected Bytes ..   496
  Key Exchanges ReXmitted    0                    QUICKMODE ReXmitted .... 0
  Key Exchanges Replayed     0                    QUICKMODE Replayed ..... 0

  NAT Traversal Details
    NAT Allowed ..........   NO
    Remote UDP Port ......   500

  Local Identity Type ....   01
  Local Identity .........   192.168.66.12
  Remote Identity Type ...   01
  Remote Identity ........   192.168.65.108
********************************* BOTTOM OF DATA ********************************
```

# How You Use IP Security Monitoring Attributes

A STACK resource provides IP Security Monitoring attributes. You can use these attributes to collect statistical information. You can set alerts to warn you of abnormal attribute values.

The following process shows you how to implement IP Security Monitoring:

1. Activate IP Security Monitoring:
   a. Enter **/IPMON** and then **UM** next to a STACK resource on the current system.
   b. Use the A (Activate) action to activate IP Security Monitoring.
2. Set attribute alerts. Set alerts for the IP Security Monitoring attributes as required. The attributes have the following prefixes:
   - DynTunnel
   - IKEKeyMsg
   - IKETunnel
   - IPFiltPkts

   For example, IKEKeyMsgFailedAuth monitors the number of key exchange (phase 1) message authentication failures for the stack during IKE Phase 1 negotiations. You can set an alert to warn you if the number exceeds a specified threshold.

# Chapter 10: Understanding Historical Network Performance

This section contains the following topics:



## How You Use Historical Performance for Planning

CA NetMaster NM for TCP/IP stores collected data that can help you plan your network for the future. The following facilities are available:

- WebCenter IP Growth Tracker helps you plan for future growth.
- ReportCenter produces reports that help you understand the historical performance of the network.
- IP History helps you analyze past events.

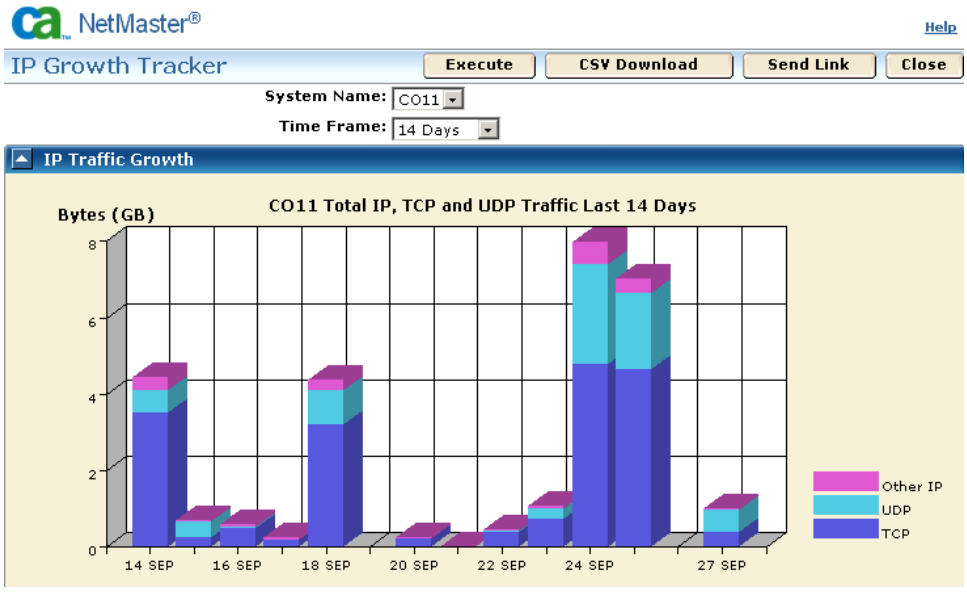
## WebCenter IP Growth Tracker

The IP Growth Tracker uses column charts to show the growth in IP traffic on a system over a period. The page also shows the distribution of TCP connections by the time over which the connections are active.

You access the IP Growth Tracker page from the WebCenter login dialog (if enabled by the WEBCENTER parameter group) or from Performance Center after you log in.

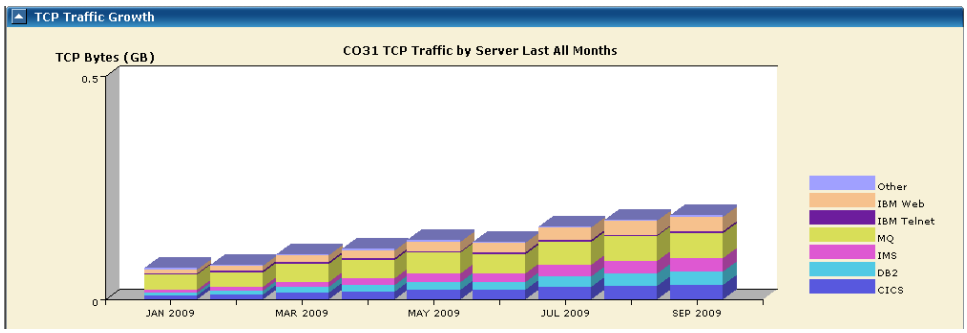
### Example: IP Traffic Growth

This example shows the IP traffic growth on the CO11 system over the last 14 days:




### Example: TCP Traffic Growth

This example shows the TCP traffic growth by the type of server on the CO31 system over the months that have data:



# ReportCenter

ReportCenter is an optional, separately implemented component that stores network performance data collected by multiple regions in a mainframe SQL database. You can then use WebCenter to generate web-based graphical historical and trend reports from this data.

ReportCenter provides a variety of predefined reports. Reports are provided for the following resources:

- Stack workload (comprising FTP, Telnet, and business application traffic)
- Stack IP, TCP, and UDP activity
- Stack network interface device links
- Virtual IP Addresses (VIPAs)
- Open System Adapters (OSAs)
- CISCO interface processors
- Enterprise Extender (EE)
- Communication storage management
- Address space and ports
- Generic SNMP MIB attributes
- File transfer

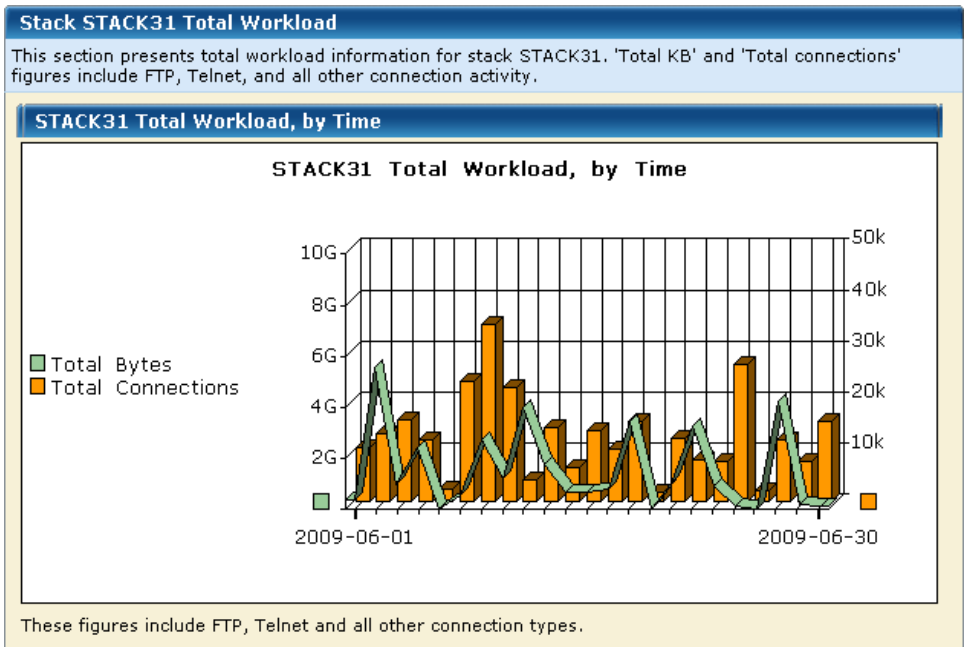
The Report Examples is a collection of pre-generated ReportCenter reports.

### Example: Stack Workload Analysis Report

The Stack Workload Analysis report contains the following information:

- Total workload
- Concurrent active connections
- Workload and business applications
- FTP workload
- Telnet workload

This example shows the total workload on a stack over one month.



# IP History

Each region has an events database. The database stores information about connection, FTP, Telnet, and Cisco channel card events on the system. You can search this database for specific events, and produce online and printed historical reports.

The data provides input to network trend analysis and an audit trail of network activity that can be used in future network planning. You can extract the data for analysis by exporting it to other data analysis and reporting tools such as Microsoft Excel.

To access the IP History functions, enter the /IPHIST shortcut. You can also access these functions from WebCenter, History, IP Events, which enables you to download the search results in comma-separated value (CSV) format.

# Chapter 11: Quick Tours

This section contains the following topics:



## Overview

The quick tours take you through some of the features of CA NetMaster NM for TCP/IP. You can access these features using either the 3270 interface or the WebCenter interface.

You can use the quick tours to gain experience with the following activities:

- Viewing the available monitors
- Listing the IP resources defined to your region
- Listing the stacks defined to your system
- Obtaining a list of IP connections
- Producing a graph of the number of IP packets delivered by a stack
- Using WebCenter to display diagnostic and performance information and to monitor resources

## 3270 Tours

These tours familiarize you with the 3270 interface.

## Access Monitors

The following monitors are available to you with CA NetMaster NM for TCP/IP:

**IP Summary Display**

Displays a status-at-a-glance of your IP network traffic. Data on this display is sourced from the Packet Analyzer and is in real time. The Summary Display is optionally displayed on the bottom part of your Primary Menu.

**IP Resource Monitor**

Displays your IP resources (as discovered by Express Setup). Use the resource monitor to view performance history and diagnostic information about your resources.

**IP Node Monitor**

Displays your IP nodes (as discovered by Express Setup). Use the IP node monitor to display ping RTT average, and view performance history and diagnostic information about your IP nodes.

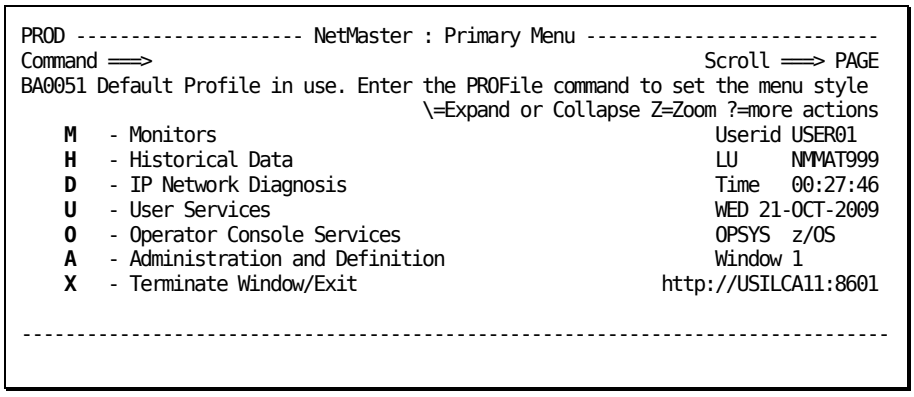
**Alert Monitor**

Displays alerts when a defined event is triggered or a defined threshold is exceeded.

**To access the monitors available with your product**

1. Access your NetMaster : Primary Menu.

   Your user profile determines whether the IP Summary Display is displayed below the following menu items:




2. Enter **M** (Monitors).

   The Monitors : Primary Menu appears.

   **Note:** To access an option from anywhere in your product, use the shortcuts listed to the right of the Monitors : Primary Menu. For example, to display the IP Resource Monitor, enter **/IPMON** at the prompt on any panel.

3. Enter **I** (IP Resource Monitor).

   The IP Resource Monitor panel appears.

```
PROD----------------------- IP Resource Monitor --------------------CO11-0001
Command ===>                                                 Scroll ===> CSR

    S=Info H=Performance History OV=Performance Overview AL=Alerts ?=List Cmds
                                          Monitor Alert Max Last  Next
   Resource        Class   System   Actual  Status  Count Sev Samp  Samp  Ovr
   TCPIP01         STACK   CO11     ACTIVE  Ok      0     -   10:16 10:31
   SNSWILMA        STACK   CO11     DEGRADED Error  0     -   10:21 10:31
   OSA-01          OSA     CO11     ACTIVE  Ok      3     2   10:16 10:31
   OSA-02          OSA     CO11     ACTIVE  Ok      0     -   10:16 10:31
   NMDCIP2         CIP     CO11     ACTIVE  Ok      0     -   10:21 10:31
   EE              EE      CO11     ACTIVE  Ok      0     -   10:16 10:31
   172.24.171.24   VIPA    CO11     ACTIVE  Ok      0     -   10:18 10:33
   CSM             CSM     CO11     ACTIVE  Ok      0     -   10:16 10:31
   BPXOINIT        ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16
   CCITCP          ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16
   CCITCPGW        ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16
   DFSKERN         ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16
   DYLMCICS        ASMON   CO11     INACTIVE -      0     -   10:16 11:16
   EDBC11          ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16
   FTPD111         ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16
   INETD7          ASMON   CO11     ACTIVE  Ok      0     -   10:16 11:16

 F1=Help      F2=Split     F3=Exit      F4=Add       F5=Find
 F7=Backward  F8=Forward   F9=Swap
```

**Note:** To enter a command against one of the listed resources, tab to the left side of the resource and type the command next to the resource name.

4. Enter **?** next to a STACK resource.

   A panel appears that lists all the commands available for this resource.

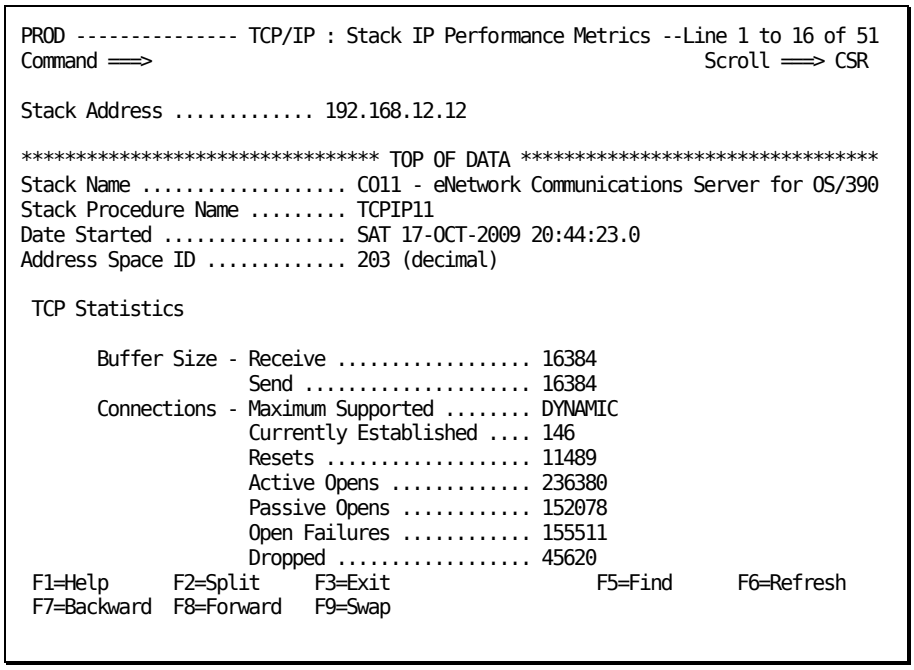
```
PROD------------------ Valid Line Commands for TCPIP01 -----------------------
Command ===>                                                 Scroll ===> PAGE

                                    S=Select Required Command  ?=Command Help
    Command       Description
    CMD           Issue Modify to Stack
    D             Display Address Space
    DL            Display Stack Network Interfaces
    DP            Display Profile Configuration Libraries
    DT            Graph TCP Connection Duration Times
    H             Display Performance History
    IC            List IP Connections
    ICF           List IP Connections (Advanced)
    IF            List FTP Connections
    IL            List TCP Listeners
    IP            Display IP, TCP, and UDP Performance
    IPM           Display IP, TCP, and UDP Summary
    IS            Display IPSec Performance History
    ISD           List Dynamic Tunnels (IPSec)
    ISF           List IP Filters (IPSec)
    ISK           List IKE Tunnels (IPSec)
    ISM           List Manual Tunnels (IPSec)
 F1=Help      F2=Split     F3=Exit      F4=FullList  F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap
```

   The commands that are specific to a resource appear in turquoise at the top of the list.

5. Type **S** next to the IPM command.

   The Stack IP Performance Metrics panel appears. This panel displays a current analysis of the stack.

   **Note:** On a CA TCPaccess CS stack, the display is slightly different.



```
PROD ---------------- TCP/IP : Stack IP Performance Metrics --Line 1 to 16 of 51
Command ===>                                                    Scroll ===> CSR

Stack Address ............. 192.168.12.12

********************************* TOP OF DATA ********************************
Stack Name ................... CO11 - eNetwork Communications Server for OS/390
Stack Procedure Name ......... TCPIP11
Date Started ................. SAT 17-OCT-2009 20:44:23.0
Address Space ID ............. 203 (decimal)

 TCP Statistics

       Buffer Size - Receive ................... 16384
                     Send ...................... 16384
       Connections - Maximum Supported ........ DYNAMIC
                     Currently Established .... 146
                     Resets .................... 11489
                     Active Opens .............. 236380
                     Passive Opens ............. 152078
                     Open Failures ............. 155511
                     Dropped ................... 45620
 F1=Help      F2=Split     F3=Exit                  F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap
```

6. Press F3 (Exit) to return to the monitor.

## View Performance Results

CA NetMaster NM for TCP/IP collects and records the following information:

- Performance information about the monitored resources such as stacks
- Workload statistics about your stack

Various commands display different types of performance.

The following procedure shows you how to view the results of stack IP performance monitoring.

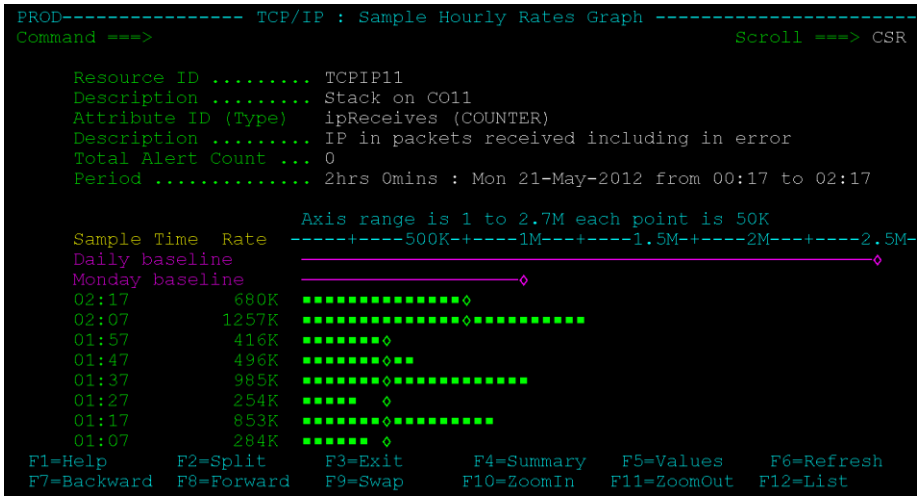
**Follow these steps:**

1. From the IP Resource Monitor, enter **IP** next to a STACK resource.

   The Stack IP, TCP and UDP History panel appears that displays the results of the stack IP performance monitoring.

2. From an expanded list, enter **D** next to an attribute.

   A detailed display of the values appears. The display shows the values for up to the last 12 samples.




   **Note:** To display a summary of performance history over the last day, enter **S** next to the attribute on the Stack IP, TCP and UDP History panel. You can also press F4 (Summary) on the Sample Hourly Rates Graph panel. Summary data is available only after an hourly summary occurs, which requires a sample for that particular attribute at the beginning of the hour.

3. Press F3 (Exit).

   You return to the performance display.

4. Enter **==** at the command prompt.

   You return to the Primary Menu.

## Diagnose Network Problems

Although the IP resource and node monitors have display commands to help you diagnose problems, additional diagnostic functions are available from the Network Diagnosis : Primary Menu.

**To access diagnostic functions**

1. From the NetMaster : Primary Menu, enter **D** (IP Network Diagnosis).

   The Network Diagnosis : Primary Menu appears.

2. Select **C** (Connections (IP, Telnet)).

   The Connections panel appears.

3. Select **CF** (List Connections (Advanced)).

   The Connection List Criteria panel appears.

4. Press F6 (Action).

   The Connections (Advanced) panel appears. This panel lists active connections. You can press F11 to display columns to the right.

```
PROD-------------- TCP/IP : Connections (Advanced) -----------Stack: *MULTIPLE*
Command ===>                                                  Scroll ===> PAGE

    Line 35 of 315                          Refresh Every ...      Seconds
           S=View I=Information CS=Statistics PT=Packet Trace Z=Drop ?=Actions
    Foreign                 Local                   LU
    Host              Port  Host              LPort Name     User ID  TaskName
    172.24.122.116    2865  172.24.172.8       1023 T01V0069 USER01   TCPIP01
    172.24.3.10      50004  172.24.172.8       1041 -        -        -
    172.24.206.195    2049  172.24.172.8       1079 -        -        MVSNFSC
    172.24.206.195    2049  172.24.172.8       1096 -        -        MVSNFSC
    172.24.206.195    2049  172.24.172.8       1179 -        -        MVSNFSC
    172.24.151.147    1382  172.24.172.8       1202 -        -        CCITCP
    172.24.151.147    1393  172.24.172.8       1202 -        -        CCITCP
    172.24.151.147    1385  172.24.172.8       1202 -        -        CCITCP
    172.24.151.162    1369  172.24.172.8       1202 -        -        CCITCP
    172.24.66.4       7005  172.24.172.8       3202 -        -        CCITCPG2
    172.24.66.61      7005  172.24.172.8       3203 -        -        CCITCPG2
    172.24.80.194    65535  172.24.172.8       3396 -        -        PROD
    172.24.80.194    65535  172.24.172.8       3397 -        -        PROD
    172.24.66.11      7031  172.24.172.8       3398 -        -        PROD
    172.24.200.72     6664  172.24.172.8       3399 -        -        PROD
 F1=Help      F2=Split     F3=Exit                                   F6=Refresh
 F7=Backward  F8=Forward   F9=Swap                F11=Right    F12=Traces
```

From this panel, you can perform actions such as ping, traceroute and packet trace, or you can simply review the details of a connection.

**To display packet and byte statistics**

1. Enter **CS** (Statistics) next to a connection.

   The Connection Statistics panel appears.

```
PROD------------------- TCP/IP : Connection Statistics -----------------------
Command ===>                                                 Scroll ===> CSR


 Connection Details
   Local IP address:port ................. 172.24.17.12:1023
   Remote IP address:port ................ 172.24.172.123:2865
   Connection state ...................... ESTABLISHED
   Connection started .................... 21-OCT-2009 17:45:14
   Turn count ............................ 27

                                  Bytes      Bytes    Packets    Packets
 Statistics for last 5 minutes      In        Out         In        Out
                          20.44      0          0          0          0
                          20.43    156        304          2          2
                          20.42    116        304          1          2
                          20.41    156        304          2          2
                          20.40    156        304          2          2

                                  Bytes      Bytes    Packets    Packets
 Statistics for last hour           In        Out         In        Out
                          20.45    428        912          5          6
                          20.40    700       1520          8         10
                          20.35    660       1520          7         10
                          20.30    660       1520          7         10
                          20.25    620       1520          6         10
                          20.20    700       1520          8         10
                          20.15    660       1520          7         10
                          20.10    700       1520          8         10
                          20.05    660       1520          7         10
                          20.00    700       2036          8         11
                          19.55    900       4616         13         16
                          19.50    700       1520          8         10

                                  Bytes      Bytes    Packets    Packets
 Connection duration                In        Out         In        Out
   Total .....................     28150       111K       345        445
   Payload only ..............     14342      93531         -          -
```

This panel enables you to display packet and byte statistics for a specific IP connection. You can refresh this display (F6), or display basic information together with packet-specific data from both the local and remote perspective (F12).

**Statistics for last 5 minutes**

Shows byte and packet counts in 1-minute intervals for the last 5 minutes.

**Statistics for last hour**

Shows byte and packet counts in 5-minute intervals for the last hour.

**Connection duration**

Shows byte and packet counts since the connection was started.

2. Press F3 (Exit).

   You return to the Connections (Advanced) panel.

**To perform a packet trace**

1. Identify a connection that has packets flowing, that is, there is activity in the Bytes Out and Bytes In columns.
2. Enter **PT** (Activate Packet Trace) next to the connection, and wait for a few seconds to collect packets.

   The packets are traced for this connection.
3. Enter **PTV** (View Packet Trace) next to the connection.

   The most recent packets on the connection are listed.

```
PROD--------------------- SmartTrace : Packet List ----------------------------
Command ===>                                                  Scroll ===> CSR

                                                              S/V=View P=Print
   Stack ......... TCPIP01             Total Traced 44
   Local Host .... 172.24.151.162  <--> Foreign Host 172.24.172.8
   Local Port .... 1369                Foreign Port 1202
   Protocol ...... TCP

        Dir  +Time  Bytes  Summary Information
   0001  -> <0.001   1492  Ack     Win=65535 Seq=1412574111 Ack=2241384874
   0002  -> <0.001   1232  Ack Psh Win=65535 Seq=1412575563 Ack=2241384874
   0003  -> <0.001   1492  Ack     Win=65535 Seq=1412576755 Ack=2241384874
   0004  -> <0.001   1492  Ack     Win=65535 Seq=1412578207 Ack=2241384874
   0005  -> <0.001   1232  Ack Psh Win=65535 Seq=1412579659 Ack=2241384874
   0006  -> <0.001   1492  Ack     Win=65535 Seq=1412580851 Ack=2241384874
   0007  -> <0.001   1155  Ack Psh Win=65535 Seq=1412582303 Ack=2241384874
   0008 <-   0.044     40  Ack     Win=65535 Seq=2241384874 Ack=1412571467
   0009 <-  <0.001     40  Ack     Win=65535 Seq=2241384874 Ack=1412575563
   0010 <-  <0.001     40  Ack     Win=65535 Seq=2241384874 Ack=1412580851
   0011 <-   0.001     40  Ack     Win=65535 Seq=2241384874 Ack=1412583418
   0012 <-   0.037    516  Ack Psh Win=65535 Seq=2241384874 Ack=1412583418
   0013  ->  0.222     40  Ack Psh Win=65535 Seq=1412583418 Ack=2241385350
   0014 <-   1.930    516  Ack Psh Win=65535 Seq=2241385350 Ack=1412583418
 F1=Help      F2=Split     F3=Exit                 F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

4. Enter **S** next to a packet.

   The data for that packet appears.
5. Press F3 (Exit) twice.

   You return to the Connections (Advanced) panel.

6. Enter **PTD** (Inactivate and Delete Packet Trace) next to the connection being traced, and press Enter to confirm your action.

   The trace is stopped and deleted.

7. Press F3 (Exit) three times.

   You return to the Network Diagnosis : Primary Menu.

## Get Online Help

You can get online help from any panel in this product.

**To get online help for the current panel**

1. Press F1 (Help).

   The online help displays information about the fields and actions available on this panel.

2. Press F4 (Return).

   You exit from the online help.

# WebCenter Tours

These tours familiarize you with the WebCenter interface. WebCenter provides a web browser interface to most of the tasks available from the 3270 interface.

## Access WebCenter

Use this procedure to access the WebCenter interface.

**To access WebCenter**

1. Start your web browser, and enter the WebCenter web access uniform resource locator (URL).

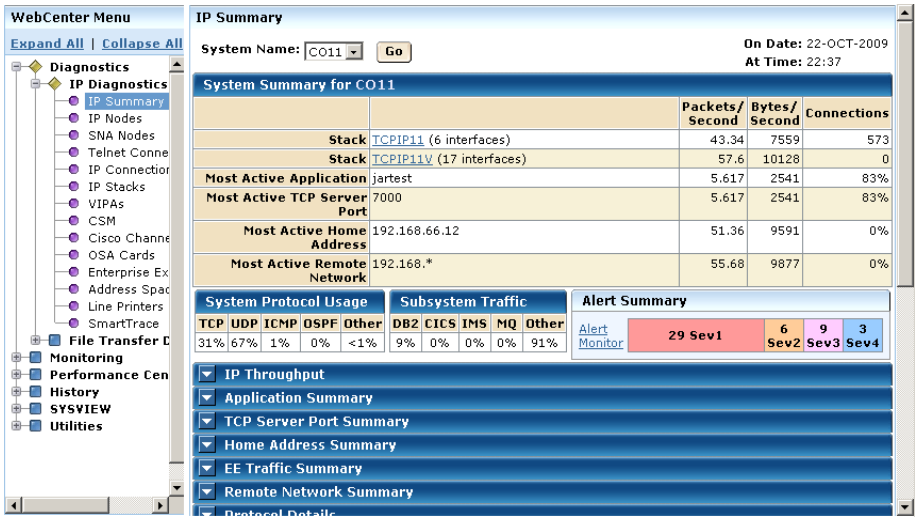
   **Note:** The WebCenter web access URL is defined when the product is installed. If you do not know the URL, ask your system administrator or refer to the NetMaster : Primary Menu.

   The WebCenter login page appears.

   **Note:** You can bookmark the WebCenter Access URL in your web browser. The bookmark lets you access WebCenter easily and quickly in the future.

2. Enter the same user ID and password that you use for your 3270 logon.

   The WebCenter home page appears.




   The left side of the WebCenter page contains the WebCenter menu, which you can use to access the WebCenter functions.

## Access Monitors

The monitoring options available with WebCenter are similar to the options available with the 3270 interface.

To view the monitoring options, click the Monitoring option from the WebCenter menu.

From this page, you can monitor the following:

- Alerts

- IP nodes
- IP resources

## View Performance Results

Use this procedure to view the performance history of a stack.

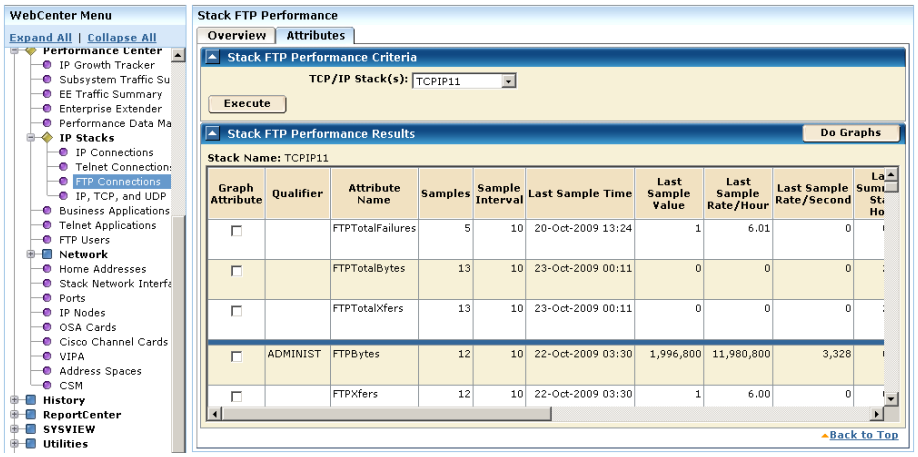
**To display performance information**

1. Click Performance Center, IP Stacks, FTP Connections.

   The Stack FTP Performance page appears.

2. Click the Attributes tab, select a TCP/IP stack from the drop-down list, and click Execute.

   The Stack FTP Performance Results appear.




3. Select the Graph Attribute check box for one of the attributes, and click Do Graphs.

   The page is refreshed, and detail and summary graphs of the selected attribute appears, showing the sampled values over time.

## Diagnose Network Problems

Use this procedure to review the connectivity of a specified host.

**To display diagnostics information**

1. Click Diagnostics, IP Nodes.

   The IP Node Diagnostics page appears.

2. Enter the IP address or name of a remote node, and click a tab to perform one of the diagnostic functions. For example, click Connections.

   Connections with the node are listed.

**To perform a packet trace**

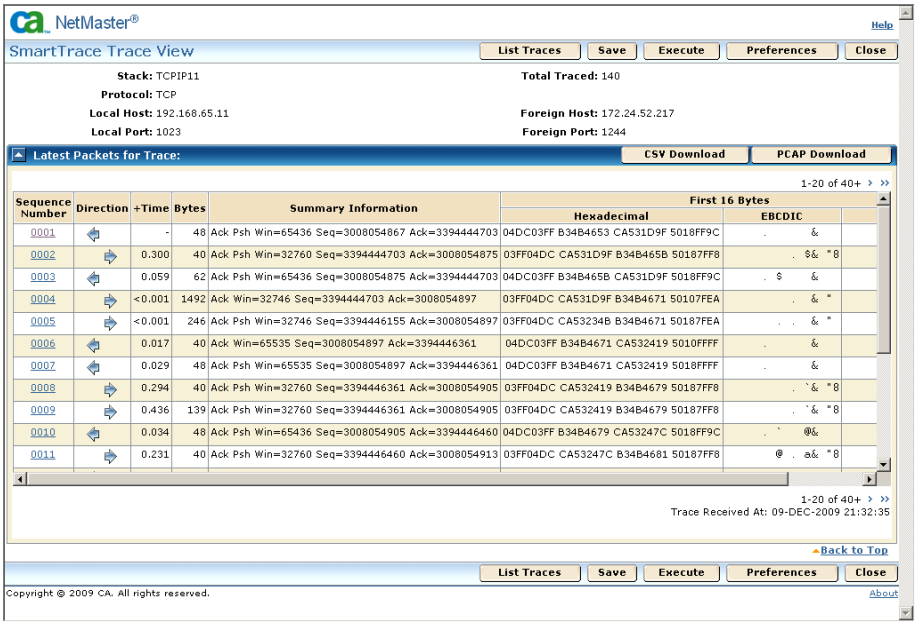
1. Identify a connection that has packets flowing, that is, there is activity in the Bytes Out and Bytes In columns.

2. Select the Activate Packet Trace action for the connection, click Go, confirm the action, and wait for a few seconds to collect packets.

   The packets are traced for this connection, as flagged in the Tracing column.

3. Select the View Packet Trace action, and click Go.

   The most recent packets in the connection are listed, for example:




4. Click the Sequence Number link of a packet.

   The date for that packet appears.

When you finish with the trace, return to the IP Diagnostics page, select Clear Packet Trace, and click Go to stop and delete the trace.

# Index

## P



## R



## S



## T



## U



## W