

# CA NetMaster® Network Management for TCP/IP

## User Guide

Release 12.1



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS (CA ACF2)
- CA CPT™ CICS Programmers' Toolkit for TCP/IP (CA CPT)
- 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 NetMaster® Socket Management for CICS (CA NetMaster SM for CICS)
- CA NetSpy™ Network Performance (CA NetSpy)
- CA SOLVE:Access™ Session Management (CA SOLVE:Access)
- CA SOLVE:Operations® Automation for CICS (CA SOLVE:Operations Automation for CICS)
- CA SYSVIEW® Performance Management (CA SYSVIEW)
- CA TCPaccess™ Communications Server (CA TCPaccess CS)
- CA Top Secret® for z/OS (CA Top Secret)

# 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](mailto: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 21

|  |    |
|--|----|
| System Services .....                    | 21 |
| Operator Console .....                   | 22 |
| Alert Monitor .....                      | 23 |
| Security .....                           | 23 |
| Broadcast Services .....                 | 23 |
| Print Management .....                   | 23 |
| Communications .....                     | 24 |
| Report Writer .....                      | 24 |
| Application Development .....            | 24 |
| Automation Services .....                | 25 |
| Knowledge Base .....                     | 26 |
| Status Monitor .....                     | 26 |
| Automation Services Processes .....      | 28 |
| Multisystem Support.....                 | 29 |
| Automation Services Administration ..... | 30 |
| IP Summary Display.....                  | 30 |
| Connections Management .....             | 31 |
| Packet Tracing .....                     | 32 |
| MIBinsight .....                         | 32 |
| Performance Monitoring.....              | 33 |
| Event History .....                      | 33 |
| WebCenter .....                          | 33 |
| ReportCenter.....                        | 34 |

## Chapter 2: Getting Started 35

|  |    |
|--|----|
| Log On .....                                       | 35 |
| If Region Initialization Is Still in Progress..... | 36 |
| If the System Image Is Still Being Loaded.....     | 36 |
| Log Off .....                                      | 36 |
| Your Password.....                                 | 37 |
| Change Your Password.....                          | 37 |
| Authority Levels .....                             | 38 |
| Access Functions .....                             | 38 |
| Select an Option.....                              | 38 |
| Specify a Shortcut .....                           | 38 |

---

|                                    |    |
|------------------------------------|----|
| Specify a Path .....               | 39 |
| Lists .....                        | 41 |
| Scrolling .....                    | 41 |
| Search for an Item .....           | 42 |
| Data Entry Panels .....            | 43 |
| UPDATE Mode .....                  | 43 |
| Enter Data .....                   | 43 |
| Validate and File Data .....       | 44 |
| Move Between Panels .....          | 44 |
| Online Help .....                  | 46 |
| Tip of the Day .....               | 47 |
| Help About a Panel .....           | 47 |
| Help About Fields on a Panel ..... | 47 |
| Help for a Message .....           | 48 |
| Work in Two Windows .....          | 48 |
| Split Screens .....                | 49 |
| Swap Screens .....                 | 49 |

## Chapter 3: Using the IP Summary Display 51

|  |    |
|--|----|
| IP Summary Display .....               | 51 |
| Access IP Summary Display .....        | 52 |
| Expand or Collapse a Summary .....     | 52 |
| Condition Summary .....                | 53 |
| Stack IP, TCP, and UDP Layers .....    | 54 |
| Stack Network Interfaces .....         | 54 |
| Ports .....                            | 54 |
| Enterprise Extender .....              | 55 |
| APPN/HPR .....                         | 55 |
| Diagnose a Problematic Condition ..... | 56 |
| IP Traffic Summary .....               | 57 |
| Change Display .....                   | 57 |
| IP Throughput .....                    | 58 |
| Applications .....                     | 59 |
| TCP Server Port .....                  | 60 |
| Home Address .....                     | 61 |
| Remote Network .....                   | 61 |
| IP Protocol .....                      | 63 |
| Subsystem .....                        | 63 |
| Summaries by Stacks .....              | 64 |
| EE Traffic Explorer .....              | 64 |
| Bytes by VIPA .....                    | 65 |

---

|                               |    |
|-------------------------------|----|
| Bytes by EE Connection .....  | 66 |
| Bytes by EE Port .....        | 66 |
| Bytes by Protocol Layer ..... | 67 |
| Bytes by Payload .....        | 68 |
| Bytes by Direction .....      | 68 |
| Packets by Type .....         | 69 |
| Packet Indicators .....       | 70 |
| Alert Summary .....           | 71 |

## Chapter 4: Managing Connections 73

|  |    |
|--|----|
| Connection Lists .....   | 73 |
| Telnet Connection List .....                                       | 74 |
| FTP Connection List .....  | 74 |
| CICS Socket Connection List .....                                  | 75 |
| General Connection List .....                                      | 75 |
| Listener List .....  | 75 |
| Which List Connections Option Should I Use? .....                  | 76 |
| List Connections .....   | 76 |
| Store Criteria .....   | 77 |
| Recall Criteria .....  | 77 |
| Sort Connection Lists .....  | 78 |
| Locate Information on Sorted Connection Lists .....                | 78 |
| List Specific Connections .....                                    | 79 |
| Find an LU Name .....  | 79 |
| Find an IP Address .....   | 80 |
| Display Connections Graphically .....                              | 80 |
| Display Connection Statistics .....                                | 81 |
| Connections for Multiple Systems .....                             | 81 |
| Display Connections for Multiple Systems .....                     | 82 |
| Display Connection Information .....                               | 83 |
| Display AT-TLS Information .....                                   | 84 |
| Check for SNA Related Problems on Telnet Connections .....         | 84 |
| Check the VTAM Status of an LU .....                               | 84 |
| Analyze SNA Sessions .....   | 85 |
| Look Up a Device Name .....  | 85 |
| Drop a Connection .....  | 86 |
| Diagnose Data- and Protocol-Related Problems in a Connection ..... | 86 |
| Diagnose Telnet Response Time Problems .....                       | 87 |
| View End-to-End Response Times .....                               | 87 |
| Diagnose Throughput of Data Transfers .....                        | 88 |
| View End-to-End Throughput .....                                   | 88 |

---

## **Chapter 5: Managing Alerts** **89**

|  |    |
|--|----|
| Alerts .....   | 89 |
| Alert Monitor .....  | 90 |
| Access the Alert Monitor.....                                      | 90 |
| Sort Alerts.....   | 91 |
| Filter Alerts .....  | 91 |
| Change the Display Format .....                                    | 91 |
| Change the Alert Monitor Profile Using the User Profile Menu ..... | 92 |
| How to Work with Alerts.....                                       | 92 |
| Display Alert Details .....  | 93 |
| Print Alert Details .....  | 93 |
| Access the Transient Log from the Alert Monitor .....              | 93 |
| Raise a Trouble Ticket for an Alert .....                          | 94 |
| Add Operator Notes to an Alert .....                               | 94 |
| Close Alerts.....  | 95 |
| Display Alert History .....  | 95 |

## **Chapter 6: Managing IP Nodes** **97**

|  |     |
|--|-----|
| IP Node Monitor.....                                 | 97  |
| Access the IP Node Monitor .....                     | 98  |
| Interpret the Status of IP Nodes.....                | 98  |
| Use IP Node Commands .....                           | 99  |
| Packet Tracing .....                                 | 99  |
| Intensive Monitoring.....                            | 100 |
| Apply Intensive Monitoring Mode to an IP Node .....  | 100 |
| Reset Intensive Monitoring Mode for an IP Node ..... | 100 |
| Performance History .....                            | 101 |
| MIBinsight Browser .....                             | 101 |

## **Chapter 7: Managing IP Resources** **103**

|   |     |
|---|-----|
| Features That Help You Manage Your IP Resources ..... | 103 |
| IP Resource Monitor.....                              | 106 |
| Access the IP Resource Monitor .....                  | 107 |
| Interpret the Status of IP Resources .....            | 107 |
| Use IP Resource Commands.....                         | 108 |
| Add a Resource.....                                   | 108 |
| Packet Tracing .....                                  | 108 |
| Performance History .....                             | 108 |



---

## Chapter 8: Managing Stacks 111

|   |     |
|---|-----|
| TCP/IP Stack Support .....                          | 111 |
| Display TCP/IP Stacks .....                         | 111 |
| Packet Tracing .....                                | 112 |
| Display Stack Performance .....                     | 112 |
| Display Performance History .....                   | 113 |
| Display IP, TCP, and UDP Activity Summary .....     | 114 |
| Display IP Traffic Statistics .....                 | 114 |
| Issue Console Commands .....                        | 115 |
| Display Device Links .....                          | 115 |
| Device Links Graphic Display .....                  | 115 |
| Display Device Links Graphically .....              | 117 |
| Display Device Links Information .....              | 118 |
| CA TCPAccess CS Parameters Library .....            | 118 |
| Browse the CA TCPAccess CS Parameters Library ..... | 118 |
| Browse a PARMS Member .....                         | 119 |
| Change a PARMS Member .....                         | 119 |
| IBM Configuration Data Sets .....                   | 120 |
| Edit Data Sets .....                                | 120 |
| Update a Data Set .....                             | 121 |
| Change Configuration Using Obeyfile Data Sets ..... | 121 |
| Execute an Obeyfile Data Set .....                  | 122 |
| Check Your Obeyfile Results .....                   | 122 |
| Create a New Member of an Obeyfile Data Set .....   | 123 |
| Display Workload Manager Status .....               | 123 |
| Display the WLM Status of IBM TCP/IP Stacks .....   | 123 |
| Display the WLM Status of Telnet Servers .....      | 124 |
| Display Telnet Cluster List .....                   | 124 |
| List Remote Addresses .....                         | 124 |
| Display Address Space Activities .....              | 125 |

## Chapter 9: Managing Open Systems Adapters 127

|  |     |
|--|-----|
| Open Systems Adapters .....                            | 127 |
| Monitor OSAs .....                                     | 128 |
| Display OSA Utilization .....                          | 128 |
| Display OSA-2 Utilization .....                        | 128 |
| Display OSA Express or DirectExpress Utilization ..... | 128 |
| Display OSA Performance History .....                  | 129 |
| List OSA Devices .....                                 | 130 |
| Display OSA Configuration .....                        | 131 |
| Display the OSA Address Table .....                    | 131 |

---

## Chapter 10: Managing Cisco Channel Cards 133

|   |     |
|---|-----|
| Cisco Channel Cards .....                           | 134 |
| Channel Card Status .....                           | 134 |
| Monitor and Diagnose Channel Cards.....             | 135 |
| Display Channel Card Information .....              | 135 |
| Display Application Information .....               | 136 |
| Display Channel Card Performance History .....      | 137 |
| Diagnose Telnet Connection Problems .....           | 138 |
| Display a Telnet LU Mini Trace.....                 | 138 |
| Start a Telnet Connection to the Router .....       | 138 |
| Display Channel Information .....                   | 138 |
| Display TN3270 Server Information .....             | 139 |
| List PUs for a Server .....                         | 139 |
| List LUs for a PU .....                             | 140 |
| Display the TN3270 Server Log .....                 | 140 |
| Display CLAW Information .....                      | 141 |
| Display CLAW Subchannel Information.....            | 141 |
| Sort Entries on the Cisco CLAW Subchannel List..... | 142 |
| Display TCP Offload Information .....               | 142 |
| Display CSNA Information .....                      | 142 |
| Display Internal LAN Information .....              | 143 |
| Display Internal LAN Adapters .....                 | 143 |

## Chapter 11: Managing Enterprise Extender 145

|  |     |
|--|-----|
| Enterprise Extender.....                               | 145 |
| Monitor and Diagnose Enterprise Extender .....         | 146 |
| Check EE Connectivity .....                            | 146 |
| Display EE UDP Connections .....                       | 147 |
| Display UDP Port Activity .....                        | 147 |
| Display RTP Pipes .....                                | 147 |
| Display EE Traffic Statistics by CP .....              | 148 |
| Display EE Traffic Statistics by CP and Priority ..... | 148 |
| Run EE VTAM Commands.....                              | 148 |
| Detect RTP Pipe in Red Status .....                    | 149 |
| Check EE RTP Health.....                               | 149 |
| Check Transmission Group PU RTP Health .....           | 150 |
| Define EE RTP Health Thresholds .....                  | 150 |
| Packet Tracing .....                                   | 151 |
| SmartTrace with EE .....                               | 151 |
| Display Enterprise Extender Performance History .....  | 154 |
| Display XCA Major Node .....                           | 155 |

---

|                                   |     |
|-----------------------------------|-----|
| Display EE Traffic Analysis ..... | 156 |
| EE Traffic Analysis.....          | 156 |

## **Chapter 12: Managing APPN/HPR Resources 157**

|   |     |
|---|-----|
| APPN/HPR .....                                    | 157 |
| Monitor and Diagnose APPN/HPR Resources .....     | 158 |
| Display APPN/HPR Performance History .....        | 159 |
| Display Transport Resources List Entries.....     | 160 |
| Display RTP Pipes .....                           | 160 |
| Display Dependent LU Requestors.....              | 160 |
| Display CP-CP Sessions .....                      | 161 |
| Test APPN Connectivity .....                      | 161 |
| Display APPN Directory Information .....          | 162 |
| Display APPN Subnetwork Topology Information..... | 162 |
| Check RTP Health .....                            | 163 |
| Check RTP Health on a Local System.....           | 163 |
| Check RTP Health on a Multisystem .....           | 163 |
| Define RTP Health Thresholds.....                 | 164 |
| Run RTP VTAM Commands .....                       | 165 |

## **Chapter 13: Managing VIPA Resources 167**

|  |     |
|--|-----|
| Virtual IP Addresses (VIPAs) .....       | 167 |
| VIPA Resource Names .....                | 168 |
| Monitor and Diagnose VIPAs.....          | 168 |
| Display VIPA Details.....                | 169 |
| Display VIPA Performance History .....   | 170 |
| List IP Connections to a VIPA.....       | 170 |
| List Telnet Connections to a VIPA .....  | 170 |
| Check the Connection Routing Table ..... | 171 |
| Modify VIPA Definitions .....            | 171 |

## **Chapter 14: Managing Address Spaces 173**

|  |     |
|--|-----|
| Monitor Your Address Spaces .....              | 173 |
| External Telnet Servers .....                  | 174 |
| Check Telnet LUs .....                         | 175 |
| Packet Tracing .....                           | 175 |
| Display Address Space Performance History..... | 176 |
| Display Address Space IP Traffic.....          | 177 |
| DB2 Network Information Center .....           | 177 |

---

## **Chapter 15: Managing CSM Resources** **179**

|                                       |     |
|---------------------------------------|-----|
| CSM Resources .....                   | 179 |
| Display CSM Usage .....               | 179 |
| Display CSM Performance History ..... | 180 |

## **Chapter 16: Managing CICS Resources** **181**

|  |     |
|--|-----|
| Diagnose Your CICS Resources .....                               | 181 |
| List CICS Connections from a Socket Management Perspective ..... | 181 |
| Display Information About a CICMON Resource .....                | 182 |
| Stop and Restart CA NetMaster SM for CICS and CA CPT .....       | 182 |
| Stop and Restart the Command Server Interface .....              | 182 |
| Start a CICS Server .....  | 183 |
| Start CICS Transactions .....                                    | 183 |
| Monitor CICS Resource Performance .....                          | 184 |
| Monitor CICS IP Traffic .....                                    | 184 |

## **Chapter 17: Managing IP Security** **185**

|   |     |
|---|-----|
| IP Network Security Center .....          | 185 |
| IPSec Management .....                    | 185 |
| How You Access Management Functions ..... | 186 |
| Limitations .....                         | 186 |

## **Chapter 18: Diagnosing IP Networks** **187**

|  |     |
|--|-----|
| Access Network Diagnosis Functions .....                             | 187 |
| How to Trace a TCP/IP Route .....                                    | 187 |
| Perform a Traceroute From the Network Diagnosis Functions Menu ..... | 188 |
| Use Traceroute Action .....  | 188 |
| Browse MIBs .....  | 190 |
| Browse System Information .....                                      | 190 |
| Browse Host Interfaces .....   | 191 |
| Display a Routing Table .....  | 191 |
| Actions on the Routing Table .....                                   | 192 |
| Test Connectivity .....  | 193 |
| Perform a Ping .....   | 193 |
| Interpret Responses to a Ping .....                                  | 194 |

## **Chapter 19: Using SmartTrace** **195**

|                        |     |
|------------------------|-----|
| SmartTrace .....       | 196 |
| SmartTrace Modes ..... | 196 |

---

|   |     |
|---|-----|
| SmartTrace Line Command Mode.....                         | 197 |
| SmartTrace OCS Mode .....                                 | 198 |
| Schedule Tracing from OCS .....                           | 199 |
| SmartTrace Menu Mode .....                                | 200 |
| Access Packet Tracing Menu .....                          | 200 |
| Definition Types .....                                    | 201 |
| Selection Criteria.....                                   | 202 |
| Add a SmartTrace Definition .....                         | 204 |
| Copy a SmartTrace Definition .....                        | 205 |
| Activate a SmartTrace Definition .....                    | 205 |
| Stop a SmartTrace Definition .....                        | 206 |
| Delete a SmartTrace Definition .....                      | 206 |
| List SmartTrace Definitions .....                         | 207 |
| List Active SmartTrace Definitions .....                  | 207 |
| View a Trace .....  | 208 |
| View a Trace from a Resource or a Connection .....        | 210 |
| View a Trace from the Packet Tracing Menu .....           | 211 |
| Locate Packet Data.....                                   | 212 |
| Decode Packet Data for Specific Protocols and Ports ..... | 213 |
| Hide Decoded Information from the Packet List.....        | 218 |
| View Packet Data .....                                    | 219 |
| Print Packet Data.....                                    | 225 |
| Save a Trace.....   | 226 |
| Export a Trace .....                                      | 226 |
| Import a Trace .....                                      | 228 |
| Print a Trace .....                                       | 228 |
| Generate Trace Reports .....                              | 229 |

## Chapter 20: Using CTRACE 231

|  |     |
|--|-----|
| CTRACE .....                               | 231 |
| Display CTRACE Packet Tracing Menu .....   | 231 |
| How to Perform a Trace and Save Data ..... | 232 |
| Start a Trace .....                        | 232 |
| List Active Traces.....                    | 233 |
| Stop a Trace.....                          | 233 |
| Save CTRACE Data .....                     | 234 |
| View the Saved Packet Trace .....          | 234 |
| List IP Addresses in a Trace .....         | 234 |
| List Saved Traces .....                    | 237 |
| List Connections in a Trace.....           | 238 |
| List Packets in a Selected Trace.....      | 240 |

---

|                                       |     |
|---------------------------------------|-----|
| View Data for a Selected Packet ..... | 240 |
| Print Formatted Packet Details .....  | 241 |
| Errors in Packets.....                | 241 |
| View Packets in Error .....           | 242 |
| Deal with Errors in Packets .....     | 242 |
| Export a Trace .....                  | 243 |

## Chapter 21: Using Telnet 245

|  |     |
|--|-----|
| Use Telnet to Connect to Remote Hosts .....                      | 245 |
| Connect in Full Screen Mode .....                                | 245 |
| Connect in OCS Takeover Mode or Line Mode .....                  | 246 |
| Start Telnet Connections.....                                    | 246 |
| Other Methods of Starting Full-Screen Telnet Connections .....   | 246 |
| Telnet Display.....  | 247 |
| Telnet Function Key Assignments .....                            | 247 |
| Edit Text on the Telnet Display .....                            | 248 |
| Manage Your Telnet Connection.....                               | 249 |
| Search Data on the Telnet Display .....                          | 249 |
| Print from the Telnet Display .....                              | 250 |
| Set Your Telnet Options .....                                    | 251 |
| Issue Telnet Commands .....                                      | 252 |
| Clear the Buffer .....   | 252 |
| Hide or Display the Function Key Assignments .....               | 253 |
| Display Telnet Connection Details .....                          | 253 |
| End Your Telnet Connection .....                                 | 253 |
| Use Line Commands to Connect to a Remote Host .....              | 254 |
| TELNET Command: Start a Telnet Connection .....                  | 254 |
| Use Telnet in OCS Takeover Mode.....                             | 255 |
| Use Telnet in Line Mode .....                                    | 256 |
| Automate Commands Issued to Remote Hosts .....                   | 257 |
| End a Telnet Connection in Line Mode or OCS Take-over Mode ..... | 257 |
| Send Control Codes or Special Characters to the Remote Host..... | 258 |
| Using the ---more--- Prompt .....                                | 258 |

## Chapter 22: Diagnosing Line Printers 259

|   |     |
|---|-----|
| Line Printer Diagnostics Panel .....        | 259 |
| Access Line Printer Diagnostics Panel ..... | 260 |
| Query Printer Status.....                   | 260 |
| Delete an Entry in the Print Queue .....    | 261 |
| Send a Test Print .....                     | 261 |

---

## Chapter 23: Using MIBinsight 263

|   |     |
|---|-----|
| MIBinsight .....  | 263 |
| MIBinsight Browser .....                                | 264 |
| Access MIBinsight Browser .....                         | 264 |
| SNMP Tree.....  | 265 |
| Display SNMP Tree in Flat Mode.....                     | 266 |
| Display SNMP Tree in Explore Mode.....                  | 266 |
| Expand and Collapse the Tree .....                      | 266 |
| Add MIB Definition .....                                | 267 |
| Delete MIB Definition.....                              | 267 |
| Sort MIB Objects .....                                  | 268 |
| Display the Value of a Selected MIB Object .....        | 269 |
| Display the Values of the Next n MIB Objects.....       | 270 |
| Skip a Table or Group .....                             | 270 |
| Walk the MIB.....                                       | 270 |
| Browse the Value of MIB Objects.....                    | 270 |
| View the Full Definition of a MIB Object.....           | 271 |
| View an Enumerated MIB Object.....                      | 271 |
| View an Indexed MIB Object.....                         | 271 |
| Display the Object Values of a Selected MIB Table ..... | 271 |
| Update the Value of MIB Objects.....                    | 272 |
| Reformat Octet String Object Values .....               | 272 |
| Delete Objects from the MIBinsight Browser .....        | 273 |
| Add an OID .....  | 273 |
| Get First OID .....                                     | 273 |
| Print MIB .....   | 274 |
| Maintain Your User Security Details for MIBinsight..... | 274 |

## Chapter 24: Performance History 275

|  |     |
|--|-----|
| Performance Data .....   | 275 |
| Performance Displays.....  | 276 |
| Attribute List Format on History Panels .....                        | 277 |
| Performance Graphs .....   | 278 |
| Attribute Types .....  | 278 |
| Baselines.....   | 279 |
| How to Access Performance Displays .....                             | 280 |
| Display Performance History from the IP Resource Monitor.....        | 280 |
| Display Performance History from the IP Node Monitor .....           | 281 |
| Display Performance History from Resource Management Menus .....     | 281 |
| Display Performance History from the Performance Overviews Menu..... | 282 |
| How to Access Performance Graphs .....                               | 283 |

---

|  |     |
|--|-----|
| Display Sample Values Graph.....   | 284 |
| Display Sample Hourly Rates Graph.....                                   | 285 |
| Display Hourly Summary Graph .....                                       | 286 |
| How to Access Baselines .....  | 286 |
| Display Current Baselines and Differences for Monitored Attributes ..... | 287 |
| Display Stored Baseline Values for an Attribute .....                    | 287 |
| Display Samples List .....   | 288 |
| Display Hourly Summary List.....   | 289 |
| Display Daily Summary List .....   | 290 |
| Display Weekly Interval List .....                                       | 291 |

## **Chapter 25: IP Event History** **293**

|  |     |
|--|-----|
| History Reports.....   | 293 |
| View Reports .....   | 294 |
| Search the TCP/IP Events Database .....  | 295 |
| Examples of Custom Searches .....  | 295 |
| Extract Data to a File .....   | 298 |
| Print Reports .....  | 298 |
| Print a Predefined Report .....  | 299 |
| Check the Print Queue .....  | 299 |
| Define Reports .....   | 299 |
| Reporting Over Extended Periods Using the System Management Facility (SMF) ..... | 301 |
| History of IP Activities .....   | 302 |

## **Chapter 26: Using Operator Console Services** **303**

|   |     |
|---|-----|
| Operator Console Services .....               | 303 |
| Access OCS .....                              | 304 |
| OCS Panel .....                               | 304 |
| Command Line .....                            | 304 |
| Operating Mode Indicators.....                | 304 |
| Roll Delete Area .....                        | 305 |
| Non-roll Delete Area .....                    | 305 |
| Roll-delimiter Line .....                     | 305 |
| Title Line .....                              | 305 |
| Time Display .....                            | 305 |
| Run Multiple OCS Panels .....                 | 306 |
| Set Window IDs .....                          | 306 |
| Function Keys .....                           | 307 |
| Conversational Function Keys .....            | 307 |
| Prefix and Suffix Function Keys .....         | 307 |
| Assign Your Own Values to Function Keys ..... | 308 |



---

|  |     |
|--|-----|
| Specify Commands to Function Keys .....                          | 309 |
| Specify Function Keys Using NCL Procedures .....                 | 310 |
| Use Commands in OCS .....  | 311 |
| Command Authority Levels .....                                   | 311 |
| Abbreviate Commands .....  | 311 |
| Reuse Commands .....   | 312 |
| Rename Commands .....  | 313 |
| Monitor and Control in OCS .....                                 | 314 |
| Control Message Presentation Speed .....                         | 314 |
| Unwrap Messages .....  | 315 |
| Clear the OCS Window .....                                       | 316 |
| Receive Non-roll Delete Messages .....                           | 316 |
| Hide NRD Messages .....  | 317 |
| Restore Hidden NRD Messages .....                                | 317 |
| Delete NRD Messages .....  | 317 |
| Use NRD Messages with ROF Sessions .....                         | 318 |
| Use the Activity Log to Help Monitor Your Regions .....          | 318 |
| Interpret Messages and Codes to Help Monitor Your Region .....   | 318 |
| Issue Commands .....   | 318 |
| Issue Commands in Background Environments .....                  | 319 |
| Issue Commands at Specified Times .....                          | 320 |
| Network Commands .....   | 324 |
| Execute or Start NCL Processes from OCS .....                    | 324 |
| Execute NCL Processes Serially .....                             | 325 |
| Execute NCL Processes Concurrently .....                         | 325 |
| NCL Identifiers .....  | 325 |
| Execute an NCL Process from a Serial or Concurrent Process ..... | 326 |
| Start REXX Programs from OCS .....                               | 326 |
| Issue System Commands from Your Console .....                    | 327 |
| Use the SYSCMD Facility .....                                    | 327 |

## **Chapter 27: Using Logs 329**

|   |     |
|---|-----|
| Log Types .....   | 329 |
| Display a Transient Log .....                             | 329 |
| Set Criteria to Display Logged Messages Selectively ..... | 330 |
| Display User-defined Log Messages .....                   | 331 |
| Obtain Help on a Logged Message .....                     | 331 |
| Print a Transient Log .....                               | 332 |
| Reset a Transient Log .....                               | 332 |
| Display the Activity Log .....                            | 333 |
| Browse the Activity Log Online .....                      | 333 |

---

|   |     |
|---|-----|
| Record Additional Information in the Activity Log ..... | 334 |
| Telnet Activity in the Log .....                        | 334 |
| FTP Activity in the Log .....                           | 335 |

## Chapter 28: Using Monitors 337

|   |     |
|---|-----|
| Resource Monitors .....                                 | 337 |
| Graphical Monitor .....                                 | 338 |
| Access the Graphical Monitor .....                      | 338 |
| Interpret the Graphical Monitor Display .....           | 339 |
| Operations From the Graphical Monitor .....             | 339 |
| Change to a Different Default Icon Panel .....          | 341 |
| Monitor Display .....                                   | 341 |
| Organize the Information on the Monitor .....           | 342 |
| Change to a Different Monitor Filter .....              | 343 |
| Change Your Default Monitor Profile .....               | 344 |
| Use Commands in the Status and Graphical Monitors ..... | 344 |
| Find Out More About Monitored Resources .....           | 345 |
| Reply to a WTOR Message .....                           | 345 |
| Override Monitoring Mode .....                          | 345 |
| Override Alerting Mode .....                            | 346 |
| Acknowledge a Link Failure .....                        | 347 |
| Respond to the Initialization Status Panel .....        | 347 |
| Respond to the Database Synchronization Panel .....     | 348 |

## Chapter 29: Using WebCenter 349

|                                |     |
|--------------------------------|-----|
| WebCenter Features .....       | 349 |
| Set Up Your Web Browser .....  | 350 |
| Set Up Internet Explorer ..... | 350 |
| Set Up Firefox .....           | 352 |
| Log On to WebCenter .....      | 353 |
| CA SYSVIEW Integration .....   | 354 |

## Chapter 30: Using Print Services 355

|   |     |
|---|-----|
| Print Services Manager .....                | 355 |
| Access PSM .....                            | 355 |
| List Entries in the Print Queue .....       | 356 |
| Display the Output of a Print Request ..... | 356 |
| Confirm Printing .....                      | 357 |
| Select the Printer .....                    | 357 |

---

|  |            |
|--|------------|
| <b>Appendix A: Packet Analyzer Records</b> | <b>359</b> |
| <b>Index</b>                               | <b>415</b> |



# Chapter 1: Introduction

---

This chapter introduces the basic components that make up your product.

Other chapters in this guide provide the following information:

- The chapter "Getting Started" helps you get started with using the product.
- The chapters "Using the IP Summary Display" to "Managing CICS Resources" help you monitor and manage resources defined in your region.
- The chapters "Diagnosing IP Networks" to "Event History" help you diagnose problems in your network and analyze the performance of defined resources.
- The last few chapters describe other facilities that you can use to support your network management tasks.

This section contains the following topics:

[System Services](#) (see page 21)

[Automation Services](#) (see page 25)

[IP Summary Display](#) (see page 30)

[Connections Management](#) (see page 31)

[Packet Tracing](#) (see page 32)

[MIBinsight](#) (see page 32)

[Performance Monitoring](#) (see page 33)

[Event History](#) (see page 33)

[WebCenter](#) (see page 33)

[ReportCenter](#) (see page 34)

## System Services

System Services provides a central core of basic functions and services.

## Operator Console

Operator Console Services (OCS) provides an operator environment for command entry to monitor and control your region.

OCS is used in conjunction with the following system services:

### **Activity Log**

Allows you to access all the commands, messages, or errors that have been issued and logged in the region for any given day

### **Network Information Utility File**

Provides descriptions of errors and codes that are displayed in OCS

### **Remote Operator Facility (ROF)**

Allows you to monitor and control remote regions through OCS

### **Network Partitioning Facility (NPF)**

Allows you to subdivide your network so that different parts are controlled by different operators

### **Event Distribution Services (EDS)**

Allows you to filter out unwanted messages in OCS before they are passed to an application procedure

### **Multiple Access Interface-Operator Console (MAI-OC)**

Allows you to log on to VTAM applications for monitoring and control

## Alert Monitor

The Alert Monitor provides an event notification system that tells you that a problem has been detected and that some action needs to be taken.

Alerts provide pro-active notification of performance-related network events. An alert is raised if a monitored attribute exceeds a user-specified threshold value or the calculated baseline and is automatically deleted when the threshold is no longer exceeded.

Alerts are also generated by event detectors when a particular event occurs, for example, the availability of a listener port or the occurrence of a File Transfer Protocol (FTP) failure.

You can update, track, and delete alerts from the Alert Monitor. You can raise a problem ticket from an alert. Alerts may also be forwarded to other applications and platforms.

**Note:** For information about defining monitoring thresholds and event detectors, see the *Implementation Guide*.

The Alert Monitor provides a single point to view problems in your IP network.

The alert monitor is also available through WebCenter.

## Security

Security for your system is provided by the User ID Access Maintenance Subsystem (UAMS). UAMS provides logon and password checking facilities, and the ability to control the authority and privileges of users. It can work together with your external security system.

**Note:** For more information, see the *Security Guide*.

## Broadcast Services

Broadcast Services let you send broadcast messages to all users. Messages can be sent to terminals or can be sent to specific users based on selection criteria.

## Print Management

The Print Services Manager (PSM) is a spooling facility that lets you control the physical printing of the reports your organization generates on JES or network printers.

## Communications

Several facilities enable communication between regions and programs, and collect the following types of message flows:

### **Inter-Network Management Connection (INMC)**

Lets you establish and monitor links between multiple regions.

### **Advanced Program-to-Program Communication (APPC)**

Lets you use the APPC protocol to connect multiple regions.

### **Inter System Routing (ISR)**

Lets you use INMC to provide centralized control at the system level.

### **Program-to-Program Interface (PPI)**

Enables programs to communicate with each other.

## Report Writer

Report Writer provides a facility for defining report layouts and generating reports to suit your particular site requirements.

## Application Development

Using application development facilities, you can write your own menus, panels, and applications using the following facilities:

- Network Control Language
- REXX
- Managed Object Development Services

## Network Control Language

Network Control Language (NCL) is the interpretive language that is used to develop procedures, which can be executed by your product.

**Note:** For more information about NCL and its features, see the *Network Control Language Programming Guide* and the *Network Control Language Reference Guide*.



## REXX

Your product supports the REXX language. You can write REXX programs to perform various tasks in your product. However, there are differences in the use of the supported REXX when compared with IBM's REXX.

**Note:** For more information, see *NetMaster REXX Guide*.

## Managed Object Development Services

Together with NCL, Managed Object Development Services (MODS) lets you create your own applications and develop panels to provide access to them. The following features are available:

### Application Register

The definitions of all applications that are built in MODS must be defined in the application register.

### Common Application Services (CAS)

A collection of high-quality, special-purpose NCL routines designed to facilitate program development.

### Panel Services

A facility to create and maintain full-screen panel definitions.

### Mapping Services

A facility that enables programmers to define complex data structures for use by NCL applications.

### Administrative Functions

Maintains MODS control libraries, panel libraries, and object services support functions.

**Note:** For more information about MODS, see the *Managed Object Development Services Guide*.

## Automation Services

Automation Services is a collection of facilities that let you manage resources in your system. Automation Services provides operational control and desired state automation, or a framework for performance monitoring.

## Knowledge Base

Automation Services uses a knowledge base to maintain resource information. System images, in which you define resources that are to be managed by a region, are part of the knowledge base.

## Status Monitor

The status monitor technology is used to provide monitors specific to the resource classes supported by your product. For example, CA NetMaster NM for TCP/IP has an IP Resource Monitor and an IP Node Monitor.

The status monitor provides a consolidated view of the status of all resources. The status monitor is updated asynchronously, so the display is always up-to-date.

You can apply flexible filtering criteria to determine the resources that appear on the status monitor. You can issue commands from the status monitor against a resource. Each class of resource has its own commands, which may display information about the resource or perform actions against it.

## IP Node Monitor

The IP Node Monitor gives visibility to critical IP nodes such as routers.

You can issue simple commands from the IP Node Monitor to ping a node, perform a traceroute, or view information in the node's MIB. You can also perform intensive monitoring on the node to help you determine the cause of a performance problem.

The IP Node Monitor is also available through WebCenter.

## IP Resource Monitor

The IP Resource Monitor gives visibility to the following types of critical IP resources:

### IP stacks

You can monitor CA TCPaccess CS and IBM's Communications Server (IBM TCP/IP) stacks for:

- Connection, Telnet, and FTP workload
- IP network, and Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) performance
- Network interfaces
- Address spaces
- Port throughput
- Simple Network Management Protocol (SNMP) management information base (MIB) attributes

### Virtual IP addresses (VIPAs)

Are IP addresses that are not associated with a physical adapter. You can monitor dynamic VIPA status and connection workload.

### Open Systems Adapters (OSAs)

Are IBM hardware devices that combine the functions of a communications controller and a channel, for connecting a system to a network. You can monitor OSA2, OSA-Express, and OSA DirectExpress usage, throughput, and error counts.

### Enterprise Extender

Provides high performance SNA access over an IP network. You can monitor:

- Line availability
- Traffic by VIPA
- Traffic by CP
- Retransmission rates
- RTP health

### **APPN/HPR**

Enables SNA LU to LU sessions between peer devices using high performance routing. You can monitor the number of RTP pipes:

- Available
- With LU to LU sessions
- With severe traffic congestion for more than five minutes
- With an inbound or outbound queue over your specified limit
- In a STALLED state
- With more than one recent serious path switch

### **Communications Storage Manager (CSM)**

Monitors IBM's Communications Server buffer pools. The monitoring of CSM buffer usage lets you compare data space, extended common services area (ECSA), and fixed storage usage between tasks.

### **Address spaces**

Let you monitor any IP server or application to help ensure the availability of listener ports, and raise alerts if the IP port traffic is outside acceptable levels.

### **Cisco channel cards**

Provides proactive notification of potential problems with Channel Interface Processor (CIP) or Channel Port Adapter (CPA) devices, and the ability to track the history of usage for capacity planning.

### **CICS resources**

(CA NetMaster SM for CICS configured in region) Let you monitor CICS resources.

The IP Resource Monitor monitors the performance and availability of these resources.

The IP Resource Monitor is also available through WebCenter.

## **Automation Services Processes**

An Automation Services process is a means of performing an action. You can define a process and have it executed on demand, or automatically on behalf of a resource.

Processes are defined by selecting one or more macros. A set of macros is distributed with your product. For example, there are macros to issue operating system commands, generate alerts, issue an SNMP TRAP, and issue a WTO. Macro parameters are supplied through full-screen panels, so that a process is easy to build and requires no programming knowledge.

## Multisystem Support

Automation Services provides focal point management to support multisystem operation (that is, management at a focal point with subordinates feeding information to it) as follows:

### **Peer-to-peer architecture**

Supports full connectivity between multiple regions. Regions linked in this way are known as focal point regions. (A stand-alone region is also regarded as a focal point region.)

When regions are communicating with each other, authorized users can monitor and control all managed resources from any terminal connected to a focal point region.

All focal point regions have the knowledge base synchronized.

### **Subordinate**

Enables you to reduce the amount of traffic in your multisystem environment. You link subordinates to focal point regions that provide central monitoring and control. A subordinate has visibility and control of the locally managed resources only.

### **Independent Operation**

Each region can run independently of other regions. If no communication links are available, each region still provides full monitoring, control, and automation of its own managed resources. If one region fails, automation continues for resources that are managed by the other regions.

You can also transmit various types of data from a stand-alone region to another region.

### **Communication Access Methods**

Multisystem links support the following communication access methods: EndPoint Services (EPS), TCP/IP, and VTAM.

### **Multisystem Knowledge Base**

Automation Services automatically maintains synchronization between linked knowledge bases, with automatic recovery in the event of link failure.

## Automation Services Administration

Automation Services provides the following implementation and administration functions:

- The ability to update prompt lists. These are lists of valid values (from which you choose one value) that are displayed when you enter a question mark (?) in a prompted field. Prompted fields are identified by the presence of a plus sign (+) at the start of the input field.
- The ability to write your own NCL procedures or macros for use in Automation Services processes.
- The ability to define commonly used monitor commands—these commands are also NCL procedures.

## IP Summary Display

The IP Summary Display provides a single place from where you can get a snapshot of the most useful information about the IP conditions and activities on your systems. You can drill down further to perform additional diagnostics.

If enabled in your menu profile, the display appears on the primary menu when you log on.

### More information:

[IP Summary Display](#) (see page 51)

[Condition Summary](#) (see page 53)

[IP Traffic Summary](#) (see page 57)

[EE Traffic Explorer](#) (see page 64)

[Alert Summary](#) (see page 71)

## Connections Management

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.

## Packet Tracing

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.

## MIBinsight

MIBinsight is a component that lets you manage SNMP Management Information Bases (MIBs). MIBinsight comprises a compiler, a browser, and the ability to monitor MIB attributes.

To browse or monitor a MIB attribute of an IP resource without MIBinsight, you must specify a unique Object Identifier (OID). OIDs are a string of numbers (usually very long); they are not very user-friendly. MIBinsight puts a face on these numbers and lets you view the knowledge of the resource in a user-friendly way.



## Performance Monitoring

Performance attribute samples and hourly summaries are maintained for all monitored IP resources and nodes. Performance history displays are available from the IP Resource Monitor and the IP Node Monitor, and from some diagnostic displays. These displays can help you identify trends and potential problems in your network.

For example, from the IP Resource Monitor you can look at the performance history for a stack's packet activity as samples and hourly aggregates.

Various styles of graphs are presented, depending on the type of attribute being sampled:

- A gauge value (GAUGE), such as average CPU utilization for a router
- A rate value (COUNT or TOTAL), which represents change in a counter, for example, errors per hour
- Non-numeric values (ENUM) such as status values (for example, OK and TIMEOUT)

## Event 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.

## WebCenter

WebCenter is a web browser interface to the region. The interface provides web access to functions such as monitoring and history.

The same user ID and password for your region are used to [access WebCenter](#) (see page 353).

The WebCenter web server runs in the region's address space. It is entirely z/OS hosted, and requires no third-party web servers or external components.

Problem resolution time is decreased and ease of use increased. Help desk users who are not familiar with z/OS mainframe 3270 interfaces can perform management functions with their standard web browser.

Every page of WebCenter has context-sensitive online help.

## 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.

# Chapter 2: Getting Started

---

These topics explain how to access and navigate the product's 3270 interface, and the major components of that interface.

This section contains the following topics:

[Log On](#) (see page 35)

[Log Off](#) (see page 36)

[Your Password](#) (see page 37)

[Access Functions](#) (see page 38)

[Lists](#) (see page 41)

[Data Entry Panels](#) (see page 43)

[Online Help](#) (see page 46)

[Work in Two Windows](#) (see page 48)

## Log On

To access your product, you must log on to it through a region. The logon procedure is the same whether you are logging on in a single system or a multisystem environment. Before you can log on to a region, you need a user ID and password. Ensure that your system administrator has defined your user ID to the region and has allocated the relevant level of authority.

**Note:** You may have access to one or more regions. This depends on whether your organization has set up a single system or a multisystem environment.

### To log on to your product

1. Use your installation defined method for establishing SNA sessions to connect to the ACB name of the region.

For example, enter **LOGON APPLID**(*acb-name*), using the ACB name of the region.

2. Enter your user ID and password on the displayed logon panel.

The Primary Menu appears.

**Note:** When you first log on to a region, the region uses a default profile for your primary menu. You can update the profile to change the format of the menu. To update the profile, enter **PROFILE** at the command prompt.

## If Region Initialization Is Still in Progress

If the Initialization in Progress panel appears on your screen instead of the primary menu, the initialization of the region is still in progress. Press F3 (Exit) to exit to the primary menu.

**Note:** For information about the initialization process, see the *Installation Guide*.

## If the System Image Is Still Being Loaded

If the local system image is still being loaded, the primary menu contains the **LS** option. You can select this option to monitor the loading process. You can also perform functions that do not depend on an active local image.

**Note:** For information about system image loading, see the *Administration Guide*.

## Log Off

To log off from the region, enter **=X** at the prompt. This terminates your current window.

If you are at the primary menu, enter **X** at the prompt to terminate your current window.

**Note:** You can have two windows for each logon to a region. If you have two windows, repeat the procedure to terminate the remaining window to log off from the region.

**More information:**

[Work in Two Windows](#) (see page 48)

## Your Password

Your password is verified by the User Access Maintenance Subsystem (UAMS).

The subsystem lets you change your password, or prompts you to change your password when it has expired after a period of time. You can change your password at any time after you log on to a region. The change becomes effective the next time you log on to the region.

**Note:** Your installation might have linked UAMS with an external security system, such as CA ACF2, CA Top Secret, and Resource Access Control Facility (RACF). If this is the case, your system administrator will tell you of any special considerations that apply when changing your password.

In a multisystem environment, the administrator might have set up the environment for the synchronization of UAMS user definitions and passwords. Changed passwords are then synchronized across connected regions.

## Change Your Password

### To change your password

1. Enter **/CHGPWD** at the prompt.

The User Password Maintenance panel appears.

2. Complete the following fields:

#### **Current Password**

Specifies your current password.

#### **New Password**

Specifies your new password.

Retype your new password, and press F3 (File).

The system changes your password.

**Note:** If UAMS synchronization is enabled, a Linked Regions UAMS Update Report panel appears when you save your changed password. The panel reports the success or failure of the password change in the connected regions.

## Authority Levels

Your user ID in UAMS determines your level of access to your product, the functions you can perform, and the commands you can issue.

If you attempt to perform an unauthorized function or issue an unauthorized command, an error message appears, telling you that you are not authorized to perform that function or issue that command.

## Access Functions

To access functions through the user interface menus, do *one* of the following:

- Select an option from each menu that leads to the function.
- Specify a path.
- Specify a shortcut.

### Select an Option

You select an option by entering the option code at the prompt. For example, entering **M** at the prompt on the primary menu takes you to the Monitors primary menu.

If you specify a collapsed or expanded menu format in your profile, you can expand or collapse the displayed menu hierarchy. In these formats, you can also place your cursor beside a required option and press Enter to select it.

**Note:** For more information, press F1 (help) from the primary menu.

### Specify a Shortcut

**Note:** The PMENUCONTROL parameter group controls the shortcuts. Your administrator can disable shortcuts or change the shortcut character.

You can jump to the panel of a function directly by using shortcuts. You can specify the shortcut at a prompt in one of the following ways:

- Specify `/shortcut-name` to retain the current panel on return.
- Specify `=/shortcut-name` to close the current panel and return to the primary menu on exit.

An entry on a menu can have an associated shortcut, displayed in turquoise.

**Note:** If you do not remember a shortcut, enter `/` or `=/` to list the shortcuts and then select one.

## **/shortcut-name**

**Important!** If the current panel provides automatic updates and you no longer need this information, use **=/shortcut-name** rather than a nested shortcut. This saves storage and resources because the region does not need to maintain a display that you no longer need.

To select the function you want, enter its corresponding shortcut, preceded by the slash (/) character, at a prompt.

When you access a function by using its shortcut, your current panel is retained. When you press F3 to exit out of the function, this panel, with any updates, is restored. By using shortcuts, panels can be nested to a maximum of 64 levels.

For example, to access the Alert Monitor History Menu without retaining the current panel, enter **=/ALHIST** at the prompt on your current panel. When you are finished with the menu, press F3 to display the primary menu.

## **=/shortcut-name**

When you have finished with your current panel, you can access the next function by prefixing the shortcut call with the equals (=) sign. This goes directly to the function without retaining the current panel and closes all other nested panels in this window.

For example, to access the Alert Monitor History Menu without retaining the current panel, enter **=/ALHIST** at the prompt on your current panel. When you are finished with the menu, press F3 to display the primary menu.

## **Access a Function That Does Not Have a Shortcut**

You can combine a shortcut with option codes to form a path to access a function that does not have a shortcut itself.

For example, to access the alert history, you can enter the **/ALHIST.B** path.

## **Specify a Path**

You can jump to the panel of a function directly by specifying the exact path to that panel. Construct the path by linking the options you need with periods. Depending on which panel you start from, you can display a panel that:

- Is lower in the panel hierarchy
- Is higher in the panel hierarchy
- Requires input data

## Lower in the Panel Hierarchy

If you start from a menu and want to access a panel lower in the panel hierarchy, specify the path as it is. For example, if you are at the primary menu and want to change your password, type **U.P** at the prompt and press Enter.

## Higher in the Panel Hierarchy

If you want to access a panel that requires you to pass through a panel higher up in the panel hierarchy, you must precede the path specification with the equals sign (=). The = character brings you back to the primary menu and then to the required panel. You can specify such a path at any prompt. For example, if you are at the Alert Monitor and want to change your password, enter **=U.P** at the prompt and press Enter.

To return to the primary menu, enter **==**.

## Input Data

If you want to access a panel that requires you to enter data, you can enter the data by separating them from the path by a semicolon (;).

For example, if you are at the primary menu and want to access the alert history for the linked region PROD2, type **H.A;PROD2** at the prompt and press Enter.

Some panels have more than one input field for entering data. You should use the correct number of semicolons to identify the field.

For example, you must use two semicolons if you want to enter *data\_2* in the second field:

*option\_1.option\_2;;data\_2*



## Lists

Lists comprise a series of items that you can select or against which you can perform actions. The panel shows the actions that you can perform on the listed items.

There are four types of list:

### Action Lists

Let you apply *actions* to one or more listed items. Enter the required action code beside the appropriate records.

### Single Selection Lists

Let you select one item from a list (for example, the list of valid values for a data entry field) by doing *one* of the following:

- Entering the **S** (Select) action code beside the item
- Moving the cursor to a position anywhere in the line containing the item you want to select and pressing Enter

### Multiple Selections Lists

Let you select one or more items in a list (for example, the list of panels used to customize your user profile).

### Numbered Lists

Let you select a single item from the list by entering the appropriate number at the prompt (for example, the list of valid values for a data entry field).

## Scrolling

If the listed information cannot fit onto the screen, use scrolling to access the off-screen information. You can scroll vertically and horizontally.

### Scroll Vertically

Use the F8 (Forward) or F7 (Backward) function key to scroll the displayed information by the amount displayed at the Scroll prompt.

The following table shows valid scroll amounts.

| Scroll Amount | Action   |
|---------------|--|
| C (or CSR)    | If scrolling forward, the line on which the cursor is currently positioned is moved to the top of the screen.<br>If scrolling backward, the line on which the cursor is currently positioned is moved to the bottom of the screen. |

| Scroll Amount | Action  |
|---------------|---|
| D (or DATA)   | <p>The display is scrolled one full page, less one row, in the specified direction.</p> <p>If scrolling forward, the last line of the current page appears as the first line on the next page.</p> <p>If scrolling backward, the first line on the current page appears as the last line on the next page.</p>          |
| H (or HALF)   | <p>The display is moved half a page in the specified direction.</p>   |
| M (or MAX)    | <p>The display is moved to the beginning or the end of the displayed information, depending on the function key (Forward or Backward) used.</p>   |
| P (or PAGE)   | <p>The display is moved one full page in the specified direction.</p>   |
| <i>n</i>      | <p>The display is moved <i>n</i> lines in the specified direction.</p> <p>If you enter a temporary scroll amount at the command prompt (for example, Command ==&gt; 5), then when you press the F7 (Backward) or F8 (Forward) function key, the displayed information is scrolled by the specified value once only.</p> |

## Scroll Horizontally

Use the F11 (Right) or F10 (Left) function key to scroll the displayed information to the right or to the left.

## Search for an Item

You can search for specific items in the retrieved information by using the F5 (Find) function key or the LOCATE command.

## F5 (Find) Function Key

The F5 (Find) function key lets you find text in the retrieved information. Enter the text you want to find, and press F5. If the text contains more than one word, enclose the text in quotation marks.

You can press F5 again to find the next instance of the text.

For some lists, you can enhance the Find function in the following ways:

- Expand the search beyond the columns currently displayed by using the FMODE command
- Change the number of records searched between prompts by using the F PROMPT command

**Note:** For information about the FMODE and F PROMPT commands, see the online help.

## LOCATE Command

The LOCATE command enables you to locate a particular record in a list. Enter **LOCATE** or **L** followed by a text string mask. The command locates the first record name that matches the mask.

# Data Entry Panels

Resource definitions are displayed and maintained through a sequence of panels on which you enter the data for that resource.

## UPDATE Mode

Many definition panels enable authorized users to switch from the BROWSE mode to the UPDATE mode by pressing F4 (Edit). You can then edit the displayed information.

## Enter Data

On a color screen, mandatory fields that you must complete are colored white. Optional fields, which you can complete as and when required, are colored turquoise. Both types of fields can be prompted fields that provide you with a list of valid values, from which you can choose one item.

## Prompted Fields with a List of Valid Values

Many fields on the data entry panels are linked to lists containing the values that you can choose for the field. These fields are called prompted fields. Most, but *not* all, prompted fields are identified by a plus sign (+).

Enter ? in a prompted field to display the value list, which can be a numbered list or a single select list.

You can prefix the question mark (?) with one or more characters. The displayed list is then restricted to values that start with those characters. For example, enter **S?** to display a list of values that start with S.

## Validate and File Data

During data entry, you can press Enter to validate your data. Validation also occurs when you:

- Access another panel (for example, when you press F8 (Forward) to access the next panel)
- Save your entered data (for example, when you press F3 (File) to save a definition)

When you finish entering data, you can do *one* of following:

- Press F3 (File) to save the data and exit the panel.
- Press F4 (Save) to save the data and remain on the panel. When adding definitions, this enables you to quickly create other similar definitions, minimizing the typing required.
- If you do *not* want to save the data, press F12 (Cancel) to exit the panel.

## Move Between Panels

Some functions lead to a series of data entry panels (for example, when you update a resource definition).

You can use *one* of the following methods to move through these panels, depending on what you need to do:

- Select all panels.
- Select specific panels from the Panel Display List.
- Select a panel from another panel.
- Select a panel from the Index Menu.
- Save a sequence of definition panels for repeated access.

## Select All Panels

You may want to access every panel. All panels are listed on a Panel Display List (for example, the panel that lists the resource definition panels). Enter **S** next to the name of the panel you want to access first, or enter the number that identifies that panel in the panel sequence at the command prompt (for example, 1 for the first panel). The selected panel appears.

Press F8 (Forward) to scroll forward to the next panel; press F7 (Backward) to scroll backward to the previous panel.

When you finish entering data, press F3 (File) to save the data. Press F12 (Cancel) if you decide not to save the data.

## Select Specific Panels from the Panel Display List

You may want to access certain panels only (for example, when you want to update only certain parts of a resource definition). All the panels required for a definition are listed on a Panel Display List. Type **S** next to the names of the panels you want to access. After you complete your selections, press Enter to display the first panel you selected. Then press F8 (Forward) to scroll forward through the panels you selected. Press F7 (Backward) to scroll backward through the panels you selected.

When you finish entering the data, press F3 (File) to save the data. Press F12 (Cancel) if you decide not to save the data.

## Select a Panel from Another Panel

If you want to skip to a panel that is not next in the sequence, and you know the sequence number of the panel you want, enter that number at the command prompt. The required panel appears.

## Select a Panel from the Index Menu

From some data entry panels, you can press F11 (Panels) to display the Index Menu panel. This menu lists all the panels available for that function. Use the Index Menu if you want to jump to a panel but do not know its place in the panel sequence.

**Note:** If you have selected two or more panels previously, pressing F11 (Panels) displays a list of the selected panels only. You can press F6 (AllPanel or SelPanel) to switch between the full list and the partial list.

## Save a Sequence of Definition Panels for Repeated Access

On a definition list panel, you can select more than one definition. You can then work on the selected definitions in sequence. Each definition can contain a number of definition panels. Normally, the list of panels appears on your screen for you to select each time you access a new definition. However, if you want to browse or update the same panels for each selected definition, you can save the list of panels you want, as shown in the following procedure.

As you move through the sequence of selected definitions, the panels appear on your screen according to the saved list. You do not have to select the panels again when you move on to the next definition.

### To save the resource definition panels for repeated access

1. Enter the **/RADMIN.R.ASMON** path.

The Address Space Monitor List panel appears.

2. Type **B** (Browse) or **U** (Update) next to the definitions you want to access and press Enter.

**Note:** You can use the F7 (Backward) or F8 (Forward) function keys to scroll through the list.

The Panel Display List window appears.

3. Type **S** next to the panels you want, and press F4 (SaveSeq).

The system saves the list of selected panels.

4. Press Enter.

The first selected panel appears.

**Note:** When you finish with one group definition, the panels for the next definition are displayed in the same sequence.

## Online Help

Online help is provided for panels and messages.

Context-sensitive help is available at different levels. When you are viewing a help panel, pressing F1 (Help) takes you to the next level of help available. Pressing F3 (Exit) takes you back to the previous level, or exits from help and returns you to the application. Pressing F4 (Return) exits help and returns you to the application immediately.

## Tip of the Day

The region displays a tip about using the product at the bottom of the primary menu.

To display the detailed tip, place the cursor on the tip and press F1 (Help).

## Help About a Panel

Panel-based online help includes information about what each panel is used for, how to complete the fields, the actions you can perform, and the use of available function keys. Use this online help to supplement the information in this guide while you are working in the region.

Press F1 (Help) to retrieve the online help for a given panel. When you are viewing a help panel, you can press F6 (HelpHelp) to find out how to use the help facility.

If the block of help text you require splits across two panels, use the arrow keys to move the cursor to the top or the bottom of the block and press F8 (Forward) or F7 (Backward) to bring the block into view.

## Help About Fields on a Panel

Many panels provide field-level online help.

To retrieve the online help for an input field, move your cursor to the field and press F1 (Help).

## Help for a Message

While you are working in the region, you receive messages that advise you of various events. These messages might be providing information only (for example, informing you that an update was successful). They might also alert you to errors (for example, if you try to enter an action that is not valid for a resource).

Each message has detailed online help text associated with it. Access the help text for a particular message in *one* of the following ways:

- If you are at a panel and a message appears in red on the third line of that panel, move the cursor to that line and press F1 (Help).
- If you receive a message referring you to the activity log for more detail, enter **/LOG** at the prompt to display the activity log.
- If you are using the activity log, a Command Entry panel, or Operator Console Services (OCS), you can do *one* of the following:
  - Move the cursor to the line displaying the message, and press F1 (Help).
  - Type the message ID at the prompt, and press F1 (Help).
- If you are viewing a transient log, enter **H** beside the message.
- You can also enter **/CODES** to display the Messages and Codes Menu that enables you to obtain help on messages and on miscellaneous error codes.

## Work in Two Windows

You can divide your physical screen into two logical windows. Each window operates independently of the other, enabling you to perform multiple functions concurrently.

To open a second window in the region, press the F2 (Split) or F9 (Swap) function key.

When one window takes up the entire screen, the other window is considered *closed*.



## Split Screens

Using the SPLIT command, you can perform the following actions:

- Split your screen horizontally and have one window above the other. Move the cursor to a row where you want to split screens, and press F2 (Split).
- Split your screen vertically and have two windows side by side. Move the cursor to any column on the bottom row, and press F2 (Split).
- Return a split screen to single window display in one of the following ways:
  - Move the cursor to the first line on your screen, and press F2 (Split) to minimize the window. The window containing the cursor disappears, and the other window expands to full size.
  - Enter =X to exit one of the windows. Your session with that window ends.

## Swap Screens

Using the SWAP command, you can perform the following actions:

- Reverse the dimensions of the active window if you have two windows open and both are visible on the screen, and switch between them.
- Open a second full-screen window if you are currently operating with a single window open, and then switch between them.

### **To swap two full-screen windows**

1. Display one of the panels.
2. Press F9 (Swap).  
The primary menu appears.
3. Proceed to the second panel you require and press F9 (Swap).  
The first of your swap-panels appears.
4. Press F9 (Swap) to switch between the two swap-panels.



# Chapter 3: Using the IP Summary Display

---

This section contains the following topics:

[IP Summary Display](#) (see page 51)

[Condition Summary](#) (see page 53)

[IP Traffic Summary](#) (see page 57)

[EE Traffic Explorer](#) (see page 64)

[Alert Summary](#) (see page 71)

## IP Summary 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 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.

## Access IP Summary Display

Use the PROFILE command to have the IP Summary Display appear at the bottom of the primary menu every time you log on to the region.

### To turn the primary menu IP Summary Display on

1. Enter **PROFILE** at the ==> prompt on the primary menu.

The Primary Menu Format Control panel appears.

2. Complete the values in the IP Summary Display field.

**Note:** For information on the fields and commands available, press F1 (Help).

Press F3 (File).

The IP Summary Display appears at the bottom of the primary menu.

### Notes:

- You can specify:

- That this display refreshes each five minutes.
- The summary components that are refreshed.

For performance reasons, be careful in specifying this if you often leave the primary menu unattended or in a background window.

- To list the available actions on a summary line, enter a question mark (?).
- Enter **Z** next to Condition Summary, EE Traffic Explorer, or IP Traffic Summary to display just Condition Summary or IP Traffic Summary on its own panel.

## Display IP Summary Alone

To display the IP Summary Display on its own panel, enter **/IPSUM** at the command prompt.

**Note:** When the display is viewed on its own panel, it is initially static. Press F6 (AutoRef) to cause the display to refresh automatically at regular five-minute intervals.

## Expand or Collapse a Summary

To expand or collapse a summary on the IP Summary Display, put the cursor beside the summary and press Enter.

To collapse all summaries, use *one* of the following methods as appropriate:

- At the primary menu, enter == at the Command prompt.
- At its own panel, press F12 (Collapse).

## 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

You can perform the following actions from the Condition Summary:

- If your monitoring environment consists of linked regions, you can enter **A** or **L** next to Condition Summary to switch between multisystem or local view.
- You can enter **A** or **P** next to Ports to switch between listing ports by address space or port number.
- You can enter **I** next to a condition to display or hide a brief explanation of what the condition is about. You can obtain more detailed information by entering **HLP** next to the condition.
- The status of a condition is based on the alerting criteria of its underlying attribute. To change the criteria, enter **UA** next to the attribute. The changes are reflected on the display at the next 5-minute period occurring after the next sample is taken for attribute being monitored.

## Stack IP, TCP, and UDP Layers

The Stack IP, TCP, and UDP Layers summary displays the status of key conditions for each stack that is monitored on a system. The summary consists of several levels. Each level summarizes the status of the underlying conditions.

### 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.

```

PROD15----- TCP/IP : Summary Display -----Hold
Command ==> Scroll ==> PAGE

      IP System + CO31                               .=Expand or Collapse ?=more actions

      Condition Summary 23:55                        Warning Problem Status
      - CO11 Conditions                               0      1 PROBLEM
      - CO31 Conditions                               0     13 PROBLEM
      | Stack IP, TCP, and UDP Layers                 0      2 PROBLEM
      | - TCPIP31A                                     0      0 OK
      |   TCPIP31V                                    0      2 PROBLEM
      |   IP Input Bytes/Hr                          562K  PROBLEM 1M
      |   IP Output Bytes/Hr                         863K  PROBLEM 5M
      |   IP Fragmentation %                         0      0 10%
      |   IP Fragmentation Fail %                   0      0 10%
      |   IP Reassembly %                           0      0 10%
      |   IP Reassembly Failure %                   0      0 10%
      |   IP Input Error %                          0      0 10%
      |   IP Input Discard %                        0      0 10%
      |   IP Output Discard %                       0      0 10%
      |   TCP Current Connections                   11  PROBLEM 50
      |   TCP Retransmissions %                     51.40 PROBLEM 100%
      |   tcpSegmentsRxmt%
      |   The condition monitors the percentage of TCP segments sent
      |   that were retransmissions. Retransmission is needed when the
      |   destination host does not acknowledge receipt of a segment
      |   within a timeout period, or when a packet carrying a TCP
      |   segment is lost or discarded before arriving at the
      |   destination host. Server congestion and hardware errors can
      |   cause packet loss, resulting in retransmissions. High
      |   retransmissions cause increased network traffic, lower network
      |   throughput, and can impact response times.
      |   TCP Cons Dropped/Hr                       132  PROBLEM 500
      |   TCP Rcv Out-of-Order %                     0      0 10%
      |   TCP Receive Error %                        0      0 10%
      |   UDP Discard %                             23.87 PROBLEM 50%
      - Stack Network Interfaces                     0      2 PROBLEM
      - Boats /Bw.sugheba 0      2 PROBLEM

```

## Stack Network Interfaces

The Stack Network Interfaces summary displays the status of key conditions for each stack network interface monitored on a system. It consists of several summary levels. Each level summarizes the status of the underlying conditions.

## Ports

The Ports summary displays the status of key conditions for each port monitored on a system. You can view the ports by protocol and port number (by default or through the P action) or by address space (through the A action). It consists of several summary levels. Each level summarizes the status of the underlying conditions.

### Example: Condition of Ports by Port Number

This example shows a partially expanded display. The sorting order is protocol (TCP followed by UDP), port number, stack, and address space.

```

PROD15----- TCP/IP : Summary Display -----Hold
Command ==> Scroll ==> PAGE

IP System + C031

Condition Summary 00:15
Warning Problem Status
0- Stack IP, TCP, and UDP Layers 0 2 PROBLEM
0- Stack Network Interfaces 0 2 PROBLEM
0- Ports (by number) 0 9 PROBLEM
  0- TCP 21 TCPIP31A FTDP31A1 0 0 OK
  0- TCP 21 TCPIP31V FTDP31V1 0 0 OK
  0- TCP 23 TCPIP31A TCPIP31A 0 1 PROBLEM
  0- TCP 23 TCPIP31V TCPIP31V 0 0 OK
    | Listener Port Status LISTEN
    | Active Connections 0 500
    | Cons in Backlog Queue 0 50
    | Backlog Cons Rejected/Hr 0 5
  0- TCP 24 TCPIP31V TCPIP31V 0 0 OK
  0- TCP 1023 TCPIP31V TCPIP31V 0 0 OK
  0- TCP 1024 TCPIP31A TCPIP31A 0 0 OK
  0- TCP 1024 TCPIP31V TCPIP31V 0 0 OK
  0- TCP 1026 TCPIP31V OSNMP31V 0 1 PROBLEM
  0- TCP 1031 TCPIP31V TCPIP31V 0 0 OK
  0- TCP 1123 TCPIP31A TCPIP31A 0 1 PROBLEM
  0- TCP 1205 TCPIP31V CCITCP3 0 0 OK
  0- TCP 2023 TCPIP31A TCPIP31A 0 1 PROBLEM
  0- TCP 2073 TCPIP31A FTDP31A2 0 0 OK
  0- TCP 2073 TCPIP31V FTDP31A2 0 0 OK
  0- TCP 2615 TCPIP31V PROD15 0 0 OK
  0- TCP 2715 TCPIP31A COMP15 0 0 OK
  0- TCP 2815 TCPIP31A COMP15 0 0 OK
  0- TCP 3123 TCPIP31A TCPIP31A 0 1 PROBLEM
  0- TCP 3124 TCPIP31A TCPTN31A 0 0 OK
  0- TCP 3124 TCPIP31V TCPTN31A 0 1 PROBLEM
  0- TCP 4123 TCPIP31A TCPIP31A 0 1 PROBLEM
  0- TCP 5057 TCPIP31A D91ADIST 0 0 OK
  0- TCP 5057 TCPIP31V D91ADIST 0 0 OK
  0- TCP 5058 TCPIP31A D91ADIST 0 0 OK
  0- TCP 5058 TCPIP31V D91ADIST 0 0 OK
  0- TCP 5059 TCPIP31A D91ADIST 0 0 OK

F1=Help F2=Split F3=Exit F5=Find F6=AutoRef
F7=Backward F8=Forward F9=Swap F12=Collapse

```

## Enterprise Extender

The Enterprise Extender (EE) summary displays EE resource use, throughput rates, error percentages, and exceptional conditions. Conditions are shown at the EE network level and for up to the ten busiest remote control points (CPs) for which an EE connection is active. The summary consists of several levels. Each level summarizes the status of the underlying conditions.

## APPN/HPR

The APPN/HPR summary displays APPN/HPR RTP pipe utilization and exceptions, at the APPN network level. It consists of several summary levels. Each level summarizes the status of the underlying conditions.

## Diagnose a Problematic Condition

In a production IP environment, Condition Summary usually shows no PROBLEMs, a few WARNINGS (for you to correct the situation before problems occur), and mostly OKs. The following procedure shows you how to diagnose a condition.

### To diagnose a condition

1. Put the cursor next to the condition summary that shows PROBLEM or WARNING, and press Enter.

The summary expands to its contributors.

2. Repeat Step 1 until you get to the underlying conditions.

A list of conditions is displayed with a bar chart showing their health: red for PROBLEM, yellow for WARNING, and green for OK.

3. Enter **HLP** beside the problematic condition.

Information about the condition appears. It identifies the attribute monitored for that condition, and provides an explanation and some recommended actions.

4. Follow the recommended actions, and continue diagnosis using, for example, the following features:

- Diagnosis menus let you diagnose problems from the resource perspective. For example, the /STACK shortcut takes you to the Stack Management menu.
- SmartTrace lets you diagnose problems from the packet flow perspective. It lets you trace packets.
- Automation Services line commands can be issued on the condition line. Enter ? to list the Condition Summary options for the monitored resource.

### More information:

[Features That Help You Manage Your IP Resources](#) (see page 103)

[SmartTrace Line Command Mode](#) (see page 197)



## 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

## Change Display

You can choose to sort IP Traffic Summary by system or stack.

To sort the display by system, enter **SYS** beside IP Traffic Summary.

To sort the display by stack, enter **STK** beside IP Traffic Summary.

**Note:** To apply a sort order as the default, you can enter it in your profile by entering **PROFILE** at the Primary Menu.

## IP Throughput

IP Throughput summarizes the TCP/IP throughput for the specified system. The summary shows the total number of stacks and interfaces for that system. It also shows the packet and byte rates, and the number of connections for the system.

### Example: IP Traffic for Monitored Stacks and Interfaces

The following example shows an expanded display.

```

      IP System + CO11                                     .-Expand or Collapse ?=more actions
      IP Traffic Summary 17:05
      IP Throughput: Total: 7 Stks, 35 Interfaces          Pkts/Sec      B/Sec      Conns
                    Connections  ---Packets/Second---      ---Bytes/S
                    Active      In      Out      In      Out
      CO11:
      | TCPIP11          205      39.36      49.37      6166
      | | OSA2           181      30.61      34.33      4295  70%
      | | OSA1           -        30.33 >99%      17.59      4255 >99%
      | | HIPERLFF       -        0.263 <1%      16.75      36.75 <1%
      | | LOOPBACK6      -        0.017 <1%      0          0 <1%
      | | LOOPBACK6      -        0          0          0          0 0%
      | | LNKVIPA        -        0          0          0          0 0%
      | TCPIP11V         5        3.660 9%      10.89      1261 20%
      | SNBUTL1M        12        2.222 6%      1.222 2%
  
```

The displayed percentages have the following meanings:

- For a stack, for example, TCPIP11, it indicates a percentage of the total for the *system*.
- For an item under a stack, for example, OSA1, it indicates a percentage of the total for the *stack*.

## Interface Traffic Statistics

Entering S next to an interface displays the IP traffic statistics for the interface. The panel also includes the relative traffic for the applications that used the interface. This information enables you to see which applications are making the most use of the interface.

### Example: Interface Traffic by Applications

The following example shows the distribution of traffic on an interface by applications:

```

Interface ..... OSA2                               Stack ..... TCPIP11 (CO11)
SRB/Port name .... DSX6200/OSD020                 Port number ..... 00
CHPID ..... 02                                     Data device ..... 6202
Type ..... OSD (OSA-E3)                           Media ..... Multimode Fiber
Speed ..... 1000 mb/sec full duplex                MAC address ..... 00145E79F356
Connection mode .... Layer 3                       Jumbo frames ..... Yes
IP Version ..... IPv4

Interface Traffic Statistics

Application      Bytes      446M 100%  ---10--20--30--40--50--60--70--80--90--
FTP              326M  73%
SBank-Supp       28.4M   6%
WEBMHTTP         20.1M   4%
CH-Sess          19.0M   4%
15 more...

Time  Pkts In  Stk% Count  Pkts Out  Stk% Count  Bytes In  Stk% Count  Bytes Out  Stk% Count
19.49  63%  6809  41%  3702  56%  774k  43%  874k  43%
19.48  75%  6546  28%  3176  72%  1264k  36%  760k  36%
19.47  73%  6510  30%  2301  57%  652k  34%  596k  34%
19.46  66%  7239  47%  3994  64%  771k  41%  749k  41%
19.45  65%  6339  50%  5046  78%  952k  62%  2046k  62%
19.45  77%  35709  40%  16690  66%  4418k  42%  5116k  42%
19.40  77%  35362  37%  17180  68%  4653k  42%  5033k  42%
  
```

**More information:**

[Application Traffic Statistics](#) (see page 60)

## Applications

Applications summarizes the IP usage by business applications for the specified system. The summary shows the busiest application for that system, the packet and byte rates, and connections for the busiest application as a percentage of the total for the system.

### 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.

|   |  |             |     |                      |     |       |     |                    |     |                                     |     |  |  |  |  |  |  |  |  |
|---|--|-------------|-----|----------------------|-----|-------|-----|--------------------|-----|-------------------------------------|-----|--|--|--|--|--|--|--|--|
| IP System + CO11                            |  |             |     |                      |     |       |     |                    |     | .=Expand or Collapse ?=more actions |     |  |  |  |  |  |  |  |  |
| IP Traffic Summary 17:25                    |  |             |     |                      |     |       |     |                    |     | Pkts/Sec B/Sec Conns                |     |  |  |  |  |  |  |  |  |
| IP Throughput: Total: 7 Stks, 35 Interfaces |  |             |     |                      |     |       |     |                    |     | 79.11 16.7K 203                     |     |  |  |  |  |  |  |  |  |
| Applications: Most active: TCPIP11          |  |             |     |                      |     |       |     |                    |     | 2.603 1672 4%                       |     |  |  |  |  |  |  |  |  |
| System/                                     |  | Connections |     | ---Packets/Second--- |     |       |     | ---Bytes/Second--- |     |                                     |     |  |  |  |  |  |  |  |  |
| Appl.                                       |  | Active      |     | In                   |     | Out   |     | In                 |     | Out                                 |     |  |  |  |  |  |  |  |  |
| CO11  |  | 203         |     | 22.37                |     | 23.36 |     | 3328               |     | 7457                                |     |  |  |  |  |  |  |  |  |
| TCPIP11                                     |  | 9           | 4%  | 1.300                | 6%  | 1.303 | 6%  | 56.53              | 2%  | 1616                                | 22% |  |  |  |  |  |  |  |  |
| TCPIPv6 fd00:7a06:a20:100::31               |  | 1           | 0%  | 1.417                | 6%  | 1.103 | 5%  | 928                | 28% | 436.9                               | 6%  |  |  |  |  |  |  |  |  |
| PROD44                                      |  | 2           | 1%  | 1.020                | 5%  | 1.307 | 6%  | 80.28              | 2%  | 1279                                | 17% |  |  |  |  |  |  |  |  |
| PROD9                                       |  | 5           | 2%  | 1.810                | 8%  | 1.637 | 7%  | 141.8              | 4%  | 1024                                | 14% |  |  |  |  |  |  |  |  |
| MVSNFSC                                     |  | 10          | 5%  | 2.597                | 12% | 2.653 | 11% | 702.9              | 21% | 455.3                               | 6%  |  |  |  |  |  |  |  |  |
| CCISSLGW                                    |  | 1           | 0%  | 0.913                | 4%  | 0.790 | 3%  | 431.2              | 13% | 348.5                               | 5%  |  |  |  |  |  |  |  |  |
| CGI-Appls7                                  |  | 33          | 16% | 1.413                | 6%  | 1.810 | 8%  | 217.3              | 7%  | 528.3                               | 7%  |  |  |  |  |  |  |  |  |

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**.

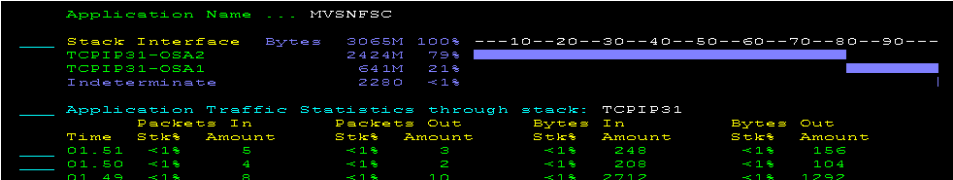
**Note:** For more information about business applications, see the *Implementation Guide*.

## Application Traffic Statistics

Entering S next to an application displays the Application Traffic Statistics panel. The panel displays the IP traffic statistics for the business application. It also includes the relative traffic over the interfaces used by the application, enabling you to see of which interfaces the application is making the most use.

### Example: Application Traffic by Interfaces

The following example shows the traffic distribution of an application over two OSAs:



More information:

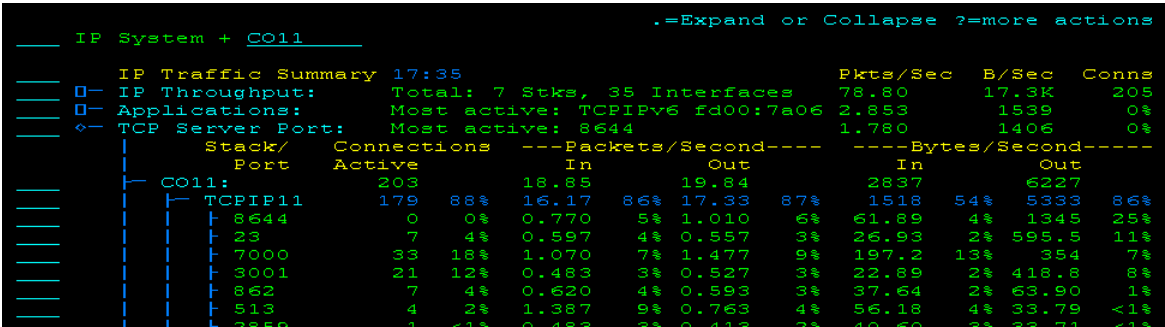
[Interface Traffic Statistics](#) (see page 58)

## TCP Server Port

TCP Server Port summarizes the statistics of TCP server ports for the specified system. The summary shows the busiest port for that system, the packet and byte rates, and connections for the busiest port as a percentage of the total for the system.

### Example: IP Traffic for TCP Server Ports

The following example shows a partially expanded display.



## Home Address

Home Address summarizes the statistics of monitored home addresses for the specified system. The summary shows the busiest home address for that system, the packet and byte rates, and connections for the busiest home address as a percentage of the total for the system.

### Example: IP Traffic for Home Addresses of Monitored Stacks

The following example shows a partially expanded display.

```

IP System + CO11                                     .=Expand or Collapse ?=more actions
-----
IP Traffic Summary 17:45
IP Throughput:      Total: 7 Stks, 35 Interfaces      Pkts/Sec      B/Sec      Conns
Applications:      Most active: FTP                  5.310         4491        0%
TCP Server Port:    Most active: 3505                 2.197         2206        0%
Home Address:       Most active: 192.168.65.11         78.04         18.1K       99%
  Stack/
  Home Address      Active      Connections  ---Packets/Second---  ---Bytes/Se
  CO11:
  | TCPIP11          179      89%      39.09      87%      40.24      90%      8265      86%      1
  | | 192.168.65.11  177      99%      38.44      98%      39.60      98%      8186      >99%
  | | 192.168.36.74   0       0%       0.600      2%       0.600      1%       73.40      <1%      1
  | | 192.168.66.11   0       0%       0.017      <1%      0.010      <1%      3.627      <1%      2
  | | *LOOPBACK       0       0%       0.027      <1%      0.027      <1%      2.080      <1%      2
  | | 192.168.36.75   0       0%       0          0%       0          0%       0          0%
  | TCPIP11V          5       2%       2.080      5%       2.183      5%       1008      11%
  | SWSWTLMA          12      6%       1.567      4%       0.893      2%       176.7      2%      1

```

## Remote Network

Remote Network summarizes the statistics of the remote networks that are communicating with the specified system. The summary shows the busiest remote network for that system, the packet and byte rates, and connections for the busiest remote network as a percentage of the total for the system.

### Example: IP Traffic for Remote Networks Seen by Monitored Stacks

The following example shows a partially expanded display.

```

IP System + CO11                                     .=Expand or Collapse ?=more actions
-----
IP Traffic Summary 17:55
IP Throughput:      Total: 7 Stks, 35 Interfaces      Pkts/Sec      B/Sec      Conns
Applications:      Most active: FTP                  145.1         147K        0%
TCP Server Port:    Most active: 3702                 144.6         147K        0%
Home Address:       Most active: 192.168.65.11         206.5         157K       99%
Remote Network:     Most active: 192.168.*             180           154K       30%
  Stack/
  Remote Network    Active      Connections  ---Packets/Second---  ---Bytes/Se
  CO11:
  | TCPIP11          179      89%      129      96%      78.29      95%      148K      >99%
  | | 192.168.*       53      30%      118.1     92%      61.84      79%      147K      >99%
  | | 172.31.*        44      25%      5.340      4%       9.080      12%      459.1     <1%
  | | 172.30.*        51      28%      2.820      2%       3.470      4%       249.9     <1%      7
  | | 172.20.*        12       7%       1.947      2%       1.737      2%       99.88     <1%      3
  | | 172.16.*        13       7%       0.597      <1%      1.410      2%       41.37     <1%      3
  | | 172.16.0.*      4       2%       0.133      <1%      0.222      <1%      7.333     <1%      3

```

## Remote IP Address Lists

The list enables you to identify remote IP addresses that have sent packets to or received packets from a mainframe stack since the Packet Analyzer was last started.

You can sort a list of remote addresses. For a remote address, you can view any available traffic statistics. You can also look up the host name of an address.

The following action is available in Remote Network:

### RI

Lists the busiest addresses in a remote network for the past 5 minutes.

### Example: Busiest Remote Addresses

You enter RI next to the 192.168.\* remote network and list the busiest remote IP addresses.

```

___  Remote Network:  Most active: 192.168.*      73.64      55517      85%
    Stack/           Connections ---Packets/Second--- ---Bytes/Se
    Remote Network  Active      In      Out      In
    COll:           328      86.67      93.9      35996      6
    TCPiP11         322  98%      85.7  99%  91.93  98%  35881 >99% 6
    RI              1  192.168.*      275  85%  39.22  46%  34.42  37%  32139  90% 2

PROD1----- TCP/IP : Remote IP Addresses for 192.168.* -----TCPIP11
Command ==>                                         Scroll ==> CSR

Sort Order: Last 5min Bytes (Descending)      Filter: None
Line 1 of 45 (from 45 matching records, 474 total records)
S=Traffic Statistics NL=Name Lookup DT=Duration Times C=Connections
Remote ----- Last 5 Minutes -----
Address Packets Pkts In Pkts Out Bytes Bytes In Bytes Out
192.168.65.11 8366 4183 4183 9.09M 4.543M 4.543M
192.168.65.31 11895 6655 5240 5.936M 4.253M 1.683M
192.168.210.246 2436 1936 500 2.769M 2.721M 48440
192.168.200.140 1159 545 614 294828 240626 54202
192.168.219.199 875 438 437 225957 145128 80829
192.168.107.159 108 48 60 21510 6096 15414
192.168.65.61 277 138 139 18013 8900 9113
192.168.27.92 36 18 18 10048 7292 2756
192.168.112.128 29 0 29 7714 0 7714
192.168.36.149 34 17 17 5356 2672 2684
192.168.200.176 30 15 15 4580 1160 3420
192.168.204.45 30 15 15 4550 2270 2280
192.168.36.150 30 15 15 4550 2270 2280
192.168.36.159 29 15 14 4498 2270 2228
F1=Help F2=Split F3=Exit F4=Return F5=Find F6=Refresh

```

More information:

[List Remote Addresses](#) (see page 124)

## IP Protocol

IP Protocol summarizes the throughput by protocol for the specified system. The summary shows which protocols use most of the bandwidth. It shows the bytes in and out for each protocol as a percentage of the total for the system.

### Example: IP Traffic for Monitored Stacks by Protocol

The following example shows a partially expanded display.

```

      IP System + CO11                                     .==Expand or Collapse ?=more actions
      IP Traffic Summary 18:05
      IP Throughput:      Total: 7 Stks, 35 Interfaces      Pkts/Sec   B/Sec   Conns
      Applications:      Most active: TCPIPv6 fd00:7a06      2.863      1539      0%
      TCP Server Port:    Most active: 23                  1.423      590.2      4%
      Home Address:       Most active: 192.168.65.11        65.20      13.8K      98%
      Remote Network:     Most active: 192.168.*            39.65      9825      29%
      IP Protocol:        TCP: 48%  UDP: 44%  ICMP: 8%  OSPF: <1%  Other: <1%
      System/Stack      Pkts Bytes   Pkts Bytes   Pkts Bytes   Pkts Bytes   Pkts Bytes
      CO11:
      | TCPIP11          48%  48%   38%  44%   13%   8%   <1%  <1%  <1%  <1%
      | TCPIP11V         50%  46%   35%  45%   14%   9%   0%   0%   0%   0%
      | TCPIP11A         79%  89%   12%   7%   8%   4%   0%   0%   0%   0%
      | TCPIP11A         0%   0%   94%  99%   6%   1%   0%   0%   0%   0%
      | SNBVT1MA        20%  27%   35%  45%   3%   5%   24%  15%  17%   0%
  
```

## Subsystem

Subsystem provides visibility of the following IBM subsystems in the context of IP traffic:

- Customer Information Control System (CICS)
- DB2
- Information Management System (IMS)
- WebSphere MQ

The explorer shows the relative IP traffic in bytes for the subsystems and the constituent address spaces.

From the 3270 interface, you can expand a subsystem to its address spaces and you can expand an address space to the stacks it uses. You can also list associated connections and view the data samples.

### Example: Explorer with DB2 Expanded

The following explorer display shows a DB2 subsystem with two address spaces:

```

      Subsystem: 13:00  DB2: 30%  CICS: 20%  IMS: <1%  MQ: 9%  Other: 40%
      System/      Total
      Subsystem Bytes
      MVS1:        2000M 100%
      | DB2         800M  40%
      | | VSDIST    200M  10%
      | | VSDIST    600M  30%
      | CICS        200M  10%
      | IMS         200M  10%
      | MQ          100M   5%
      | Other       700M  35%
  
```

## Summaries by Stacks

You get a different view of the summaries when you sort them by stacks.

|     |                          |               |  |                |         |              |       |       |       |            |          |       |       |
|-----|--------------------------|---------------|--|----------------|---------|--------------|-------|-------|-------|------------|----------|-------|-------|
|     | IP Traffic Summary 00:58 |               |  |                |         |              |       |       |       |            | Pkts/Sec | B/Sec | Conns |
| [-] | TCPIP31                  | 6 Interfaces  |  |                |         |              |       | 178.6 |       | 112K       | 129      |       |       |
| [-] | SNSSLATE                 | 2 Interfaces  |  |                |         |              |       | 29.86 |       | 26017      | 4        |       |       |
| [-] | TCPIP31V                 | 15 Interfaces |  |                |         |              |       | 0.31  |       | 28.02      | 1        |       |       |
| [-] | TCPIP99                  | 3 Interfaces  |  |                |         |              |       | 0.227 |       | 14.8       | 0        |       |       |
|     |                          | Connections   |  | Packets/Second |         | Bytes/Second |       |       |       |            |          |       |       |
|     |                          | Active        |  | In             |         | Out          |       | In    |       | Out        |          |       |       |
|     | Interfaces:              | 0             | 0%   | 0.113          | <1%     | 0.113        | <1%   | 7.707 | <1%   | 7.093      | <1%      |       |       |
|     | LOOPBACK                 | -             |  | 0.08           | 71%     | 0.08         | 71%   | 5.08  | 66%   | 5.08       | 72%      |       |       |
|     | OSA                      | -             |  | 0.033          | 29%     | 0.033        | 29%   | 2.627 | 34%   | 2.013      | 28%      |       |       |
|     | LOOPBACK6                | -             |  | 0              | 0%      | 0            | 0%    | 0     | 0%    | 0          | 0%       |       |       |
|     | Home Addresses:          |               |  |                |         |              |       |       |       |            |          |       |       |
|     | *LOOPBACK                | 0             | 0%   | 0.08           | 71%     | 0.08         | 71%   | 5.08  | 66%   | 5.08       | 72%      |       |       |
|     | 192.168.36.31            | 0             | 0%   | 0.033          | 29%     | 0.033        | 29%   | 2.627 | 34%   | 2.013      | 28%      |       |       |
|     | TCP Server Ports:        |               | IPSD0003 No statistics available for system PROD4411 |                |         |              |       |       |       |            |          |       |       |
|     | Remote Networks:         |               |  |                |         |              |       |       |       |            |          |       |       |
|     | 192.168.*                | 0             | 0%   | 0.03           | 26%     | 0.03         | 26%   | 2.427 | 31%   | 1.813      | 26%      |       |       |
|     | 172.24.*                 | 0             | 0%   | 0.003          | 3%      | 0.003        | 3%    | 0.2   | 3%    | 0.2        | 3%       |       |       |
|     | Non-Remote               | 0             | 0%   | 0.08           | 71%     | 0.08         | 71%   | 5.08  | 66%   | 5.08       | 72%      |       |       |
|     | IP Protocols:            |               | TCP:   |                | 0%      | UDP:         |       | 51%   | ICMP: |            | 49%      |       |       |
|     | Applications:            |               | Most active:   |                | MVSNFSC |              | 80.18 |       | 57400 |            | 3%       |       |       |
| [-] | Subsystem:               |               | DB2:   |                | 5%      | CICS:        |       | 0%    | IMS:  |            | 0%       |       |       |
| [-] |                          |               |  |                |         |              |       | MQ:   | 0%    | Other: 95% |          |       |       |

## 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.



## Bytes by VIPA

Bytes by VIPA totals the bytes sent and received over all EE connections that a specified VIPA.

**Note:** One VIPA can support one or many connections.

### Example: Bytes by VIPA

The following example shows an expanded display.

```
EE Traffic Explorer Traffic for hour: 00:00 (only 59 mins)
  Bytes by VIPA      Most Active: 172.16.0.0      31.4M >99%
  Total Bytes      31.7M 100% ---10--20--30--40--50--60--70--80--90--
  172.16.0.0      31.4M >99% ████████████████████████████████████████
  172.31.255.255_  229K <1%
```

## Bytes by EE Connection

Bytes by EE Connection totals the bytes sent and received by all RTP Pipes, for all traffic priorities, on a specified EE Connection.

The EE connection is identified by its remote CP name.

### Example: Bytes by EE Connection

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

|                                |  |  |
|--------------------------------|--|--|
| EE Traffic Explorer            | Traffic for hour: 00:00 (only 59 mins) |  |
| [-] Bytes by VIPA              | Most Active: 172.16.0.0                | 31.4M >99%                               |
| [-] [-] Bytes by EE Connection | Most Active: USIL0001.A07X00           | 31.4M >99%                               |
| Total Bytes                    | 31.7M 100%                             | ---10--20--30--40--50--60--70--80--90--- |
| USIL0001.A07X00                | 31.4M >99%                             |  |
| USIL0002.A31X22                | 0 0%                                   |  |
| NMD1.NMD1AP                    | 116K <1%                               |  |
| Others                         | 113K <1%                               |  |

## Bytes by EE Port

Bytes by EE Port totals the bytes sent and received over each EE port.

### Example: Bytes by EE Port

This example shows an expanded display.

|                                |  |  |
|--------------------------------|--|--|
| EE Traffic Explorer            | Traffic for hour: 00:00 (only 59 mins) |  |
| [-] Bytes by VIPA              | Most Active: 172.16.0.0                | 31.4M >99%                               |
| [-] [-] Bytes by EE Connection | Most Active: USIL0001.A07X00           | 31.4M >99%                               |
| [-] [-] [-] Bytes by EE Port   | Most Active: 12001                     | 31.4M >99%                               |
| Total Bytes                    | 31.7M 100%                             | ---10--20--30--40--50--60--70--80--90--- |
| 12000                          | 226K <1%                               |  |
| 12001                          | 31.4M >99%                             |  |
| 12002                          | 33.1K <1%                              |  |
| 12003                          | 17.2K <1%                              |  |
| 12004                          | 0 0%                                   |  |

## Bytes by Protocol Layer

Bytes by Protocol Layer totals the bytes sent and received over all EE connections by the following protocols:

### IP Headers

Contains addressing and control information.

### UDP Headers

Contains source and destination port information.

### LLC Headers

Use this option to establish the connection, send data as NLPs, terminate the connection, send a negative response, and send a heartbeat.

### NHDR (NLP) Network Layer Headers

Used to route NLPs (network layer packets) from one RTP end point to the other.

### THDR Transport Header

Identifies the RTP pipe.

### SNA TH Transmission Headers

Identifies the SNA LU-LU session.

### SNA RH Request Headers

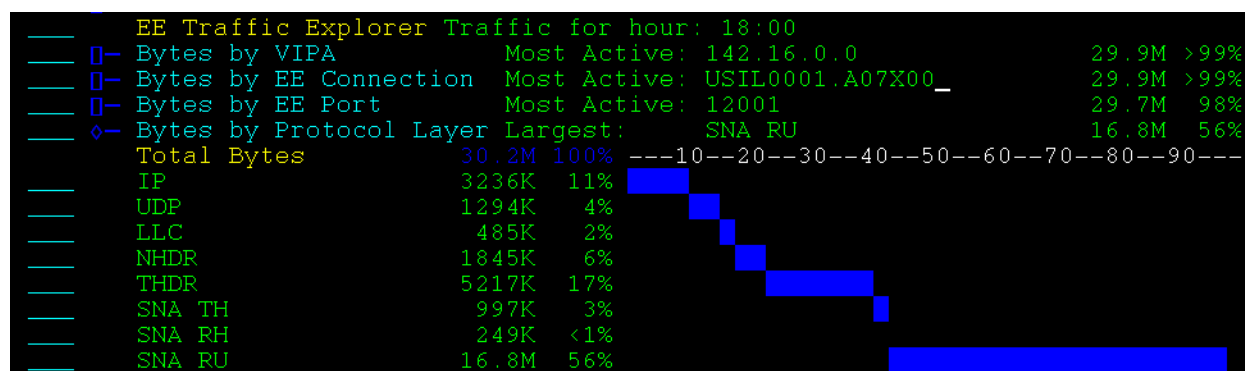
Identifies the type of data in the RU.

### SNA RU Request Units

Specifies the data sent by the SNA application. An RU is an SNA command and response, or user data.

### Example: Bytes by Protocol Layer

This example shows an expanded display. The protocol layer with the largest number of bytes transferred is SNA RU.



## Bytes by Payload

Bytes by payload shows the ratio of payload to total transmission over all EE connections. This display shows the following payload types:

### EE Overhead

Displays the overhead EE requires to send the APPN/HPR data.

### APPN/HPR Overhead

Displays the overhead that APPN/HPR requires to send the SNA application data.

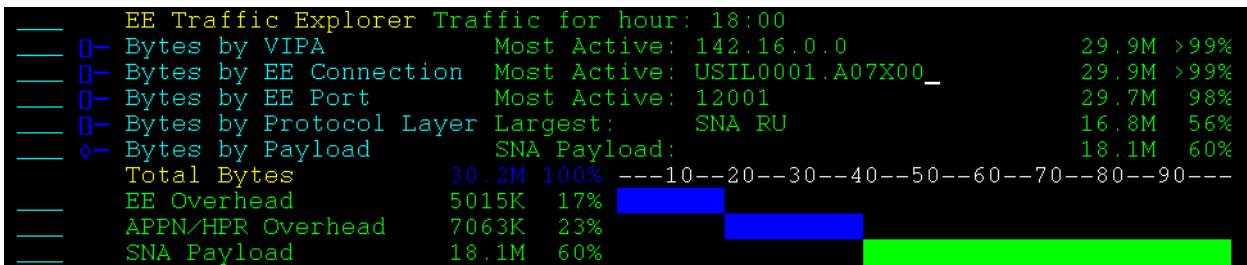
### SNA Payload

Displays the SNA application traffic.

**Note:** It is normal EE operation for the proportion of payload to overhead to vary with the traffic load.

### Example: Bytes by Payload

This example shows an expanded display. SNA data is 60% of the total traffic.

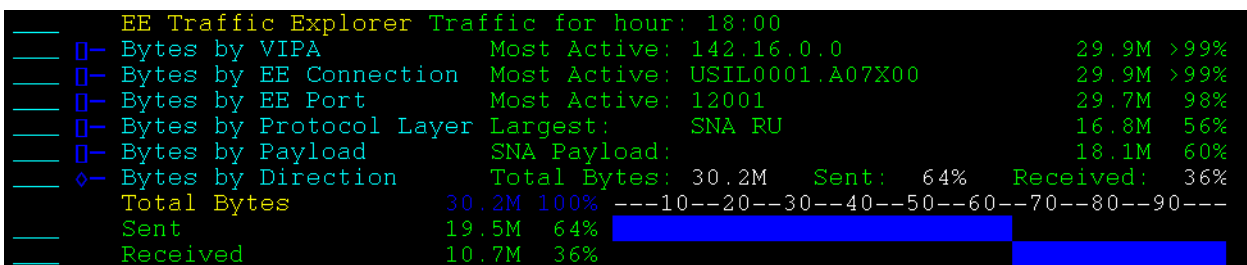


## Bytes by Direction

Bytes by Direction totals the bytes sent and received over all EE connections.

### Example: Bytes by Direction

This example shows an expanded display. More bytes have been sent than received.



## Packets by Type

Packets by type totals the packets sent and received into the following types:

### Heartbeat

Specifies an LLC TEST frame, sent by the EE connection endpoints to check whether the connection is active.

### XID

Specifies LLC XID frames, which are exchanged by the endpoints to negotiate and confirm the configuration of a new EE connection.

### HPR Control

Specifies an HPR control packet, which is an NLP with no NLP data.

### SNA

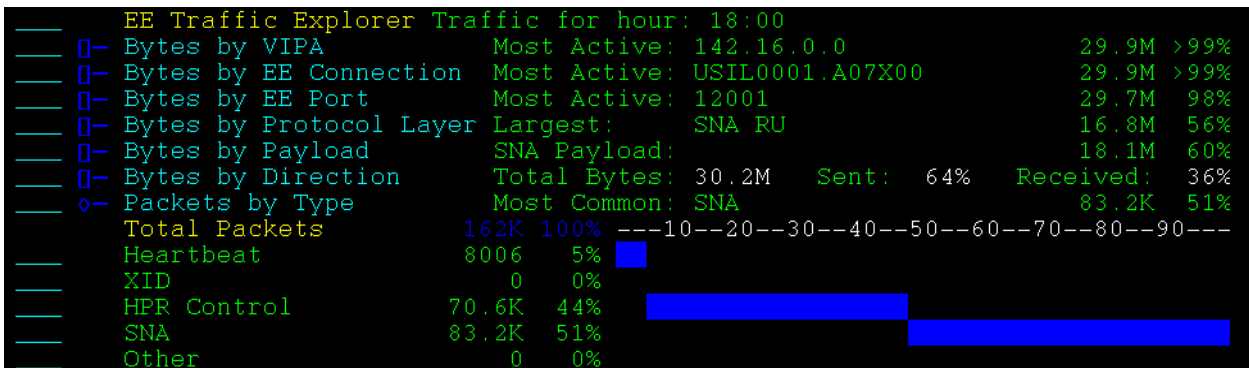
Specifies an SNA packet, which includes at least one SNA TH, RH, or RU.

### Other

Specifies LLC frames, other than XID or TEST, and function routing NLPs.

### Example: Packets by Type

This example shows an expanded display. SNA is the most popular packet type.

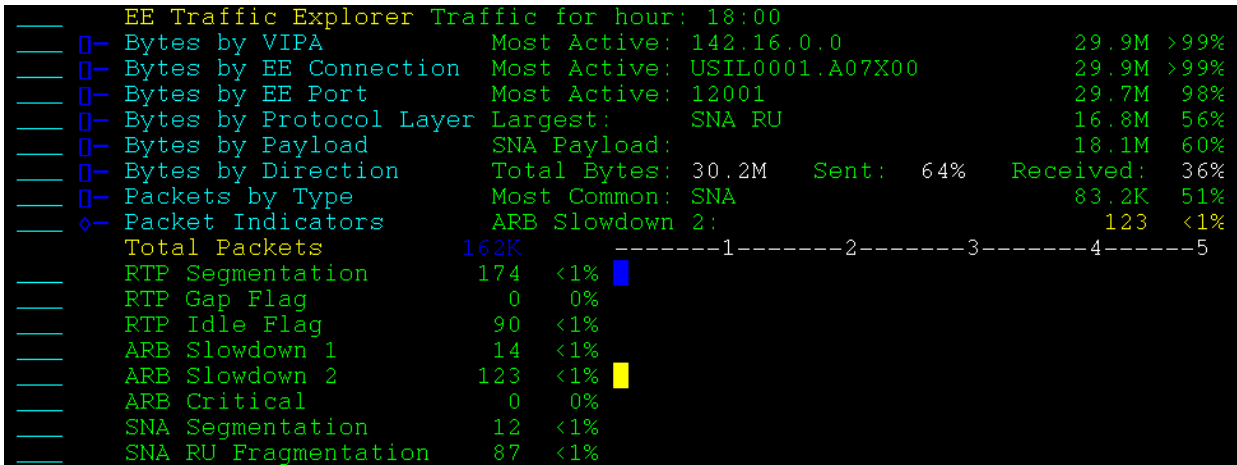


## Packet Indicators

Packet indicators shows the total packets grouped by the transmission header control settings. The values are independent of each other and do not add up to 100%.

### Example: Packet Indicators

This example shows an expanded display.



## 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.

```

PROD44----- TCP/IP : Summary Display -----Hold
Command ==>                                     Scroll ==> CSR

      .=Expand or Collapse ?=more actions

___ IP System + CO11 ___

___ Condition Summary 03:00
___ 0- Stack IP, TCP, and UDP Layers           Warning 3 Problem 24 PROBLEM
___ 0- Stack Network Interfaces                2      26 PROBLEM
___ 0- Ports (by number)                       0      24 PROBLEM
___ 0- Enterprise Extender                     0      2 PROBLEM
___ 0- APPN/HPR (SERVER01.A31X99)              1      0 WARNING
___ 0- Region Health                           0      0 OK

___ IP Traffic Summary 03:02
___ 0- IP Throughput: Total: 4 Stks, 26 Interfaces Pkts/Sec B/Sec Conns
___ 0- Applications: Most active: MF2T7SRV          96.06 60724 11%
___ 0- TCP Server Port: Most active: 8810           27.12 23646 2%
___ 0- Home Address: Most active: 192.168.65.31      201.6 114K 92%
___ 0- Remote Network: Most active: 192.168.*        135.9 85084 37%
___ 0- IP Protocol: TCP: >99% UDP: <1% ICMP: <1% OSPF: 0% Other: <1%
___ 0- Subsystem: DB2: 7% CICS: 0% IMS: 0% MQ: 0% Other: 93%

___ EE Traffic Explorer Traffic for hour: 02:00 (only 59 mins)
___ 0- Bytes by VIPA Most Active: 192.168.66.41      43378 100%
___ 0- Bytes by EE Connection Most Active: SERVER01.A13X99 43378 100%
___ 0- Bytes by EE Port Most Active: 12003 (medium) 36930 85%
___ 0- Bytes by Protocol Layer Largest: SNA RU 19580 45%
___ 0- Bytes by Payload SNA Payload: 20696 48%
___ 0- Bytes by Direction Total Bytes: 43378 Sent: 49% Received: 51%
___ 0- Packets by Type Most Common: Heartbeat 208 50%
___ 0- Packet Indicators RTP Idle Flag: 20 5%

___ Alert Summary: 28/1 581 sev2 121 sev3 12/4
*** ***** Bottom of data *****

```





# Chapter 4: Managing Connections

---

This section contains the following topics:

- [Connection Lists](#) (see page 73)
- [List Connections](#) (see page 76)
- [Store Criteria](#) (see page 77)
- [Recall Criteria](#) (see page 77)
- [Sort Connection Lists](#) (see page 78)
- [Locate Information on Sorted Connection Lists](#) (see page 78)
- [List Specific Connections](#) (see page 79)
- [Display Connections Graphically](#) (see page 80)
- [Display Connection Statistics](#) (see page 81)
- [Connections for Multiple Systems](#) (see page 81)
- [Display Connection Information](#) (see page 83)
- [Display AT-TLS Information](#) (see page 84)
- [Check for SNA Related Problems on Telnet Connections](#) (see page 84)
- [Look Up a Device Name](#) (see page 85)
- [Drop a Connection](#) (see page 86)
- [Diagnose Data- and Protocol-Related Problems in a Connection](#) (see page 86)
- [Diagnose Telnet Response Time Problems](#) (see page 87)
- [Diagnose Throughput of Data Transfers](#) (see page 88)

## Connection Lists

From a connection list you can diagnose performance or connectivity related problems. For example, if an FTP file transfer is taking an unusually long time or is stalling, you may want to view the connection information to see if there are any data transfer problems.

You can produce a list of connections to the IBM TCP/IP or CA TCPaccess CS host, or Cisco channel card, to match a set of criteria. For example, you can produce a list specifically for all Telnet connections or, more generally, for all connections with a particular task name. You can also produce a list of all connections with a particular local port number.

For each connection list option, there is a Connection List Criteria panel. This appears when you select an option, and it lets you specify criteria to filter the connections to display. You can limit the maximum number of connections displayed for each stack and set the initial sorting order.

## Telnet Connection List

The Telnet Connection List displays information about the current state of active Telnet connections to a TCP/IP host or Cisco channel card.

The Telnet Connection List can provide the following types of information:

- Mapping of IP addresses to LU names and VTAM application names
- Combined information from more than one of these sources—IBM TCP/IP, CA TCPaccess CS, or the channel card

You can use the actions shown on the TCP/IP : Telnet Connection List, for example, P=Ping or T=TraceRoute, to investigate problems occurring on any of the listed connections.

You can list the following connections:

### **Telnet Connections**

Displays standard Telnet connection details, for example, host, port, LU name, application, server, and byte counts.

### **Telnet Connections (Advanced)**

Displays all standard details, plus User ID, Round Trip Time (RTT), retransmit, and fragment data from the Packet Analyzer.

### **Telnet Connections (NetSpy RTM)**

(CA NetSpy required) Displays all standard details, plus session type, average network response time, and average host response time.

### **Telnet Connections (Advanced + RTM)**

(CA NetSpy required) Displays all advanced details, plus session type, average network response time, average host response time, and packet counts.

## FTP Connection List

The FTP Connections list displays information about FTP connections that use IBM stacks on systems with at least z/OS V1R10.0.

You can list connections that satisfy specified criteria. From the list, you can perform actions to investigate problems occurring on a connection.

## CICS Socket Connection List

CICS Socket Connection List displays information about the current state of any active CICS socket connections.

**Note:** CICS socket connection lists are available only if your TCP/IP management region is configured with CA NetMaster SM for CICS.

You can list the following connections:

### **CICS Socket Connections**

(CA NetMaster SM for CICS required) Displays CICS socket connections from the Packet Analyzer.

### **CICS Socket Connections (with History)**

(CA NetMaster SM for CICS required) Displays general connection details for active and closed connections.

## General Connection List

The Connection List displays information about the current state of any active connections to the selected stack.

You can investigate problems occurring on any of the listed connections by using the actions shown on the Connection List panel.

You can list the following connections:

### **General Connections**

Displays general IP connection details for any connections, including local host, remote host, port, task name, start time, idle time, stack, and byte counts.

### **General Connections (Advanced)**

Displays general connection details, plus Telnet User ID, packet counts, elapsed time, RTT, retransmit, and fragment data from the Packet Analyzer.

### **General Connections (with History)**

Displays advanced general connection details for active and closed connections.

## Listener List

The TCP Listeners list displays information about listeners for IBM stacks.

You can list listeners that satisfy specified criteria. From the list, you can perform actions to investigate problems occurring on a listener (for example, connections dropped because backlog exceeded).

## Which List Connections Option Should I Use?

The following table can help you to decide which option to use for which task.

| Task   | Option   |
|--|--|
| View long-running connections                                  | CF or CH   |
| Investigate whether connections are affected by network errors | TF or CF and specify local or remote retransmit values, or both. |
| Investigate whether connections have fragmented packets        | TF or CF and specify local or remote fragment values, or both.   |
| View FTP connections using IBM stacks                          | F  |
| View listener ports  | C or L   |
| View Telnet connections from CIP TN3270 interfaces             | T or TR  |

## List Connections

You can list connections that satisfy specified criteria. From the list, you can perform actions to find out more about a connection (for example, connection details such as IP addresses and packet information such as fragmentation).

### To list connections

1. Enter **/IPCON** at a prompt.  
The Connections menu appears.
2. Enter one of the Connections options at the prompt.  
The Connection List Criteria panel appears.
3. Complete the fields as required, and press F6 (Action).  
**Note:** For information about the fields, press F1 (Help).  
The requested connections are listed.

## Store Criteria

After you define criteria, you can save it for future use.

### To define and store criteria

1. Complete the criteria fields on the Connection List Criteria panel.  
**Note:** Press F1 (Help) for information about the fields.
2. Press F11 (Store).  
The Save Connection List Search Criteria panel appears.
3. Enter the following values:
  - Enter a value in the Criteria Name field that identifies this set of criteria.
  - Enter a brief description in the Description field.

Press F3 (File).

The specified criteria are stored in the virtual file system (VFS) data set.

## Recall Criteria

You can list connections by recalling a stored connection list criteria definition from the Connection List Criteria panel.

### To list connections satisfying a stored set of criteria

1. Press F5 (Recall).  
The list of stored criteria definitions appears.
2. Enter **S** next to an entry from the list.  
The stored criteria definition is used to complete the Connection List Criteria fields.
3. Press F6 (Action).  
A connection list appears, satisfying the stored criteria that you specified.

## Sort Connection Lists

The SORT command lets you display connections in a specific order. When sorting is by address, IPv4 addresses come before IPv6 addresses.

The only operand is the column heading of the column you want to sort by. For example, enter **SORT STATUS** to sort the list by status. The minimum number of characters needed to uniquely specify the column is sufficient. For example, SORT F is equivalent to SORT FOREIGN HOST.

**Note:** You can sort by most column headings.

**To sort by other than the set default value:**

1. Enter **SORT ?** at the prompt.  
The Sort Values List appears.
2. Select the sort value that you want and press Enter.  
The list is sorted in the specified order.

## Locate Information on Sorted Connection Lists

You can use the LOCATE command to position a connection list to a particular row on the list.

**Note:** You must use the SORT command to sort the list before you use the LOCATE command. The SORT NONE command disables the LOCATE command.

The value you specify after the LOCATE command applies to the sort value that applies to the list. It does not necessarily apply to the first column of the list unless you have sorted by the first column.

### Example: Locate Information on a List Sorted by Foreign Host

If you sort by foreign host and you issue the LOCATE 200 command, the cursor is positioned at the line before the first IP address that starts with 200. It locates an IPv4 address in preference to an IPv6 address. If you want to locate an IPv6 address, include the colon (:) (for example, 200:).

### Example: Locate Information on a List Sorted by Status

If you sort by status and you issue the LOCATE Listen command, the cursor is positioned at the line before the first status that starts with Listen.

## List Specific Connections

You can find a user's connection by entering the user's Telnet LU name or IP address in the LU Name or Foreign Host field (respectively) on a connection list criteria panel. By specifying an LU name or IP address, you can restrict a connection list to one particular host.

You can also limit the list by specifying an IP address mask (for example, 172.16.122.\* or fe80:\*), a Telnet LU name, or an application name mask.

For IPv4, you can specify a mask by using the asterisk (\*) wildcard for an octet of the address (matching any number from 0 through 255). For example, a mask of 172.16.122.\* matches 172.16.122.1 and 172.16.122.56.

Similarly, for IPv6, you can specify a mask by using the asterisk wildcard for a segment (matching any number from 0 through ffff).

You can specify the mask of a name by using the asterisk (\*) and question mark (?) wildcards (\* matches 0 or more characters, and ? matches exactly one character). For example, a mask of LU00\* matches LU001 and LU0056, while a mask of LU00? matches LU001 and LU005, but does not match LU0056 because the ? matches exactly one character.

## Find an LU Name

The LU name for your logon to a region appears on the right of the Primary Menu.

Some SNA applications also display the connected LU name on a panel in the application. A user can check any individual SNA application to find the LU name.

You can use the appropriate command for your application to display the LU name for the LU you are using. For example, for a CA NetMaster application, the SHOW USERS command displays LU names beside user IDs.

## Find an IP Address

Many users call their help desk with a TCP/IP problem and do not know their IP address, particularly if they have implemented the Dynamic Host Configuration Protocol (DHCP) that can cause IP addresses to change from day to day.

You can ask users to find their IP address (for their help desk to specify in the Remote Host field on the TCP/IP : Connections menu) in the following ways:

### To find your IP address on a Windows system

1. Click Start, Run.

The Run window appears.

2. Type CMD and click OK.

A command prompt window appears.

3. Enter the command IPCONFIG.

The TCP/IP Configuration appears, showing the current IP address and other information such as subnet mask and default gateway.

## PC Application Help

Some PC applications provide an IP address in the Help menu. If you are using a PC application, find your IP address by selecting *Help - About* on your application menu. The displayed window may provide the IP address of your computer.

## Display Connections Graphically

The connections from a particular remote host can be graphically displayed from a connection list.

For a connection list, you can diagnose performance- or connectivity-related problems from a graphical display.

The Telnet connections display has four layers: the TCP/IP host, the Telnet server, the connections, and the SNA applications.

When the display splits out at the third layer to show connections, it is not rejoined at the application level, even if the same application is being used. This enables the different application sessions to be distinguished.

### To display connections graphically for a specific host

1. Enter **S** next to an entry on the Connection List.

The Connections panel appears, showing the connections to the remote host.



## Display Connection Statistics

Connection Statistics displays the following statistics about the number of bytes and packets transferred in a connection:

- Counts in 1-minute and 5-minute intervals
- Total counts since the connection is being monitored
- Total counts (excluding packet headers) since the connection is being monitored

### To display connection statistics

1. Enter **CS** next to a connection on a connection list.

The Connection Statistics panel displays byte and packet statistics on a selected connection.

## Connections for Multiple Systems

The connection lists display information about the current state of active connections to multiple host systems. Connection lists for multiple systems are available for the following types of systems:

- Multiple CA TCPaccess CS hosts
- Multiple IBM TCP/IP hosts
- Multiple channel cards
- Mixed hosts including IBM TCP/IP hosts, CA TCPaccess CS hosts, and Cisco channel cards.

**Note:** Channel cards are available for selection from Telnet server connection lists (option T or TR) only.

## Display Connections for Multiple Systems

### To display a list of connections for multiple systems

1. Enter ? in the TCP/IP Stack field on the Connection List Criteria panel.

A Stack List appears.

2. Select the stacks or servers for which you want to list and press Enter.

The Connection List Criteria panel appears with \*MULTIPLE\* in the field

**Note:** To view the criteria, including the individual stacks or servers, press F10 (ViewCrit).

3. Press F6 (Action).

The connection list appears with the word \*MULTIPLE\* at the top right of the panel.

## Display Connection Information

The Connection Information panel displays details of a selected connection.

### To display the Connection Information panel

1. Enter I next to a connection on a connection list.

The Connection Information panel appears.

### Example: Diagnose Slow Connection Response Time

A connection is exhibiting slow response time. To try to find out the cause of the problem, you enter I next to the connection. The displayed information can provide hints as to why the connection is slow, for example:

#### Fragmentation?

Indicates whether transferred packets are fragmented. If a packet is too large and becomes fragmented, it needs to be reassembled at the destination. The process of fragmentation and reassembly can contribute to poor response time.

#### Retransmissions

Displays the number of retransmissions. When packets are lost, the lost segment or segments are retransmitted. Retransmissions can contribute to poor response time.

#### Min/max window size

Displays the size of the buffer that is available to receive data. The size changes as data is moved into or out of the buffer. If the receiver advertises a window size of 0 (a closed window), it stops the data transfer. Closed windows can contribute to poor response time.

You find that some of the information warrants investigation at the packet level. For example, you want to find out which packets are fragmented. You can use [SmartTrace line commands](#) (see page 197) to trace the packets flowing through the connection.

#### More information:

[View a Trace](#) (see page 208)

[Diagnose Data- and Protocol-Related Problems in a Connection](#) (see page 86)

[Diagnose Telnet Response Time Problems](#) (see page 87)

[Diagnose Throughput of Data Transfers](#) (see page 88)

## Display AT-TLS Information

A connection can use AT-TLS. You can display the AT-TLS information such as policy rules.

### To display AT-TLS Information

1. Enter **TLS** next to a connection on a connection list.  
The information appears on a Command Entry panel.
2. Review the information. If you want to keep a copy of the information, press F4 (Print).
3. Press F3 to exit.  
You are returned to the connection list.

## Check for SNA Related Problems on Telnet Connections

Problems such as a lost connection or slow response times could be occurring in the SNA rather than the TCP/IP environment. To diagnose SNA problems, you can obtain SNA information about Telnet connections by using Network Control Services (NCS), a facility that provides full screen displays and navigation of the SNA network.

**Note:** For IBM TCP/IP stacks, you can also check all Telnet LUs by applying the CL action to an ASMON resource of Type TNSERVER (IBM Telnet server) on the IP Resource Monitor.

## Check the VTAM Status of an LU

Using NCS, you can access detailed status information, configuration, and active session data.

### To check the VTAM status of an LU

1. Enter **D** (VTAM Display) beside the appropriate connection on a Telnet connection list.  
The NCS : Resource Display appears or a basic VTAM display panel for the selected connection is presented by using an appropriate VTAM display command issued in the Command Entry facility.

## Analyze SNA Sessions

The NTS : Session List panel displays a list of SNA sessions for the LU associated with the selected Telnet connection. You can view a session summary, which includes the following information:

- Activation parameters
- Virtual route status
- Trace and configuration data
- CA SOLVE:Access MAI session visibility

Because the SNA session list includes historical information, you can view session start and end times, as well as error data.

**Note:** If your site is not configured with CA NetMaster NM for SNA, an appropriate error message is returned when you try to use the Session List action. If your site is configured with CA NetMaster NM for SNA, ensure you have set up the Network Tracking System (NTS).

## Display Session Summary

### To display the session summary

1. Enter **SL** (Session List) beside the appropriate connection on the TCP/IP : Telnet Connection list.

The NTS : Session List for the selected connection appears.

## Look Up a Device Name

Being able to associate a name with a host, rather than just a series of numbers (the IP address) can make the host easier to identify. For example, the real name of the host may give you information about where that host is located—although this depends on the naming standards used by your enterprise.

### To look up a device name

1. Enter **NL** beside the appropriate connection on the connection list.

The response appears on the third line of the connection list panel.

## Drop a Connection

Where an error condition exists (for example, the connection seems to have stalled), it may be necessary to drop that connection and have the user reconnect. You must have the appropriate security level to drop a connection.

### To drop a connection

1. Enter **Z** beside the connection on the connection list.  
A confirmation dialog appears.
2. Press Enter to confirm.  
A message informing you that the connection has been dropped appears, and the connection is highlighted as having been dropped.

## Diagnose Data- and Protocol-Related Problems in a Connection

Data moves around the TCP/IP network in the form of IP packets. You use the packet trace facility to diagnose data- and protocol-related problems over the TCP/IP network.

If you are experiencing a problem such as an unexpected disconnection, you can activate IP packet tracing.

**Note:** This facility can be used with TCPaccess and IBM TCP/IP only. It is not available for Cisco channel cards.

You can trace connections by issuing [SmartTrace line commands](#) (see page 197). Use the PT command to start a trace and the PTI command to stop a trace.

You can also list the started traces from the TCP/IP : Packet Tracing Menu.

When you use packet tracing on the TCP/IP : Telnet Connection List, the packet trace is always performed on the IP address in the Foreign Host column.

If there is no Foreign Host IP address, the packet trace is performed on the local port number (for example, in the case of UDP or Listen entries).

## Diagnose Telnet Response Time Problems

By providing an evaluation of the components that make up a user's response time, the Telnet Transaction Path Analyzer lets you diagnose response time problems. The response time components that it evaluates are:

- IP network
- Telnet server
- SNA network
- Application

To provide this evaluation, the Transaction Path Analyzer performs the following actions:

- Monitor the IP network for the client.
- Check the responsiveness of the Telnet server.
- (CA NetMaster NM for SNA required) Monitor the SNA session for application and network response time.

## View End-to-End Response Times

By providing a view of end-to-end response times, the Telnet Transaction Path Analyzer supports the diagnosis of network and system performance.

### To use the Telnet Transaction Path Analyzer

1. Enter **TPA** next to a connection on a Telnet connection list.

The Telnet Transaction Path Analysis panel appears for the selected connection.

## Telnet Transaction Path Analysis Messages

Messages are displayed on the Telnet Transaction Path Analysis panel to show the status of actions performed. An example is:

```
IPGP1212 PING hubble.dept.company.com(10.16.80.25): TIME=3/3/4 MS
```

Old messages scroll as new messages are received. To view all messages, press F7 (Log).

## Session Awareness Messages

Examples of session awareness messages available after pressing F5 to start monitoring sessions are:

```
IPSM0107 COMP1 <-- SDTCP042 TERMINAL RESPONSE, NETWORK PATH TIME 0.002s.  
IPSM0105 COMP1 --> SDTCP042 APPLICATION SEND, RESPONSE TIME N/A, OPERATION WRIT  
IPSM0106 COMP1 <-- SDTCP042 TERMINAL INPUT, KEY PF03, LENGTH 3.  
IPSM0105 COMP1 --> SDTCP042 APPLICATION SEND, RESPONSE TIME 0.535s, OPERATION W
```

## Diagnose Throughput of Data Transfers

By providing an evaluation of the characteristics that make up IP connections, the Transaction Path Analyzer lets you diagnose any throughput problems of data transfers. The characteristics that it evaluates are:

- The average data transfer rate between the IP server and IP client for the elapsed time from timed samples
- Response time
- Hop length
- Alert indicator

## View End-to-End Throughput

By providing a view of end-to-end throughput times, the Transaction Path Analyzer supports the diagnosis of network and system performance.

### To use the Transaction Path Analyzer

1. Enter **TPA** next to a connection on a general connection list.

The Transaction Path Analysis panel appears for the selected connection.

**Note:** The TPA action is not allowed on connections that do not have a foreign host, as indicated by the asterisk (\*) in the Foreign Host column of any connection list.



# Chapter 5: Managing Alerts

---

This section contains the following topics:

[Alerts](#) (see page 89)

[Alert Monitor](#) (see page 90)

[Access the Alert Monitor](#) (see page 90)

[Sort Alerts](#) (see page 91)

[Filter Alerts](#) (see page 91)

[Change the Display Format](#) (see page 91)

[Change the Alert Monitor Profile Using the User Profile Menu](#) (see page 92)

[How to Work with Alerts](#) (see page 92)

[Display Alert Details](#) (see page 93)

[Access the Transient Log from the Alert Monitor](#) (see page 93)

[Raise a Trouble Ticket for an Alert](#) (see page 94)

[Add Operator Notes to an Alert](#) (see page 94)

[Close Alerts](#) (see page 95)

[Display Alert History](#) (see page 95)

## Alerts

Alerts provide proactive notification of performance-related network events. An alert can optionally be raised if a monitored attribute exceeds a user-specified threshold value or the calculated baseline, and is automatically closed when the threshold is no longer exceeded.

Alerts are also raised by event detectors when a particular event occurs, for example, the availability of a listener port or the occurrence of an FTP failure.

**Note:** For information about defining monitoring thresholds and event detectors, see the *Implementation Guide*.

## Alert Monitor

The Alert Monitor provides an integrated, correlated event notification system that indicates to operators that a problem has occurred and that some action needs to be taken. Such alerts, known as active alerts, are displayed on the Alert Monitor.

The Alert Monitor refreshes your screen each time an alert arrives. The clock in the title line indicates when the screen was refreshed last.

The title line of the Alert Monitor includes a total indicator, which shows the total number of alerts and the total number of alerts of each severity level. For example, (43: 5 23 8 7) means that there are a total of 43 alerts, comprising 5 severity one, 23 severity two, 8 severity three, and 7 severity four. Each severity level appears in a different color. The following illustration shows an example:

```
PROD1 (23.53.32)----- Alert Monitor (43: 5 23 8 7 ) -----Link: *MULTIPLE*
Command ==>                                     scroll ==> PAGE

          S/B=Browse T=Track N=Notes A=Analyze TT=TroubleTicket C=Close ?=More
Time      Description                                Resource                                Track
23 51 27  IPNODE: RINGRTT 261 ms 48% below HOBO VAL CL 02
```

The Alert Monitor can initiate actions such as starting recovery procedures and creating trouble tickets, either automatically or manually.

In a multisystem environment, you can monitor active alerts from all linked regions in a focal point region. You can monitor only local active alerts in a subordinate region.

Alerts that were raised before the region was shut down are not displayed on the Alert Monitor when the region restarts, but are displayed on the Alert History panel. The alert history contains information about all alerts.

## Access the Alert Monitor

The Alert Monitor lets you know of problems that have occurred in your environment. You can then take appropriate action based on the alert information.

### To access the Alert Monitor

1. Enter **/ALERTS** at the prompt.

The monitor appears displaying any alerts.

You can also access the Alert Monitor by issuing the AL command against a resource from a resource monitor. The monitor displays the alerts for that resource.

## Sort Alerts

Alerts are color coded by severity. They are sorted in order of severity, then time—the most severe alerts are listed first, then, in each category of severity, the most recent of the alerts are listed first.

To change the sort order, use the **SORT** command.

To list the column fields by which you can sort, enter **SORT ?**.

## Filter Alerts

You can restrict the alerts displayed by using filters. When you apply a filter, the filter name appears on the right of the Alert Monitor and the totals in the title line reflect the number of alerts displayed under the filter.

To filter alerts, enter the following command at the command prompt:

```
FILTER filter_name
```

To remove the applied filter, enter **FILTER NONE**.

**Note:** To display a selection list of filters, enter **FILTER**.

## Change the Display Format

Display format determines what and in what order information columns are displayed.

To change the alert monitor format, enter the following command at the command prompt:

```
FORMAT format_name
```

To return to the default format, enter **FORMAT DEFAULT**.

**Note:** To display a selection list of formats, enter **FORMAT**.

## Change the Alert Monitor Profile Using the User Profile Menu

### To change your alert monitor profile using the User Profile Menu

1. Enter **=U.UP** from any panel.  
The Panel Display List appears.
2. Enter **S** beside Alert Monitor Profile.  
The Alert Monitor Profile panel appears.
3. Complete the following fields:

#### **Monitor List Filter**

Specifies the name of the default filter.

#### **Monitor List Format**

Specifies how and what is displayed.

#### **Alert Sort Criteria**

Specifies the order in which the alerts are displayed.

Press F3 (File).

The changes to your user profile are saved.

## How to Work with Alerts

The Alert Monitor displays the alert when it arrives. An alert can be closed automatically by the region (when it recognizes that the problem that caused the alert no longer exists) or manually by the operator. When an alert is closed, it is removed from the active alert monitor. However, it is still accessible from the Alert History panel.

Typically, when an alert arrives, do this:

1. Enter **B** (Browse) beside the alert to find out whether any suggested recommended actions are provided.
2. Enter **A** (Analyze) beside the alert to diagnose it. Diagnosis displays additional information for some alerts.
3. Enter **T** (Track) beside the alert to indicate to other users that you will be working on it. Your user ID is displayed in the Track column.
4. Perform any necessary actions to remove the alert condition. For information about actions, press F1 (Help).
5. Enter **N** (Notes) beside the alert to view or record notes that provide future reference information about this alert in the alert definition.
6. Enter **C** (Close) beside the alert after the alert condition is resolved.

## Display Alert Details

The Alert Display describes an active alert and provides information about its generation time and its identity. An alert comes with the following information:

- General information such as severity level, the source of the alert, update history, and number of occurrences
- Possible causes of the alert and any recommended actions

### To display the Alert Display

1. Enter **B** or **S** beside an alert on the Alert Monitor panel.

The Alert Display appears.

**Note:** For information about the fields, press F1 (Help).

## Print Alert Details

### To print details about the displayed alert

1. Enter **PRINT** at the command prompt.

The Confirm Printer panel appears.

2. Specify your printing requirements, and then press F6 (Confirm).

The details are sent to the printer.

## Access the Transient Log from the Alert Monitor

If a monitored resource generates an alert, you can access the corresponding transient log for the affected resource from the Alert Monitor.

### To access the transient log

1. Enter **TL** beside the alert.

The transient log appears.

## Raise a Trouble Ticket for an Alert

If your system administrator has implemented the interface for raising a trouble ticket, you can request a trouble ticket as defined to your region.

**Note:** For information about how to implement the trouble ticket interface, see the *Administration Guide*.

### To raise a trouble ticket

1. Enter **TT** next to the alert.  
The Alert Monitor : Trouble Ticket Details panel appears.
2. Enter the details of the trouble ticket and press F6 (Confirm).  
The trouble ticket is raised.

## Add Operator Notes to an Alert

You can add notes to an alert for future reference. For example, you may want to leave the next operator some notes about an alert that has not been closed. Notes are also added automatically to provide a history of the actions performed on the alerts.

When an alert is closed, the severity and description of the alert are added to the notes so that you can easily identify which alert has been closed. When an alert severity changes, the description is added to the alert notes.

### To add notes to an alert

1. Enter **N** beside the alert.  
The Alert Notes panel appears.
2. Press F4 (Add).  
The panel becomes editable.
3. Enter your notes about the alert, and press F3 (File) when you have finished.  
The notes are saved with the alert.

**Note:** For information about how to use the editor, see the online help.

## Close Alerts

Alerts can be closed automatically by the region or manually.

For example, an alert might be generated because a monitoring threshold is exceeded. When the condition is corrected, the alert is closed automatically. Another alert might be a reminder alert and needs to be closed manually.

### To close an alert

1. Enter **C** beside the alert.

The alert is closed.

### To close multiple alerts

1. Enter **CLOSE** at the Command prompt.

The Valid Value List panel appears.

2. Select ALL to close all displayed alerts or a severity level to close alerts with that level.

The Command Confirm panel appears.

3. Press F6 (Confirm).

The targeted alerts are closed and removed from the monitor.

## Display Alert History

The alert history lists all alerts, both active and closed, that occurred during a predefined period.

### To view the alert history

1. Press F4 (History) from the alert monitor.

The alerts for the current date appear. If you want to display the alerts for the other dates, use the DATE command (for example, DATE *yyymmdd*).

**Note:** For more information about the command, see the online help.

2. (Optional) Enter **N** beside an alert to view the history of actions performed on it.

The Alert Notes panel appears.

**Note:** The length of time an alert is kept in the alert history log is set by your administrator.





# Chapter 6: Managing IP Nodes

---

This section contains the following topics:

[IP Node Monitor](#) (see page 97)

[Interpret the Status of IP Nodes](#) (see page 98)

[Use IP Node Commands](#) (see page 99)

[Packet Tracing](#) (see page 99)

[Intensive Monitoring](#) (see page 100)

[Performance History](#) (see page 101)

[MIBinsight Browser](#) (see page 101)

## IP Node Monitor

The IP Node Monitor lets you monitor specific IP nodes on a regular basis.

The IP node is associated with a host name or IP address, and is specified for monitoring. The resolved IP address is then polled at regular intervals for the values you are interested in.

Usually this includes a ping with the following results:

- If the ping is successful, the displayed device status indicates the device is reachable.
- If the ping is unsuccessful, the displayed device status indicates that it cannot be reached.

Individual users can use filters to select which IP Nodes are displayed. The monitor displays the resources selected by the filter. The filter name is shown on the title line of the monitor panel. The IP Node Monitor uses the IPNODE filter by default.

## Access the IP Node Monitor

You manage your IP nodes from the IP Node Monitor.

### Follow these steps:

1. Enter **/IPNODE** at the prompt.

The IP Node Monitor appears.

```

PROD----- IP Node Monitor -----LPAR1-0002
Command ==>                               Scroll ==> PAGE

      P=Ping TR=TraceRte TN=Telnet RT=Routing Table SI=System Info ?=List Cnds
      Max .-Last Ping-. Next Ovr
IP Node Name  Host Name      Status  Sev Avg Max Time Samp
SS1.CO.COM    ss1.co.com      Ok      -  0  1  21:39 21:49
USIL1.CO.COM  usil100.co.com  Ok      -  3  9  21:39 21:49
USIL2.CO.COM  usil100.co.com  Ok      -  3  9  21:39 21:49
USIL3         usil164.co.com  Ok      -  3  9  21:39 21:49
USI14         xe6losa.co.com  Ok      -  1  1  21:39 21:49
XE09          huh-1.co.com    Ok      - 18 21 21:39 21:49
172.16.255.255 usil10.co.com  Ok      -  0  1  21:39 21:49

F1=Help      F2=Split      F3=Exit      F4=Add      F5=Find
F7=Backward  F8=Forward    F9=Swap      F11=Right

```

**Note:** The format of the IP Node Monitor can be tailored to your requirements.

## Interpret the Status of IP Nodes

Use the following table to determine the status of monitored resources and nodes:

| Monitoring Status  | Actual State | No Outstanding Alerts | Maximum Alert Severity (1) | Maximum Alert Severity (2) | Maximum Alert Severity (3) | Maximum Alert Severity (4) |
|--------------------|--------------|-----------------------|----------------------------|----------------------------|----------------------------|----------------------------|
| Ok/Active          | ACTIVE       | OK - Green            | AlertSev1 - Red            | AlertSev2 - Yellow         | AlertSev3 - Pink           | AlertSev4 - Blue           |
| SNMPErrors/Timeout | DEGRADED     | MonError - Turquoise  | MonError - Turquoise       | MonError - Turquoise       | MonError - Turquoise       | MonError - Turquoise       |
| NoAttr/Unknown     | UNKNOWN      | Unknown - White       | Unknown - White            | Unknown - White            | Unknown - White            | Unknown - White            |
| Error/Failed       | DEGRADED     | MonFailed - Red       | MonFailed - Red            | MonFailed - Red            | MonFailed - Red            | MonFailed - Red            |

| Monitoring Status | Actual State | No Outstanding Alerts | Maximum Alert Severity (1) | Maximum Alert Severity (2) | Maximum Alert Severity (3) | Maximum Alert Severity (4) |
|-------------------|--------------|-----------------------|----------------------------|----------------------------|----------------------------|----------------------------|
| -                 | INACTIVE     | Attention - Pink      | Attention - Pink           | Attention - Pink           | Attention - Pink           | Attention - Pink           |

## Use IP Node Commands

To view the commands available on the IP Node Monitor, enter **?** next to an IP node name.

A panel appears, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to IP nodes appear first (displayed in turquoise), followed by other relevant commands.

To execute a command, enter **S** next to it.

**Note:** To list all the commands, enter **??** beside an IP node resource.

If you know the command, you can enter it next to the node directly.

## Packet Tracing

You can trace packets between your system and the IP nodes by issuing [SmartTrace line commands](#) (see page 197) beside the IP node that you want to diagnose. For example, you can issue the PT command to start a trace. When a trace is active, a T appears in the Ovr column.

The PT command lets you specify optional criteria to limit the trace. It also lets you specify whether you want to create a separate trace for each new connection during the current tracing session.

You can list the started traces from the TCP/IP : Packet Tracing Menu.

**More information:**

[Using SmartTrace](#) (see page 195)

## Intensive Monitoring

When you are diagnosing a problem, you may want to change the sampling interval to less than five minutes (the normal minimum interval). To do this, you can apply intensive monitoring mode for a specified period.

### Apply Intensive Monitoring Mode to an IP Node

#### To apply intensive monitoring mode to an IP node

1. Enter **IMM** next to a node name on the IP Node Monitor.

The TCP/IP: Intensive Monitoring Mode panel appears.

2. Complete the following fields:

##### **Name**

Specifies the name of the attribute to be intensively monitored.

##### **Sampling Interval**

Specifies the intensive sample time required (minimum 15 seconds; maximum Duration of Sample, or one second less than the current rate for the selected attribute, whichever is smaller).

##### **Intensive Mode Duration**

Specifies the period for which intensive monitoring mode is applied (minimum one minute; maximum 30 minutes).

Press F6 (Confirm).

A confirmation message appears and X appears in the Ovr column of the selected IP node.

### Reset Intensive Monitoring Mode for an IP Node

Use the IMR command to reset intensive monitoring mode for an IP node. This command sets the selected node's sampling rate (for all attributes) back to the group attribute rate.

#### To reset intensive monitoring mode for an IP node

1. Enter **IMR** next to a node name on the IP Node Monitor.

A confirmation message appears.

2. Press Enter.

Intensive monitoring mode is reset for the selected IP node and X is cleared from the Ovr column.

## Performance History

Your region stores performance history data for IP nodes that are being monitored for up to the last 70 days. You can view this data in a variety of formats by issuing line commands against a resource on the IP Node Monitor.

**More information:**

[Performance History](#) (see page 275)

## MIBinsight Browser

MIBinsight lets you display the SNMP MIBs for an IP node. You can access the MIBinsight browser from the IP Node Monitor by issuing the MIB line command.

**More information:**

[Using MIBinsight](#) (see page 263)



# Chapter 7: Managing IP Resources

---

This section contains the following topics:

[Features That Help You Manage Your IP Resources](#) (see page 103)

[IP Resource Monitor](#) (see page 106)

[Interpret the Status of IP Resources](#) (see page 107)

[Use IP Resource Commands](#) (see page 108)

[Add a Resource](#) (see page 108)

[Packet Tracing](#) (see page 108)

[Performance History](#) (see page 108)

## Features That Help You Manage Your IP Resources

Two main features are available to help you manage the IP resources defined in your regions: monitor commands and menus.

For general monitoring, you can use the IP Resource Monitor (/IPMON shortcut), which gives you at-a-glance view of the status of the monitored resources. When the status of a resource indicates problems, you can use commands to get more information and perform diagnosis.

If you know the specific resources, you can work with them using menus. The Network Diagnosis : Primary Menu (/DIAG shortcut) has options that let you access the various types of resources.

**Example: Get Traffic Information About a TCP/IP Stack Using the IP Resource Monitor**

The IP Monitor indicates that the TCPIP01 STACK-class resource is not in its normal state. You want to find out whether excessive traffic is causing the problem.

The TRS command lets you display the most recent traffic statistics on a stack. You enter the command against TCPIP01 and select the type of statistics you want.

```

COMP44----- IP Resource Monitor -----C011-0001
Command ==>                                Scroll ==> CSR

      S=Info H=Performance History OV=Performance Overview AL=Alerts ?=List Cnds
Resource Class System Actual Status Count Sev Max Last Next
TRS TCPIP01  STACK  CA11  ACTIVE  Ok      12  2  00:10 00:15
   TCPIP111  STACK  CA11  INACTIVE -       0  -  00:10 00:15
   TCPIP11A  STACK  CA11  DEGRADED SNMPErr 1   1  00:10 00:15

```

The following result shows traffic by application:

| Application  | End Time | ---Bytes--- |       | --Stack%-- |     | --Packets-- |      | --Stack%-- |     |
|--------------|----------|-------------|-------|------------|-----|-------------|------|------------|-----|
|              |          | In          | Out   | In         | Out | In          | Out  | In         | Out |
| ARCVTS20     | 02.09    | 116         | 1536  | 0%         | 0%  | 2           | 2    | 0%         | 0%  |
|              | 02.08    | 116         | 1536  | 0%         | 0%  | 2           | 2    | 0%         | 0%  |
|              | 02.07    | 116         | 1536  | 0%         | 0%  | 2           | 2    | 0%         | 0%  |
|              | 02.06    | 232         | 3072  | 0%         | 1%  | 4           | 4    | 0%         | 0%  |
|              | 02.05    | 116         | 1536  | 0%         | 0%  | 2           | 2    | 0%         | 0%  |
| CCI-Appls    | 02.09    | 25605       | 45838 | 3%         | 11% | 115         | 149  | 5%         | 7%  |
|              | 02.08    | 37644       | 76116 | 3%         | 1%  | 153         | 212  | 2%         | 2%  |
|              | 02.07    | 47801       | 127K  | 7%         | 23% | 273         | 318  | 12%        | 13% |
|              | 02.06    | 43749       | 96088 | 6%         | 26% | 211         | 261  | 10%        | 12% |
|              | 02.05    | 120K        | 3.14M | 13%        | 90% | 1586        | 2587 | 39%        | 53% |
| CCI-Appls II | 02.09    | 161         | 357   | 0%         | 0%  | 1           | 2    | 0%         | 0%  |
|              | 02.08    | 1142        | 11642 | 0%         | 0%  | 15          | 17   | 0%         | 0%  |
|              | 02.07    | 622         | 1640  | 0%         | 0%  | 5           | 5    | 0%         | 0%  |

**Example: Get Information About a TCP/IP Stack Using Menus**

A user raises an issue that the CCI-Appls application is slow. You want to find out whether excessive traffic is causing the problem.



The B - IP Business Applications option (/BIZ) on the Network Diagnosis : Primary Menu displays the Business Applications menu, from which you can select the TRS option to display the most recent traffic statistics by application:

```

COMP44----- Network Diagnosis : Primary Menu -----/DIAG
Select Option ==> B

  C - Connections (IP, Telnet, UDP, EE)      IPCON   Userid USER01
  N - IP Diagnosis (Ping, Traceroute, MIB)   IPDIAG   LU      NMF11025
  TR - Advanced Packet Tracing (SmartTrace, CTRACE) SMART   Time  00.22.23
  ST - Stacks                               STACK    MON 27-AUG-2007
  I - Stack Interfaces and Device Links      DEVLINK
  A - Address Spaces and Ports              ASMON
  O - OSA                                   OSA
  V - VIPA                                  VIPA
  EE - Enterprise Extender                  EE
  H - APPN/HPR and RTP                      APPNHPR
  CR - CIPS and Routers                     CIP
  B - IP Business Applications              BIZ
  LP - Line Printers                        LPD
  E - Help Messages and Error Codes         CODES
  X - Exit

```

```

COMP44----- TCP/IP : Business Applications -----/BIZ
Select Option ==> TRS

  TRS - Traffic for All Applications
  H   - Connection Workload Performance History
  OV  - Performance Overview and Baselines
  A   - List and Define Business Applications
  X   - Exit

System ...+ C011      ( Required TRS H OV )

```

| APPLICATION       | End<br>Time | ---Bytes--- |       | --Stack%-- |     | --Packets-- |     | --Stack%-- |     |
|-------------------|-------------|-------------|-------|------------|-----|-------------|-----|------------|-----|
|                   |             | In          | Out   | In         | Out | In          | Out | In         | Out |
| TCPIP01-CCI-Appls | 02.38       | 33340       | 122K  | 3%         | 14% | 212         | 261 | 7%         | 8%  |
|                   | 02.37       | 36158       | 76420 | 2%         | 15% | 154         | 203 | 7%         | 8%  |
|                   | 02.36       | 32350       | 66189 | 2%         | 14% | 139         | 187 | 5%         | 7%  |
|                   | 02.35       | 24436       | 62636 | 1%         | 10% | 120         | 175 | 5%         | 7%  |
|                   | 02.34       | 36998       | 78216 | 2%         | 12% | 154         | 207 | 5%         | 7%  |

**Note:** If you know the stack that the application is using, you can also get the information through the ST (Stacks) option on the Network Diagnosis : Primary Menu, which takes you to a menu for STACK-class resources.

## IP Resource Monitor

IP resources in or adjacent to your local LPAR can be managed from the IP Resource Monitor.

The IP resources to be monitored are defined in a system image. When you start the region, the system image is loaded automatically and the resources in the image are visible on the IP Resource Monitor.

Individual users can use filters to select which resources are displayed. The monitor displays the resources selected by the filter. The name of the user-selected filter is shown on the title line of the monitor panel.

**Note:** The IP Resource Monitor uses the IPRSC filter when you first access the monitor. If the title line does not identify a filter, the monitor is using the IPRSC filter.

In a multisystem environment, resources and nodes from all linked regions are, by default, visible on the monitors in any focal region. You can manage all resources or nodes from a central Resource Monitor.

### More information:

[Using Monitors](#) (see page 337)

[Managing Stacks](#) (see page 111)

[Managing Open Systems Adapters](#) (see page 127)

[Managing Cisco Channel Cards](#) (see page 133)

[Managing Enterprise Extender](#) (see page 145)

[Managing APPN/HPR Resources](#) (see page 157)

[Managing VIPA Resources](#) (see page 167)

[Managing Address Spaces](#) (see page 173)

[Managing CSM Resources](#) (see page 179)

[Managing CICS Resources](#) (see page 181)

## Access the IP Resource Monitor

You manage your IP resources from the IP Resource Monitor.

### To access the IP Resource Monitor

1. Enter **/IPMON** at the prompt.

The IP Resource Monitor appears.

|  |            |         |          |                 |       |     |       |       |     |
|--|------------|---------|----------|-----------------|-------|-----|-------|-------|-----|
| PROD----- IP Resource Monitor -----LPAR1-0002                              |            |         |          |                 |       |     |       |       |     |
| Command ==>  |            |         |          | Scroll ==> PAGE |       |     |       |       |     |
| S=Info H=Performance History OV=Performance Overview AL=Alerts ?=List Cnds |            |         |          |                 |       |     |       |       |     |
| Monitor Alert Max Last Next  |            |         |          |                 |       |     |       |       |     |
| Resource   | Class      | System  | Actual   | Status          | Count | Sev | Samp  | Samp  | Ovr |
| QA22Q6   | STACK      | CA31    | ACTIVE   | Ok              | 1     | 2   | 21:39 | 21:49 |     |
| QA24Q6   | STACK      | CA31    | ACTIVE   | Ok              | 1     | 2   | 21:39 | 21:49 |     |
| QA25P6   | STACK      | CA31    | ACTIVE   | Ok              | 1     | 2   | 21:39 | 21:49 |     |
| OSA-01   | OSA        | CA31    | ACTIVE   | Ok              | 0     | -   | 21:34 | 21:49 |     |
| OSA-02   | OSA        | CA31    | ACTIVE   | Ok              | 0     | -   | 21:34 | 21:49 |     |
| OSA-27   | OSA        | CA31    | INACTIVE | -               | 0     | -   | 21:34 | 21:49 |     |
| F1=Help  | F2=Split   | F3=Exit | F4=Add   | F5=Find         |       |     |       |       |     |
| F7=Backward  | F8=Forward | F9=Swap |          |                 |       |     |       |       |     |

**Note:** The format of the IP Resource Monitor can be tailored to your site's requirements. Your IP Resource Monitor may not look the same as the one shown here. For more information, press F1 (Help).

## Interpret the Status of IP Resources

Use the following table to determine the status of monitored resources and nodes:

| Monitoring Status | Actual State | No Outstanding Alerts | Maximum Alert Severity (1) | Maximum Alert Severity (2) | Maximum Alert Severity (3) | Maximum Alert Severity (4) |
|-------------------|--------------|-----------------------|----------------------------|----------------------------|----------------------------|----------------------------|
| Ok/Active         | ACTIVE       | OK - Green            | AlertSev1 - Red            | AlertSev2 - Yellow         | AlertSev3 - Pink           | AlertSev4 - Blue           |
| SNMPError/Timeout | DEGRADED     | MonError - Turquoise  | MonError - Turquoise       | MonError - Turquoise       | MonError - Turquoise       | MonError - Turquoise       |
| NoAttr/Unknown    | UNKNOWN      | Unknown - White       | Unknown - White            | Unknown - White            | Unknown - White            | Unknown - White            |
| Error/Failed      | DEGRADED     | MonFailed - Red       | MonFailed - Red            | MonFailed - Red            | MonFailed - Red            | MonFailed - Red            |
| -                 | INACTIVE     | Attention - Pink      | Attention - Pink           | Attention - Pink           | Attention - Pink           | Attention - Pink           |

## Use IP Resource Commands

To view the commands available on the IP Resource Monitor, enter **?** next to an IP resource name.

A panel appears, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to IP resources appear first (displayed in turquoise), followed by other relevant commands.

To execute a command, enter **S** next to it.

**Note:** To list all the commands, enter **??** beside an IP resource.

If you know the command, you can enter it next to the resource directly.

## Add a Resource

To add a resource directly from the monitor, press F4 (Add).

## Packet Tracing

You can trace connections for certain resources by issuing [SmartTrace line commands](#) (see page 197) beside the resource that you want to diagnose. Use the PT command to start a trace, the PTV command to view a trace, and the PTI command to stop a trace. When a trace is active, a T appears in the Ovr column.

You can also list the started traces from the TCP/IP : Packet Tracing Menu.

**More information:**

[Using SmartTrace](#) (see page 195)

## Performance History

Your region stores performance history data for resources that are being monitored for up to the last 70 days. You can view this data in a variety of formats by issuing line commands against a resource on the IP Resource Monitor.

**More information:**

[Performance History](#) (see page 275)





# Chapter 8: Managing Stacks

---

This section contains the following topics:

[TCP/IP Stack Support](#) (see page 111)  
[Display TCP/IP Stacks](#) (see page 111)  
[Packet Tracing](#) (see page 112)  
[Display Stack Performance](#) (see page 112)  
[Issue Console Commands](#) (see page 115)  
[Display Device Links](#) (see page 115)  
[CA TCPAccess CS Parameters Library](#) (see page 118)  
[IBM Configuration Data Sets](#) (see page 120)  
[Change Configuration Using Obeyfile Data Sets](#) (see page 121)  
[Display Workload Manager Status](#) (see page 123)  
[List Remote Addresses](#) (see page 124)  
[Display Address Space Activities](#) (see page 125)

## TCP/IP Stack Support

Your product monitors the following TCP/IP stacks:

- IBM's Communications Server
- CA TCPAccess CS

## Display TCP/IP Stacks

You can use the IP Resource Monitor to display information about TCP/IP stacks.

TCP/IP stacks are shown as class STACK.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to a STACK resource](#) (see page 108) to perform various functions.

If you know the specific stacks you want to manage, you can also work with them using the Stack Management menu. The menu shortcut is **/STACK**.

## Packet Tracing

You can trace packets on stacks from the IP Resource Monitor by issuing [SmartTrace line commands](#) (see page 197) beside the stack that you want to diagnose. Use the PT command to start a trace, the PTV command to view a trace, and the PTI command to stop a trace. When a trace is active, a T appears in the Ovr column.

**More information:**

[Using SmartTrace](#) (see page 195)

## Display Stack Performance

The IP Resource Monitor lets you display the following types of performance data for a TCP/IP stack:

- Performance history (from the most recent samples to samples up to the last ten weeks)
  - Connection, Telnet, and FTP workload
  - Stack network interface
  - IP, TCP, and UDP activity
  - Stack address space and ports
- IP, TCP, and UDP activity (current snapshot)
- IP traffic statistics, including byte and packet throughput (from the last 5 minutes to the last hour)



## Display Performance History

History panels let you monitor the performance and health status of a stack.

**Follow these steps:**

1. Enter *one* of the following commands next to a stack entry on the IP Resource Monitor:

- WC for stack connection workload performance
- WT for stack Telnet workload performance
- WF for stack FTP workload performance
- WI for stack network interface performance
- IP for stack IP, TCP, and UDP performance
- H for stack address space and port performance

The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.

2. Enter *one* of the following actions beside an attribute for more details:

- D lists the samples
- S displays the Hourly Summary Graph
- H displays the Hourly Summary List
- DL displays the Daily Summary List
- W displays the Weekly Interval List

Press F5 (Overview) to compare this resource with others on the system.

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.

## Display IP, TCP, and UDP Activity Summary

You can display a summary of IP, TCP, and UDP activities on a stack.

### To display the summary

1. Enter **IPM** next to a stack entry on the IP Resource Monitor.

The summary appears containing statistics on IP, TCP, and UDP activities. This summary is a snapshot taken at the time of the request.

## Display IP Traffic Statistics

You can display the most recent IP traffic statistics for a stack.

### Follow these steps:

1. Enter **TRS** (Display IP Traffic Statistics) next to a STACK class resource on the IP Resource Monitor.

The Traffic Statistics Selection List appears.

2. Enter **S** next to the type of statistics you want to view.

The Traffic Statistics panel appears.

### Example: IP Traffic Statistics for Local TCP Ports

For Local TCP Ports, the Traffic Statistics panel shows the following information:

- TCP connections statistics
- Number of packets and bytes sent and received in the last minute, last 5 minutes, and last hour
- Total number of packets and bytes sent and received after Packet Analyzer starts to collect data
- Number of connections by duration

To see the packet and byte throughput as a percentage of the total traffic for the stack, enter **S** next to a port.

To list the active connections, enter **C** next to a port.

## Issue Console Commands

You can issue a MODIFY command against the TCP/IP job and see the responses to the command. Both solicited and unsolicited messages from the TCP/IP job are displayed.

### To issue console commands

1. Enter **CMD** (Issue Modify to Stack) next to a stack entry on the IP Resource Monitor.  
The Stack Commands panel appears.

2. Enter a command at the command prompt.

For example, enter **D TCPIP,,HELP** in this field to issue a help command.

This command is issued as a SYSCMD. The Stack Commands panel displays messages as this command is processed.

For information about the input fields and the actions available, press F1 (Help).

## Display Device Links

If you are unable to get any connections through the TCP/IP network or through a particular interface to the TCP/IP network, you may want to check the device links in an attempt to isolate the cause of the problem.

### To display device links

1. Enter **DL** (Display Device Links) next to a stack on the IP Resource Monitor.  
The TCP/IP Device Links List appears.

## Device Links Graphic Display

The TCP/IP : Device Links graphic display is organized in the following layers:

- TCP/IP stack
- Devices
- Links and interfaces

### TCP/IP Stack Layer

The first layer represents the TCP/IP software running on this system.

## Device Layer

The second layer represents the devices used by TCP/IP to interface to the TCP/IP network. Each box in this layer contains information like the following for a device:

- Device name
- Channel protocol type (for example, LCS, CLAW, or CTC)
- Device status
- Channel address
- Channel path status (ONLINE or OFFLINE)
- An error message if applicable
- Send queue size
- MAC address of the device
- Number of packets received
- Number of packets sent

**Note:** The information varies, depending on the type of device.

If the error message PATH ERROR or CHP ERROR appears for a device, there is an error in the path or the channel path. To investigate this error, use the operating system command: D M=DEV(*devAddress*).

If the error message ERROR STATUS appears for a device, there is a configuration error.

**Note:** To investigate this error, see the installation chapter in the *Installation Guide* for CA TCPaccess CS.

If the device is running in 3172 offload mode, the word offload appears.

SNA link devices display an LU name.

## Link and Interface Layer

The third layer represents the links and interfaces that a stack uses to interface to the TCP/IP network. Each box in this layer includes the following details (if applicable) for each link:

- Link name
- Status
- IP address
- Network address
- Network mask
- Subnet address
- Subnet mask
- Maximum Transmission Unit (MTU) size
- Number of packets that are received per hour and number of packets that are sent per hour

**Note:** This information is available only if monitoring of the network interface for the stack is set as active in its definition. For more information, see the *Implementation Guide*.

## Display Device Links Graphically

### To view a graphic display of the TCP/IP interfaces

1. Press F4 (GrphDisp) at the TCP/IP Device Links List.

The TCP/IP : Device Links panel appears.

**Note:** Alternatively, you can enter **DG** beside a stack name on the IP Resource Monitor.

## Display Device Links Information

From the Device Links List panel, you can find out the following information about an interface or link:

- Which applications are using the interface or link
- Traffic statistics

For an interface or link of the VIPADefine type, you can find out about the VIPA status in the sysplex. If the VIPA is a sysplex distributor, the information includes connection statistics and weighting.

You can also find out the routes involving an interface or link.

To display device links information from Device Links List, enter an action code next to the interface or link, for example:

- Enter **S** (Show Information) next to the interface or link for which you want to display information.

The device links information appears.

- Enter **R** next to an interface or link.

The Routing Table List appears listing the paths on that interface or link.

## CA TCPaccess CS Parameters Library

The CA TCPaccess CS parameters library contains all the configuration file members that provide parameters for the various task groups in CA TCPaccess CS.

### Browse the CA TCPaccess CS Parameters Library

#### To browse the TCPACCESS.PARMS data set

1. Enter **DP** (Display Parms Library (TCPACCESS.PARMS)) beside a CA TCPaccess CS STACK entry on the IP Resource Monitor.

The TCP/IP : Command Input Fields panel appears.

2. Enter the name of your CA TCPaccess CS Parameters Library data set in the Dataset field and press F6 (Action).

The TCPaccess Parameters Library List panel appears.

## Browse a PARMS Member

### To browse a TCPaccess PARMS member

1. Enter **S** or **B** (Browse) beside the PARMS member on the TCPaccess Parameters Library List.

The Browse TCPaccess PARMS Dataset panel appears.

## Change a PARMS Member

### To change a PARMS member

1. Press F4 (Edit) from the Browse TCPaccess PARMS Dataset panel.

The Edit TCPaccess PARMS Dataset panel appears.

**Note:** If you are at the TCPaccess Parameters Library List panel, you can edit a member by entering **E** (Edit) beside a member name to display the Edit TCPaccess PARMS Dataset panel.

2. Edit the member, as required.
3. Press F4 (Save).

The changes are saved.

## Create a New Member of a PARMS Data Set

### To create a new member of a PARMS data set

1. Enter **E** *uniquemembername* or **EDIT** *uniquemembername* at the prompt on the TCPaccess Parameters Library List panel.

The Edit TCPaccess PARMS Dataset panel appears.

2. Edit the member, as required.
3. Press F4 (Save).

The changes are saved.

## IBM Configuration Data Sets

IBM TCP/IP configuration information is contained in the following data sets:

### **PROFILE.TCPIP**

Contains the configuration information required by the IBM TCP/IP application during initialization. It includes the following type of information:

- Telnet server configuration
- Device and link definitions
- Routing information

### **TCPIP.DATA**

Contains the configuration information required by the client applications. It includes the following type of information:

- The host name
- Name server information
- Socket information

### **FTP.DATA**

Contains the FTP server configuration. For information about the FTP.DATA data set and how it is used to configure your system, see IBM's Communications Server IP books.

## Edit Data Sets

The following types of commands are available to edit a data set:

### **Line Commands**

On the left of each line of text is a sequence number field. To update or add text, you enter commands in these fields to perform edit functions.

### **Primary Commands**

You can enter other commands in the Command field. Commonly used primary commands are assigned to function keys, enabling you to invoke the command by pressing a function key instead of entering the command in the Command field.



## Update a Data Set

### To update a data set

1. Enter **DP** (Display Profile Configuration Libraries) next to an IBM STACK entry on the IP Resource Monitor.

The Profile Configuration Datasets panel appears.

2. Enter **S** next to the required configuration data set entry.

The TCP/IP : Browse Profile Dataset panel appears.

3. Press F4 (Edit).

The TCP/IP Edit Profile Dataset panel appears.

4. Edit the data set, as required.

5. Press F4 (Save).

The data set is saved.

## Change Configuration Using Obeyfile Data Sets

**Note:** This section applies to IBM TCP/IP servers only.

To make changes to the configuration, use an Obeyfile data set. Changes made using an Obeyfile data set are dynamic and only affect the running system—they are lost when the IBM TCP/IP system is stopped and restarted.

You can use an Obeyfile data set to control tracing, start or stop devices, or to add new or temporarily authorized users without stopping and restarting the system.

## Execute an Obeyfile Data Set

### To execute an Obeyfile data set

1. Enter **O** (Execute Obeyfile) next to an IBM STACK entry on the IP Resource Monitor.  
The TCP/IP : STACK Execute Obeyfile panel appears.
2. Complete the following field:

#### Obeyfile Dataset

Specifies the name of the data set. This can be:

- The name of a partitioned data set (PDS), with no member name
- The name of a PDS, with a member name included
- The name of a sequential data set

Press F6 (Action).

The Obeyfile PDS List appears.

3. Enter **O** next to the Obeyfile member that you want to execute.  
The Obeyfile Confirm panel appears.
4. Press F6 (Action).  
The Obeyfile is executed.

## Check Your Obeyfile Results

The contents and results of the Obeyfile are recorded in the activity log, which you can access by entering **/LOG** at the prompt.

For information about creating Obeyfile data sets or modifying configuration data sets to change your system's configuration, see IBM's Communications Server IP books.

**Note:** You do not need to create obeyfiles for starting and stopping packet traces or devices. TCP/IP commands are automatically generated for these purposes when the appropriate actions are selected on connection and device link displays.

## Create a New Member of an Obeyfile Data Set

You can create a new member of an Obeyfile data set, or you can edit an existing one.

### To create a new member of an Obeyfile data set

1. Enter **E** *membername* or **EDIT** *membername* at the prompt on the Obeyfile PDS List panel.

The Edit Obeyfile panel appears.

2. Press F4 (Edit) from the Obeyfile Confirm panel.

The Edit Obeyfile panel appears.

**Note:** If you are at the Obeyfile PDS List panel, you can edit an Obeyfile member by entering **E** (Edit) next to a data set name to display the Edit Obeyfile panel.

3. Edit the data set, as required.
4. Press F4 (Save).

The data set is saved.

**Note:** Obeyfile processing can be used to start and stop traces and to alter the state of the interface devices as well as altering some configuration parameters. The OBEYFILE command is used to execute the IBM TCP/IP configuration commands.

## Display Workload Manager Status

(For IBM's Communications Server only) When Communications Server is running in a sysplex, it can register TCP/IP stacks and Telnet servers with the Workload Manager (WLM). Each Telnet server can register under more than one cluster name.

By checking with the WLM about the relative availability of Communications Server and its servers on each system, a domain name server (DNS) can use this information to route work, or to direct client connections, around the sysplex.

## Display the WLM Status of IBM TCP/IP Stacks

The TCP/IP Stack Workload Status panel provides information about registered TCP/IP stacks in a sysplex and their relative availability. This information lets you diagnose problems with the Domain Name Server based on the WLM.

### To display the TCP/IP stack WLM status

1. Enter **SWL** next to an IBM stack entry on the IP Resource Monitor.

The stack WLM status appears.

## Display the WLM Status of Telnet Servers

The Telnet Server Status display and the Telnet Cluster List provide the following information:

- Cluster names under which the server is registered
- Port number
- Registration status of Telnet servers running on the local system

This information lets you determine which Telnet server in a sysplex supports which type of client connection and the relative availability of Telnet server and TCP/IP stack for a particular cluster.

This procedure retrieves information for the server that runs as part of a stack. For a server that runs in its own address space ([external Telnet server](#) (see page 174)), you use the same procedure for an ASMON resource instead of a STACK resource.

### To display the Telnet Server WLM Status

1. Enter **TWL** next to an IBM stack entry on the IP Resource Monitor.

The Telnet Server Status panel appears.

## Display Telnet Cluster List

The Telnet cluster list displays the hosts that support the cluster.

### To display the Telnet Cluster List

1. Enter **S** next to the selected Telnet cluster name on the Telnet Server Status display.

The Telnet Cluster List appears.

## List Remote Addresses

The list enables you to identify remote IP addresses that have sent packets to or received packets from a mainframe stack since the Packet Analyzer was last started.

You can sort a list of remote addresses. For a remote address, you can view any available traffic statistics. You can also look up the host name of an address.

To list the remote addresses for a stack, enter **RI** (List Remote IP Addresses) next to the stack on the IP Resource Monitor.

The Remote IP Address List appears.

**More information:**

[Remote IP Address Lists](#) (see page 62)

## Display Address Space Activities

The TCP Application Activity List panel lists the address spaces known to the Packet Analyzer. The list includes the following information for each job, started task, or user:

- Connections count
- Security information
- Time of last activity
- Distribution of connections by duration
- Byte and packet statistics

You can use the **FILTER** command to restrict the list and the **SORT** command to sort the list.

To display address space activities on a stack, enter **TC** next to the stack on the IP Resource Monitor.

The TCP Application Activity List panel appears.



# Chapter 9: Managing Open Systems Adapters

---

This section contains the following topics:

- [Open Systems Adapters](#) (see page 127)
- [Monitor OSAs](#) (see page 128)
- [Display OSA Utilization](#) (see page 128)
- [Display OSA Performance History](#) (see page 129)
- [List OSA Devices](#) (see page 130)
- [Display OSA Configuration](#) (see page 131)
- [Display the OSA Address Table](#) (see page 131)

## Open Systems Adapters

The IBM Open Systems Adapter (OSA) is a hardware device that combines the functions of a communications controller and a channel, for connecting a system to a network. Visibility of OSA resources is provided in the following ways:

- OSA utilization
- OSA performance

You can also view the following:

- Device list for OSA
- OSA configuration
- OSA OAT table

## Monitor OSAs

The IP Resource Monitor provides visibility of the OSAs defined to your region. OSAs are shown as class OSA.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to an OSA resource](#) (see page 108) to perform various functions.

If you know the specific OSAs you want to manage, you can also work with them using the OSA Management menu. The menu shortcut is **/OSA**.

**Note:** To enable support for an OSA, you must have defined the OSA to your region. For information about how to define OSAs, see the *Implementation Guide*.

## Display OSA Utilization

### To display OSA utilization and general information

1. Enter **D** (Display) beside an OSA on the IP Resource Monitor.

The Open Systems Adapter Summary panel appears.

**Note:** The data displayed depends on the type of OSA; more data appears for OSA Express or OSA DirectExpress than for OSA-2.

## Display OSA-2 Utilization

The CHP %Busy value shows the percentage of time during which the OSA was busy transferring data through the CHPID shown.

## Display OSA Express or DirectExpress Utilization

Recent Performance History appears only if OSA/SF or SNMP support is enabled in the definition of the OSA resource.

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



## Display OSA Performance History

The Open Systems Adapter History panel lets you monitor the performance and health status of an OSA.

**Follow these steps:**

1. Enter **H** (History) next to an OSA on the IP Resource Monitor.

The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.

2. Enter *one* of the following actions beside an attribute for more details:

- D lists the samples
- S displays the Hourly Summary Graph
- H displays the Hourly Summary List
- DL displays the Daily Summary List
- W displays the Weekly Interval List

Press F5 (Overview) to compare this resource with others on the system.

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.

## List OSA Devices

The OSA Device List shows the devices on the OSA that are connected through it to an z/OS system. The panel provides status and configuration information about these devices.

To display the OSA device list, enter **DL** (Display Device List) next to an OSA on the IP Resource Monitor (**/IPMON**).

The OSA Device List panel appears.

You can use action codes to access additional information from this device list:

- Use the H action code to access the performance history for the OSA or for an OSA device.
- Use the I action code to access the following information:
  - Applications using the device
  - Traffic statistics
- Use the ?? action code to list the line commands that you can select and issue for the OSA.

## Display OSA Configuration

The OSA Configuration panel provides current configuration values for the hardware and software that are connected to the OSA. The information comes from the OSA Support Facility (OSA/SF) or the IOBSNMP Simple Network Management Protocol (SNMP) subagent, and falls into the following sections:

- The OSA section displays information about the system on which the data was collected.
- The Hardware Details section displays information about the OSA hardware.
- The Details for Port sections list the hardware state and selected performance data for each port.
- The Devices in Use section lists the device numbers of the OSA devices, their configuration, and their status. This information is a subset of the information you get when you list OSA devices.
- The Device Allocation by LPAR section displays the OAT.

**Note:** For information about OSA/SF, see *IBM Open Systems Adapter-Express Customer's Guide and Reference*.

To display OSA Configuration, enter **CF** (Display OSA Configuration Settings) next to an OSA on the IP Resource Monitor (**/IPMON**).

The OSA Configuration panel appears.

## Display the OSA Address Table

### To display the OSA address table

1. Enter **OAT** (Display OSA Address Table) beside an OSA on the IP Resource Monitor (**/IPMON**).

The OSA Address Table List panel appears.



# Chapter 10: Managing Cisco Channel Cards

---

This section contains the following topics:

- [Cisco Channel Cards](#) (see page 134)
- [Monitor and Diagnose Channel Cards](#) (see page 135)
- [Display Channel Card Information](#) (see page 135)
- [Display Channel Card Performance History](#) (see page 137)
- [Diagnose Telnet Connection Problems](#) (see page 138)
- [Start a Telnet Connection to the Router](#) (see page 138)
- [Display Channel Information](#) (see page 138)
- [Display TN3270 Server Information](#) (see page 139)
- [List PUs for a Server](#) (see page 139)
- [Display the TN3270 Server Log](#) (see page 140)
- [Display CLAW Information](#) (see page 141)
- [Display CLAW Subchannel Information](#) (see page 141)
- [Display TCP Offload Information](#) (see page 142)
- [Display CSNA Information](#) (see page 142)
- [Display Internal LAN Information](#) (see page 143)

## Cisco Channel Cards

The Cisco Mainframe Channel Connection (CMCC) is supported on the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). This guide refers to the CIP and CPA as Cisco channel cards.

The Cisco channel card includes the following functions:

- Interconnection controller and providing TCP/IP connectivity for the mainframe
- LAN based SNA connectivity to PUs
- TN3270 server, saving S/390 CPU cycles on the system by running on the channel card

To support the use of Cisco channel cards in your environment, you can do the following:

- List TN3270 Telnet connections by specifying IP address, LU name, and application name
- Monitor the performance and health of the channel card by providing indicators such as:
  - CPU, memory, and DMA utilization
  - Transfer rates on CLAW links
  - Error rates on channel interfaces
  - TN3270 server users and free LU counts

You can also use the following diagnostic functions:

- Obtain a history of important events on the LU.
- Obtain SNA data about the connection
- Obtain TN3270 server status information
- Monitor the behavior of the channel card and its components

## Channel Card Status

The status of the channel card and its associated components can provide information to help you tune network, and resolve problems such as:

- The network appears to be running slowly.
- Users cannot establish a session.
- Part of the network is isolated.

## Monitor and Diagnose Channel Cards

The IP Resource Monitor provides visibility of channel cards defined to your region.

Channel cards are shown as class CIP.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to a CIP resource](#) (see page 108) to perform various functions.

If you know the specific channel cards you want to manage, you can also work with them using the CIP and Router Management menu. The menu shortcut is **/CIP**.

**Note:** To enable support for a Cisco channel card, you define the channel card to your region. For information about defining a channel card, see the *Implementation Guide*.

## Display Channel Card Information

By showing the general health and status information for the channel card, the Cisco Channel Card Information panel lets you detect problems with the channel card on the router.

### To display Cisco channel card information

1. Enter **D** (Display General Information) beside a CIP on the IP Resource Monitor.

The TCP/IP : Cisco Channel Card Information panel appears.

## Display Application Information

Application information displays are available for applications specified on the Cisco Channel Card Information panel. The supported applications are:

- TN3270 server
- CSNA
- CLAW (TCP datagram)
- TCP Offload

**Note:** Not all applications support these additional application information displays.

### To display application information

1. Enter **S** next to an application in the Application column on the Cisco Channel Card Information panel.

The selected application information panel appears.



## Display Channel Card Performance History

The Cisco Channel Card History panel lets you monitor the performance and health status of a Cisco channel card.

Your system administrator controls the attributes that are sampled. The samples can include the following attributes:

- Channel card CPU use
- Channel card memory use
- DMA load (DMA communicates between the channel card and route processor)
- Channel load
- Channel errors
- TN3270 usage

For ESCON channels, the following additional information is available:

- Channel use (in bytes or percentages)
- CLAW read and write statistics

**Follow these steps:**

1. Enter **H** (History) next a CIP on the IP Resource Monitor (**/IPMON**).

The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.

2. Enter *one* of the following actions beside an attribute for more details:

- D lists the samples
- S displays the Hourly Summary Graph
- H displays the Hourly Summary List
- DL displays the Daily Summary List
- W displays the Weekly Interval List

Press F5 (Overview) to compare this resource with others on the system.

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.

## Diagnose Telnet Connection Problems

A channel card appears as a type of link on Telnet connection lists. Because CA NetMaster NM for TCP/IP supports multiple systems, a Telnet connection list can display multiple channel cards, or a mix of channel card and TCP/IP links.

To diagnose Telnet connection problems with a channel card, you can display a Telnet LU mini trace from the Telnet Connection List panel.

### Display a Telnet LU Mini Trace

The Telnet LU mini trace displays a list of current events received by the TN3270 server.

#### To display a Cisco Telnet LU mini trace

1. Enter **MT** next to the LU on which you want to perform the trace.

The TCP/IP : Cisco TN3270 LU Mini Trace panel appears.

## Start a Telnet Connection to the Router

#### To start a Telnet full-screen connection to a router containing a channel card

1. Enter **TN** (Start a Telnet Connection) beside a CIP on the IP Resource Monitor (**/IPMON**).

The TCP/IP : Telnet panel appears.

**Note:** You can also start a Telnet connection by pressing F4 on the Server Information, Channel Information, PU List, LU List, and CLAW panels.

## Display Channel Information

The TCP/IP : Cisco Channel Information panels provide details, statistics, and any error indications for devices on the channel card interfaces.

#### To display Cisco channel information

1. Enter **CI** (Channel Information) beside a CIP on the IP Resource Monitor (**/IPMON**).

The Cisco channel information appears.

## Display TN3270 Server Information

The TCP/IP : Cisco TN3270 Server Information panels lets you detect the cause of problems with TN3270 server access, for example, an SNA connectivity problem. The panels provide information such as status, configuration, and statistics related to the TN3270 server.

### To display Cisco TN3270 server information

1. Enter **TNI** (TN3270 Server Information) beside a CIP on the IP Resource Monitor (**/IPMON**).

The TCP/IP : Cisco TN3270 Server Information panel appears.

2. (Optional) Press the following function keys:

#### **F4 (Telnet)**

Starts a Telnet connection to the channel card.

#### **F5 (Log)**

Displays the TN3270 server log.

## List PUs for a Server

The TCP/IP : Cisco TN3270 PU List lets you check the PU status and configuration on the channel card side and the VTAM side.

### To display the PUs for a server

1. Enter **PU** next to the CIP device for which you want to display PUs on the IP Resource Monitor (**/IPMON**).

The TCP/IP : Cisco TN3270 PU List appears.

2. (Optional) Press the following functions keys:

#### **F4 (Telnet)**

Starts a Telnet connection to the channel card.

#### **F5 (Log)**

Displays the TN3270 server log.

## List LUs for a PU

The Cisco TN3270 LU List lets you detect any problems with LUs attached to the TN3270 server by a PU.

### To list LUs for a PU

1. Enter **S** next to the selected PU from the Cisco TN3270 PU List.

The Cisco TN3270 LU List appears.

2. (Optional) Press the following function keys:

#### **F4 (Telnet)**

Start a Telnet connection to the channel card.

#### **F5 (Log)**

Display the TN3270 server log.

## Display the TN3270 Server Log

The TN3270 Server Log provides a history of TN3270 server activities. This lets you diagnose connection problems by using information about connections that are no longer active. You can also diagnose general problems by looking for additional error messages in the log.

The log contains the following types of messages:

- Status and error messages from the TN3270 server about the server software
- Messages about individual connections

**Note:** You must define the channel card with active logging. For more information, see the *Implementation Guide*.

### To display the TN3270 Server Log

1. Enter **TNL** (TN3270 Server Log) beside a CIP on the IP Resource Monitor (**/IPMON**).

The TN3270 Server Information Panel appears.

2. Press F5 (Log).

The TN3270 Server Log appears.

## Display CLAW Information

The Cisco CLAW Information panels provide you with channel details, statistics, configuration, and any error indications for the Common Link Access to Workstation (CLAW).

This information lets you manage the CLAW support on the Cisco channel card.

### To display the Cisco CLAW information

1. Enter **CL** (CLAW Information) beside a CIP on the IP Resource Monitor (**/IPMON**).  
The TCP/IP : Cisco CLAW Information panel appears.

## Display CLAW Subchannel Information

The Cisco CLAW Subchannel List panels provide you with subchannel details and statistics for Common Link Access to Workstation (CLAW) links. These details include the following:

- Channel utilization percentages
- Transfer rates on CLAW links
- TCP/IP stack names
- System names
- Channel path IDs

This information is available from the following perspectives:

- From the channel card—where the CLAW subchannels are known and you want information about the host channel usage information (for example, what channels are being used by CLAW links to this channel card and how heavily used they are)
- From the host channel—where the host channels are known and you want information about the CLAW and other usage for those channels (for example, which devices are using CHPID 10 on PRD0)

### To display the Cisco CLAW subchannel information

1. Enter **CS** (CLAW Subchannel List) beside a CIP on the IP Resource Monitor (**/IPMON**).  
The TCP/IP : Cisco CLAW Subchannel List appears.

## Sort Entries on the Cisco CLAW Subchannel List

You can use the SORT command to display the CLAW Subchannel List in a sort order other than the default order of channel card or host.

The operand values for the command are associated with the column heading of the column that you want to sort by. For example, enter **SORT DEV** to sort the list by the device.

**Note:** You can enter **SORT ?** to display a selection list of sort fields.

## Display TCP Offload Information

The Cisco TCP Offload Information panels provide you with details, statistics, and any error indications for the Cisco channel card TCP offload. This information lets you manage the TCP offload support on the Cisco channel card.

### To display Cisco TCP offload information

1. Enter **OF** (TCP Offload Information) beside a CIP on the IP Resource Monitor (**/IPMON**).

The TCP/IP : Cisco TCP Offload Information panel appears.

## Display CSNA Information

The TCP/IP : Cisco CSNA Information panels provide you with details, statistics, and any error indications for the SNA support on the Cisco channel card. This information lets you manage the Cisco Systems Network Architecture (SNA) support on the channel card.

### To display Cisco CSNA information

1. Enter **SN** (CSNA Information) beside a CIP on the IP Resource Monitor (**/IPMON**).

The TCP/IP : Cisco CSNA Information panel appears.

## Display Internal LAN Information

The Cisco Internal LAN Information panel lets you manage the Cisco internal LAN support on the channel card.

### To display Cisco internal LAN information

1. Enter **LAN** (Internal LAN Information) beside a CIP on the IP Resource Monitor (**/IPMON**).

The TCP/IP : Cisco Internal LAN Information panel appears.

## Display Internal LAN Adapters

### To display the Cisco Internal LAN adapters

1. Enter **S** next to the required LAN at the Internal LAN Information panel.

The TCP/IP : Cisco Internal LAN Adapters panel appears.





# Chapter 11: Managing Enterprise Extender

---

This section contains the following topics:

- [Enterprise Extender](#) (see page 145)
- [Monitor and Diagnose Enterprise Extender](#) (see page 146)
- [Check EE Connectivity](#) (see page 146)
- [Display EE UDP Connections](#) (see page 147)
- [Display UDP Port Activity](#) (see page 147)
- [Display RTP Pipes](#) (see page 147)
- [Display EE Traffic Statistics by CP](#) (see page 148)
- [Display EE Traffic Statistics by CP and Priority](#) (see page 148)
- [Run EE VTAM Commands](#) (see page 148)
- [Detect RTP Pipe in Red Status](#) (see page 149)
- [Check EE RTP Health](#) (see page 149)
- [Check Transmission Group PU RTP Health](#) (see page 150)
- [Define EE RTP Health Thresholds](#) (see page 150)
- [Packet Tracing](#) (see page 151)
- [Display Enterprise Extender Performance History](#) (see page 154)
- [Display XCA Major Node](#) (see page 155)
- [Display EE Traffic Analysis](#) (see page 156)
- [EE Traffic Analysis](#) (see page 156)

## Enterprise Extender

Enterprise Extender connects SNA clients to the mainframe over an IP backbone by using the UDP protocol.

From an SNA view, Enterprise Extender is a logical link that is defined as an XCA (eXternal Communications Adapter) major node and a switched major node. Each LPAR can have only one active Enterprise Extender XCA major node. The Sessions action provides a view of Enterprise Extender sessions at the SNA node level.

From an IP view, Enterprise Extender is UDP traffic over the IP backbone. The UDP port activity action provides visibility of Enterprise Extender at the UDP port level.

The IP Resource Monitor lets you manage Enterprise Extender connections by providing both SNA and IP views of Enterprise Extender communications.

## Monitor and Diagnose Enterprise Extender

You can use the IP Resource Monitor to monitor Enterprise Extender traffic by port, and diagnose the underlying line groups and Rapid Transport Protocol (RTP) pipes.

Enterprise Extender resources are shown as class EE.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to an EE resource](#) (see page 108) to perform various functions.

You can also work with Enterprise Extender resources using:

- The Enterprise Extender Management menu. The menu shortcut is /EE.
- The Primary Menu Condition Summary.

## Check EE Connectivity

The EE connectivity test:

- Verifies remote host connections through the UDP ports
- Determines the time it takes for a host to respond
- Provides a record of the route taken by the EE packets through the network
- Highlights abnormal conditions

### To initiate an EE connectivity test

1. Enter **/EETEST** at the command prompt.  
If you have more than one remote host, the Remote Host Name/Addr List appears.
2. Enter **S** beside the required host  
If you have more than one VIPA, the EE Static VIPA List appears.
3. Enter **S** beside the required VIPA.  
The EE Connectivity Test panel appears.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

## Display EE UDP Connections

Data derived from the Packet Analyzer is used to display information about:

- The UDP connections used by EE
- Address and port information on the connections to remote CPs

To display a list of EE UDP connections enter **/EEUDP** at the command prompt.

The EE UDP Connections list appears.

**Note:** For information about the actions and fields on this panel, press F1 (Help).

## Display UDP Port Activity

Use UDP Connection Information panel uses data derived from the Packet Analyzer to display connection, byte, and packet information for a specific UDP connection.

### To display UDP port activity

1. Enter **/EEUDP** at the command prompt.

The EE UDP Connections panel appears.

2. Enter **S** against desired connection.

The EE UDP Connection Information panel appears.

**Note:** For information on the fields on this panel, press F1 (Help).

## Display RTP Pipes

You can display a list of the RTP pipes using EE.

**Note:** You cannot use this option with the base port.

To display a list of RTP pipes using an EE UDP connection, enter **/EERTP** at the command prompt.

The EE RTP Pipe List appears.

**Note:** For information on the actions and fields available on this panel, press F1 (Help).

## Display EE Traffic Statistics by CP

You can display EE traffic statistics for the control points. Only the control points with traffic in the last hour are listed.

To display EE traffic statistics by CP, enter **/EUPERF.TRS** at the command prompt.

The Enterprise Extender Traffic Statistics panel appears.

For information on the fields on this panel, press F1 (Help).

## Display EE Traffic Statistics by CP and Priority

You can display EE traffic statistics sorted by priority for the control points. The traffic is sorted by Signal, Network, High, Medium, and Low priority. Only control points with traffic in the last hour are listed.

To display EE traffic statistics by CP and priority, enter **/EUPERF.TRP** at the command prompt. The EE Traffic Statistics by Priority panel appears.

For information on the fields on this panel, press F1 (Help).

## Run EE VTAM Commands

Use this option to display a list of VTAM commands relevant to EE and APPN. The command environment provides scroll, find, command recall, and print functions.

To list the VTAM commands relevant to EE and APPN, enter **/EEV** at the command prompt.

## Detect RTP Pipe in Red Status

An RTP pipe with severe traffic congestion has ARB mode is red. To avoid spurious traffic congestion alerts, the RTPRED5M IP event detector raises an alert when ARB mode is red in two consecutive five-minute samples.

### To set the RTPRED5M detector

1. Enter **/EDETECT** at the command prompt.

The Event Detector Control List appears.

2. Enter **U** next to the RTPRED5M detector.

The RTPRED5M detector panel appears.

**Note:** For information about the actions and fields on this panel, press F1 (Help).

3. Complete the required criteria, and press F3 (File).

The alert is activated.

## Check EE RTP Health

The EE RTP health check lists any RTP pipes with the following network performance issues:

- ARB mode is RED and the condition has existed for more than five minutes
- An error pathswitch occurred in the most recent interval and more than one pathswitch occurred in the last three intervals
- RTPs are experiencing impaired throughput
- RTPs are currently in a stalled condition
- RTPs in a congested state
- Retransmission percentage exceeds the specified threshold
- RTPs have significant queuing

RTPs are monitored at five minute intervals. Each list is for a specific health check and an RTP may appear in more than one list.

The RTP Health Check can be performed on the local system or globally on all RTPs in a multisystem environment.

To access the EE RTP health check, enter **/EERH** from the command prompt.

**Note:** For information on the fields on this panel, press F1 (Help).

## Check Transmission Group PU RTP Health

The EE RTP health check reports on the RTP pipes for a specific transmission group PU. RTPs are monitored using the SNA Network Management API.

### To check transmission group PU RTP health

1. Enter **/EEXCA** from the command prompt.  
The EE XCA Major Node Summary appears.
2. Enter **RH** next to a specific Transmission Group PU.  
The RTP Health Check list appears.

**Note:** For information on the fields on this panel, press F1 (Help).

## Define EE RTP Health Thresholds

You can use the EE resource class to define thresholds for EE related RTP pipes:

- Inbound queue limit
- Outbound queue limit
- Retransmission rate

### To set the RTP health thresholds

1. Enter **/RMON** at the command prompt.  
The Resource Monitor appears.
2. Enter **U** beside the EE resource you want to define thresholds for.  
The Panel Display List appears.
3. Enter **S** beside EE Monitoring Definition.  
The EE Monitoring Definition panel appears.
4. Complete the EE RTP Health Limits fields.  
**Note:** For information about the fields, press F1 (Help).
5. Press F3 (File).  
The details are saved.

**Note:** If there is no EE resource defined in the active system image the APPNHPR limits are used. If there is no APPNHPR or EE resource in the active system image, the default of 100 is applied to inbound and outbound queues, and the default of 5% is applied for retransmission rate.

## Packet Tracing

**Note:** SmartTrace cannot see packets secured by IPSec.

You can trace packets on Enterprise Extender from the IP Resource Monitor by entering [SmartTrace line commands](#) (see page 197) next to the Enterprise Extender that you want to diagnose. Use the PT command to start a trace and the PTI command to stop a trace. When a trace is active, a T appears in the Ovr column.

The PT command lets you specify a foreign host to limit the trace, which is useful when the Enterprise Extender has connections to multiple hosts. By specifying the foreign host, you limit the trace to the connection that is causing the problem.

You can list the started traces from the TCP/IP : Packet Tracing Menu.

You can also start tracing from the EE SmartTrace Menu.

**More information:**

[Using SmartTrace](#) (see page 195)

## SmartTrace with EE

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

EE SmartTrace (/EETRACE) enables you to trace:

- Packets bound for a selected EE remote control point
- All the RTP pipes for a specific priority, flowing over one EE connection
- Individual RTP pipes
- RTP pipes using one local VIPA
- The packets using a specified UDP port

## Trace EE Remote CP

Use the EE Remote CP Trace to start and manage traces of packets bound for a selected EE remote control point.

### To start the EE Remote CP trace

1. Enter **/EETRACE.C** at the command prompt.

The Major Node summary appears.

2. Enter **PT** against a line.

The Activate Packet Trace panel appears.

3. Press F6 (Action).

The packet trace of the EE remote CP starts.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

## Trace EE UDP Connection

Use the EE UDP Connection Trace to trace all of the EE RTP pipes flowing over one EE connection.

The connection is defined by the local and remote addresses and UDP ports.

### To start the EE UDP Connection trace

1. Enter **/EETRACE.U** at the command prompt.

A list of EE UDP Connections appears.

2. Enter **PT** against a connection.

The packet trace of the selected RTP pipe starts.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

## Trace EE RTP Pipe

Use the trace EE RTP pipes to manage packet traces of individual RTP pipes.

### To start the EE RTP Pipe trace

1. Enter **/EETRACE.R** at the command prompt.

The EE RTP Pipe List appears.

2. Enter **PT** against a Pipe.

The packet trace of the selected RTP pipe starts.

**Note:** For information on the actions and fields on this panel, press F1 (Help).



## Trace EE Local VIPA

Use the EE Local VIPA Trace to trace EE packets through one local VIPA.

### To start the EE local VIPA trace

1. Enter **/EETRACE.V** at the command prompt.

The Major Node summary appears.

2. Enter **PT** against a Line Group.

The Activate Packet Trace panel appears.

3. Press F6 (Action).

The packet trace of the local IP Address (VIPA) starts.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

## Trace EE UDP Port

Use the EE UDP Port trace to trace all of the EE packets for a specified EE UDP port.

- For a traffic port (12001 to 12004), the trace includes all of the RTP pipes that use the associated priority, flowing over any EE connection
- For the signal port (12000), the trace includes signal data for every EE connection

### To start the EE UDP Port trace

1. Enter **/EETRACE.P** at the command prompt.

The Port Number prompt appears.

2. Enter the required port number.

The Activate Packet Trace panel appears.

3. Press F6 (Action).

The Packet Trace List appears.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

## Display Active and Ended EE SmartTraces

Use the EE Active and Ended Traces option to list the running, ended, and saved EE SmartTraces.

**Note:** Saved EE traces need the EE command to apply the SNA formatting.

To list all of the EE SmartTrace definitions, enter **/EETRALL** at the command prompt.

The EE Active and Ended Traces panel appears.

**Note:** For information on the actions and fields on this list, press F1 (Help).

## Display Enterprise Extender Performance History

The Enterprise Extender History panel displays collected performance data and provides graphs of selected communication attributes. You can monitor the following areas of Enterprise Extender communications to ensure that their services are available:

- Traffic through Enterprise Extender ports
- Availability of SNA lines to satisfy new connection requests

### Follow these steps:

1. Enter **H** (History) next to an EE resource on the IP Resource Monitor (**/IPMON**).

The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time that a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.

2. Enter *one* of the following actions next to an attribute for more details:

- D lists the samples
- S displays the Hourly Summary Graph
- H displays the Hourly Summary List
- DL displays the Daily Summary List
- W displays the Weekly Interval List

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.

## Display XCA Major Node

The Enterprise Extender panel displays general information about the XCA major node. It displays SNA session information (such as line and PU status) obtained by VTAM for each line group, and the IP address of the remote host connected to the session. It provides a hierarchical view of the lines associated with the XCA major node by line groups.

To display the XCA major node, enter **S** (Display XCA Major Node Summary) beside an EE entry on the IP Resource Monitor (**/IPMON**).

The Enterprise Extender panel appears, for example:

```

PROD1----- TCP/IP : COMP0001.A11X99 Enterprise Extender -----
Command ==>                                         Scroll ==> CSR

Major Node ..... EE11XCA          Stack Name ..... TCPIP11B
State ..... ACTIV          Desired State ..... ACTIV

               .=Expand or Collapse S/=Display R=RTP List ?=more actions
Line Group: EE11XCBG   IP Address: 192.168.66.12
|   Tgn: 0           Virtual Node: COMP0001.CAEENET1
| Line   Status   PU      Status   Remote CP      Remote IP Address
+ E11BL000 PALNK
+ E11BL001 PALNK
+ E11BL002 PALNK
+ E11BL003 PALNK
' E11BL004 PALNK
Line Group: EE11XCAG   IP Address: 192.168.66.40
| Line   Status   PU      Status   Remote CP      Remote IP Address
+ E11L000 PALNK
+ E11L001 PALNK
+ E11L002 PALNK

```

From the panel, you can apply various actions to a line to obtain more information. For example, applying the **S** action to an active line displays information about the node or the transmission group, and applying the **Q** action to a line displays its status.

## Display EE Traffic Analysis

Use EE Traffic Analysis to determine:

- EE traffic composition
- The busiest VIPAs and CPs
- The overhead added by EE and APPN/HPR

There are three displays:

### Hourly

Displays EE traffic data collected over the last full hour.

### Daily

Displays EE traffic data collected over the last full day.

### Cumulative

Displays EE traffic data collected since monitoring started

To display EE UDP traffic statistics enter **/EEPERF.TA** at the command prompt.

The EE Traffic Analysis panel appears.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

## EE Traffic Analysis

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

You can graph traffic for the following timeframes:

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

The hour and day graphs are only available if the Packet Analyzer and the region have been up for the full hour or day.

To view the EE Traffic Explorer, enter **/EEXP** at the command prompt. The EE Traffic Explorer panel appears.

**Note:** For information on the actions and fields on this panel, press F1 (Help).

# Chapter 12: Managing APPN/HPR Resources

---

This section contains the following topics:

- [APPN/HPR](#) (see page 157)
- [Monitor and Diagnose APPN/HPR Resources](#) (see page 158)
- [Display APPN/HPR Performance History](#) (see page 159)
- [Display Transport Resources List Entries](#) (see page 160)
- [Display RTP Pipes](#) (see page 160)
- [Display Dependent LU Requestors](#) (see page 160)
- [Display CP-CP Sessions](#) (see page 161)
- [Test APPN Connectivity](#) (see page 161)
- [Display APPN Directory Information](#) (see page 162)
- [Display APPN Subnetwork Topology Information](#) (see page 162)
- [Check RTP Health](#) (see page 163)
- [Run RTP VTAM Commands](#) (see page 165)

## APPN/HPR

Advanced Peer to Peer Networking / High Performance Routing (APPN/HPR) is an advanced SNA technique developed by IBM that enables SNA LU-LU sessions between peer devices using dynamic routing. This is in contrast to the more traditional, strictly hierarchical, subarea-oriented SNA.

APPN/HPR comprises two components: RTP (Rapid Transport Protocol) and ANR (Automatic Network Routing); ANR provides the routing, while RTP handles the route control and recovery and is responsible for the non-destructive routing around failures.

APPN/HPR links can be established over different transport mechanisms, of which Enterprise Extender (EE) is only one; therefore, EE always involves APPN/HPR.

EE carries APPN/HPR over an IP backbone, in NLPs (Network Layer Packets), allowing APPN to see the IP network as a single hop connection. UDP is the chosen protocol because it provides the best performance. One logical APPN/HPR link can traverse many hops, some of which may be EE. A system's whole EE environment may be just a small part of a much bigger picture.

Many of the most useful EE diagnostic tasks are performed at the non-EE level, that is, APPN/HPR level.

## Monitor and Diagnose APPN/HPR Resources

You can use the IP Resource Monitor to manage and monitor APPN/HPR resources. APPN/HPR resources are shown as class APPNHPR.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to an APPNHPR resource](#) (see page 108) to perform various functions.

You can view APPN/HPR RTP pipe utilization and exceptions at the APPN network level using the IP Condition Summary.

To access the IP Condition Summary, enter **/RTPCS**.

If you want, you can also display the IP Condition Summary on your Primary Menu. For information, see [Access IP Summary Display](#) (see page 52).

You can also work with APPN/HPR resources using the APPN/HPR : RTP Management Menu. The menu shortcut is **/APPNHPR**.

## Display APPN/HPR Performance History

The APPN/HPR History panel lets you monitor the performance and health status of an APPN/HPR resource.

The attributes that are sampled can include the following information:

- The number of active SNA LU-LU sessions over all RTP pipes.
- The number of RTP pipes flowing over all APPN/HPR connections.
- The number of RTP pipes that have had a red ARB mode for longer than 5 minutes.
- The number of RTP pipes where inbound NLP queuing is non-zero.
- The number of RTP pipes where outbound NLP queuing is non-zero.
- The number of RTP pipes where data flow has stalled due to buffers not being acknowledged.
- The number of RTP pipes where an error pathswitch occurred.

**Follow these steps:**

1. Enter **H** (History) next to an APPN/HPR resource on the IP Resource Monitor (**/IPMON**).

The list of monitored attributes appears.

Use F6 (AutoRfsh) to control whether the values are refreshed each time that a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4 (Expand).

2. Enter one of the following actions next to an attribute for more details:
  - **D** lists the samples.
  - **S** displays the Hourly Summary Graph.
  - **H** displays the Hourly Summary List.
  - **DL** displays the Daily Summary List.
  - **W** displays the Weekly Interval List.

Press F5 (Overview) to compare this resource with others on the system.

**Notes:**

- For more information, press F1 (Help).
- If authorized, you can update the monitored list through the UM line command.

## Display Transport Resources List Entries

The Transport Resource List panel displays the transport resource list entries (TRLEs) that define the characteristics of host-to-host channel connections. The display includes the following details:

- General information
- XCF details
- VTAM major node that defines the TRLE
- HiperSockets and OSA line details
- Details for the first read, write, and data devices

To list the TRLEs, enter **/APPNTRL** at the command prompt.

To access the details, press F11 (Right).

**Note:** For more information about the fields and actions available, press F1 (Help).

## Display RTP Pipes

The NCS : RTP Pipe List displays a list of Rapid Transport Protocol (RTP) pipes and their status. The display has multiple pages, which you can access by scrolling right. The lines on this panel are color-coded, depending on the values of connection state, congestion, and queue for each pipe.

To display a list of RTP pipes, enter **/RTP** at the prompt.

**Note:** For more information about the fields and actions available, press F1 (Help).

## Display Dependent LU Requestors

You can display a list of dependent LU requestors for which the host acts as dependent LU server (DLUS). The DLUS sends data on a contention-winner session and receives data on a contention-loser session.

To display a list of Dependent LU Requestor Resources (DLUR) resources, enter **/APPNDLU** at the command prompt.

**Note:** For more information about the fields and actions available, press F1 (Help).



## Display CP-CP Sessions

You can display a summary of CP connections from the CP-CP Session List.

From the CP-CP Session List, you can do the following:

- View the RTP Pipes for an adjacent CP
- Display connections for an adjacent CP
- Display the native VTAM display using Command Entry

To display a summary of CP connections, enter **/APPNCP** at the command prompt.

**Note:** For more information about the fields and options, press F1 (Help).

## Test APPN Connectivity

The APPN APING function tests the route to another APPN node and displays performance information for the route. The results are displayed in the following sections:

### Parameters (top)

Lets you change these parameters to perform a fresh APING for a node.

### Results (middle)

Contains a series of lines, each showing the result of one APING operation. The latest result is shown at the top of the list.

### Messages (bottom)

Displays messages relating to the latest APING operation.

**Note:** The APPN node must support the APING transaction.

### To perform an APING on a node

1. Enter **/APING** at the command prompt.

The NCS : APPN Menu appears.

2. Complete the following field:

#### Node/CP Name

Specifies the name of the resource on which you want to perform the action.

Press Enter.

The NCS : APING Results List panel appears.

**Note:** For more information about the NCS : APING Results List panel, press F1 (Help).

## Display APPN Directory Information

You can display information about a particular resource and the resources that it serves and owns from the NCS : APPN Directory Entry panel . For example, you can display a network node and the end nodes that it serves, and the LUs that it owns.

### To display APPN directory information

1. Enter **/SNAAPPN** at the command prompt.  
The NCS : APPN Menu appears.
2. Type **AD** at the command prompt and complete the following field:

#### Node/CP Name

Specifies the name of the resource on which you want to perform the action.

Press Enter.

The NCS : APPN Directory Display appears.

**Note:** For more information about the fields, press F1 (Help).

## Display APPN Subnetwork Topology Information

You can display the currently selected node (the origin control point) and any operative or quiescent adjacent destination control points from the NCS : Subnetwork Topology. The first line of the selection list on this panel shows the selected node, and the following lines list its adjacent nodes. The information displayed can vary, depending on the VTAM level of your system, and on the types of resources available in your network.

You can select any node to display node attributes. You can select an adjacent node to display transmission group attributes or to display its adjacent nodes.

To display the APPN subnetwork topology information, enter **/APPNTOP** at the command prompt.

**Note:** For more information about the fields and actions available, press F1 (Help).

## Check RTP Health

The RTP Health Check displays lists of RTP pipes that indicate the following network performance issues:

- ARB mode is RED and the condition has existed for more than five minutes
- An error pathswitch occurred in the most recent interval and more than one pathswitch occurred in the last three intervals
- RTPs are experiencing impaired throughput
- RTPs are currently in a stalled condition
- RTPs have congestion
- Retransmission percentage exceeds the specified threshold (default 5%)
- RTPs have significant queueing

RTPs are monitored using the SNA Network Management API using a five-minute interval. Each list is for a specific health check and an RTP may appear in more than one list.

The RTP Health Check can be performed on the local system or globally on all RTPs in a multisystem environment.

### Example: RTP Health Check Error Pathswitches

```

os 3 RTP pipes with recent error pathswitches

```

| Pipe     |                 | COS      | Connection           | PathSwitch  |
|----------|-----------------|----------|----------------------|-------------|
| Name     | CP Name         | Name     | State                | Psw# Reason |
| CNR0000D | USILDA01.A11X99 | #INTER   | CONNECTED            | 3 TG INOP   |
| CNR00002 | USILDA01.A11X99 | #CONNECT | CONNECTED/PATHSWITCH | 2 SRORETRY  |
| CNR00009 | USILDA01.A11X99 | #CONNECT | CALLING/PATHSWITCH   | 2 NO NCB    |

## Check RTP Health on a Local System

You can perform an RTP Health Check on a local system or a multisystem.

To check RTP health on a local system, enter **/RTPH** at the command prompt.

## Check RTP Health on a Multisystem

You can perform an RTP Health Check on a local system or a multisystem.

To check RTP health on a multisystem, enter **/RTPHG** at the command prompt.

## Define RTP Health Thresholds

To allow control over RTP health conditions, you can customize the following thresholds in the monitoring definition of the APPNHPR resource:

- Inbound Queue Depth
- Outbound Queue Depth
- Retransmission Rate

**Note:** The limits defined for the APPNHPR resource apply:

- To all health checks except for the EE resource health checks
- To the APPNHPR: RTP health check diagnostic displays

If there is no APPNHPR resource in the active system image, the default of 100 is applied to inbound and outbound queues, and the default of 5% is applied for retransmission rate.

### To define RTP health thresholds

1. Enter **/IPMON** at the command prompt.  
The Resource Monitor appears.
2. Enter **U** beside the APPNHPR resource for which you want to update the thresholds.  
The Panel Display List appears.
3. Enter **S** beside APPNHPR Monitor Definition.  
The APPNHPR Monitoring Definition panel appears.
4. Complete the RTP Health Limits field.  
**Note:** For more information about the fields, press F1 (Help).
5. Press F3 (File).  
The details are saved.

## Run RTP VTAM Commands

The RTP VTAM Command List lets you enter commonly used VTAM commands to diagnose problems with your APPN/HPR infrastructure.

### To run RTP VTAM commands

1. Enter **/RTPV** at the command prompt.  
The RTP VTAM Command List appears.
2. Enter **S** beside the command that you want to run.  
The command is executed.

**Note:** Some commands run immediately; whereas, some commands require you to enter parameters.



# Chapter 13: Managing VIPA Resources

---

This section contains the following topics:

[Virtual IP Addresses \(VIPAs\)](#) (see page 167)

[VIPA Resource Names](#) (see page 168)

[Monitor and Diagnose VIPAs](#) (see page 168)

[Display VIPA Details](#) (see page 169)

[Display VIPA Performance History](#) (see page 170)

[Check the Connection Routing Table](#) (see page 171)

[Modify VIPA Definitions](#) (see page 171)

## Virtual IP Addresses (VIPAs)

A VIPA (virtual IP address) is an IP address that is not associated with a physical adapter.

Dynamic VIPAs are playing an increasing role in mainframe-based TCP/IP networks because they provide fault tolerance and flexible workload distribution in a sysplex.

IBM supports the following types of dynamic VIPA:

- Dynamic VIPA for single application instance (application VIPA)

This type of dynamic VIPA is associated with a specific application, wherever the application is active in the sysplex.

- Dynamic VIPA for takeover/takeback

This type of dynamic VIPA is used to provide fault tolerance for failing stacks or failing MVS images in a sysplex.

- Distributed dynamic VIPA (sysplex distributor)

This type of dynamic VIPA supports workload distribution in a sysplex.

CA NetMaster NM for TCP/IP manages IBM's dynamic VIPAs by using VIPA resources. Display commands are available to show the status of the VIPA and connections through the VIPA. If you are running a multisystem environment, these displays merge information from all participating LPARs. This is particularly useful for sysplex distributor VIPAs or VIPAs that have just moved.

## VIPA Resource Names

Generally, the following name is assigned to a dynamic VIPA resource:

- (IPv4) Address of the resource
- (IPv6) Name of the interface associated with the resource

For an IPv6 dynamic VIPA activated through VIPARANGE, its name is that of the matching template, which is a user-specified name so that VIPAs in the range (which is configured with the same interface name) can be differentiated.

## Monitor and Diagnose VIPAs

The IP Resource Monitor provides visibility of the VIPAs defined to your region.

VIPAs are shown as class VIPA.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to a VIPA resource](#) (see page 108) to perform various functions.

If you know the specific VIPAs you want to manage, you can also work with them using the VIPA Management menu. The menu shortcut is **/VIPA**.



## Display VIPA Details

You want to learn about a VIPA, including the following information:

- How long has the VIPA been active?
- What is the status of the VIPA on a stack or on the stacks in a sysplex?
- For a distributed dynamic VIPA, how is the sysplex distributor distributing connections?
- What are the WLM weightings?

To display VIPA details, enter **D** (Display General Information) next to a VIPA on the IP Resource Monitor (**/IPMON**).

The VIPA Detail Display appears.

### Example: Details About a Distributed Dynamic VIPA

This example shows how a sysplex distributor is distributing connections from the VIPA, 192.168.171.24. The TCPIP31V stack on the CO31 system currently owns the VIPA.

```

PC=Port Connections .-Expand or Collapse ??=more actions
-----
VIPA..... 192.168.171.24
Interface Name ..... VIPL8DCAAB18
Origin (CO31) ..... VIPADEFINE
Active Since ..... 08/14/2012 20:50:04

-----
Sysplex Configuration
LPAR Stack Status Rank Dist DestXCF Address
-----
CO31 TCPIP31V ACTIVE BOTH 192.168.171.8
CO11 TCPIP11V BACKUP 255 DEST 192.168.171.9
XE61 TCPIP61V ACTIVE DEST 192.168.171.10

-----
Distribution Port Table on CO31
LPAR Stack Listener TSR TCSR CER SEF Total % Active %
WLM Ab Hth Flags Weight CP zAAP zIIP
-----
601 Dist Method: BaseWLM 333 86 69 92
| CO11 TCPIP11V REGN8 100 100 100 82 25 23 33
| 1 0 100 - 6 10/1 0/0 6/5
| CO31 TCPIP31V REGNL31 100 100 59 100 184 55 46 67
| XE61 TCPIP61V 1 100 100 0 100 67 20 0 0
2608 Dist Method: BaseWLM 51 13 6 8
23 Dist Method: BaseWLM 2 1 0 0
8011 Dist Method: BaseWLM 0 0 0 0
***** Bottom of data *****

```

## Display VIPA Performance History

The Monitor VIPA Performance History panel provides information and displays graphs of the performance data for the selected VIPA.

**Follow these steps:**

1. Enter **H** (History) next to a VIPA on the IP Resource Monitor (**/IPMON**).  
  
The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time a new sample is gathered.  
  
**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.
2. Enter *one* of the following actions beside an attribute for more details:
  - D lists the samples
  - S displays the Hourly Summary Graph
  - H displays the Hourly Summary List
  - DL displays the Daily Summary List
  - W displays the Weekly Interval ListPress F5 (Overview) to compare this resource with others on the system.

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.

## List IP Connections to a VIPA

**To list all IP connections to a VIPA**

1. Enter **IC** (List IP Connections to a VIPA) beside a VIPA on the IP Resource Monitor (**/IPMON**).  
  
The TCP/IP : Connections panel appears.

## List Telnet Connections to a VIPA

**To list all Telnet connections to a VIPA**

1. Enter **IT** (List Telnet Connections to a VIPA) beside a VIPA on the IP Resource Monitor (**/IPMON**).  
  
The TCP/IP : Telnet Connections panel appears.

## Check the Connection Routing Table

The VIPA Connection Routing Table panel provides information about each current connection of a sysplex distributor VIPA.

### To display information about each current connection of a sysplex distributor VIPA

1. Enter **CR** (Display Connection Routing Table) beside a sysplex distributor VIPA on the IP Resource Monitor (**/IPMON**).

The TCP/IP : VIPA Connection Routing Table appears.

## Modify VIPA Definitions

### To modify a VIPA definition

1. Enter **M** (Modify VIPA Definition) beside a VIPA on the IP Resource Monitor (**/IPMON**).

The TCP/IP : VIPA Modify Command panel appears.

2. Complete the following fields:

#### Destination Stack Name

Specifies the name of the stack that you want to modify.

#### Obeyfile Dataset at Destination

Specifies the data set name of the Obeyfile to use on the destination stack.

Press F6 (Action).

An edit panel appears, showing the obeyfile with a set of VIPADYNAMIC statements.

3. Update the VIPADYNAMIC statements, as required.
4. Press F6 (Action).

The definition is modified.



# Chapter 14: Managing Address Spaces

---

This section contains the following topics:

[Monitor Your Address Spaces](#) (see page 173)

[External Telnet Servers](#) (see page 174)

[Packet Tracing](#) (see page 175)

[Display Address Space Performance History](#) (see page 176)

[Display Address Space IP Traffic](#) (see page 177)

[DB2 Network Information Center](#) (see page 177)

## Monitor Your Address Spaces

You can use the IP Resource Monitor to display information about your monitored address spaces.

Address spaces are shown as class ASMON.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to an ASMON resource](#) (see page 108) to perform various functions.

If you know the specific address spaces you want to manage, you can also work with them using the Address Space and Port Management menu. The menu shortcut is **/ASMON**.

**Note:** To enable support for an address space, you define the address space IP resource, and the ports it uses that you want to monitor, to your region. For information about defining IP resources, see the *Implementation Guide*.

## External Telnet Servers

(For IBM's Communications Server only) If your site uses a Telnet server that run in its own address space (external Telnet server), your site can monitor them as ASMON class resources (type TNSERVER). In addition to standard ASMON commands, the following commands are available:

### **CL**

Displays the status of the LUs for the server.

### **IT and ITF**

Lists the connections to the server.

### **TWL**

Displays the status of the server.

### **More information:**

[Display the WLM Status of Telnet Servers](#) (see page 124)

## Check Telnet LUs

If IBM TCP/IP encounters an error while acquiring an LU for a Telnet connection request, it flags the LU as inactive and will not use the LU for future connections.

Over a period, a number of LUs may be flagged as inactive, which reduces the number of possible Telnet sessions available.

You can view and check the status of the LUs for a Telnet server using the IP Resource Monitor.

**Note:** Checking Telnet LUs can cause many messages to be written to the console and can take some time to complete.

To check Telnet LUs, enter **CL** (Check Telnet LUs) next to a Telnet server ASMON resource.

The Problem Telnet LUs panel appears. The panel lets you activate the LUs from the following perspectives:

- IBM TCP/IP (so they are no longer flagged as inactive)
- VTAM

If there are no problem Telnet LUs, the following message appears on the Problem Telnet LUs panel:

IPCK7704 NO TELNET LU PROBLEMS FOUND.

## Packet Tracing

You can trace packets in address spaces from the IP Resource Monitor by issuing [SmartTrace line commands](#) (see page 197) next to the address space that you want to diagnose. For example, you can issue the PT command to start a trace. When a trace is active, a T appears in the Ovr column.

The PT command lets you specify a foreign host to limit the trace. The command also lets you specify whether you want to create a separate trace for each new connection during the current tracing session.

You can list the started traces from the TCP/IP : Packet Tracing Menu.

**More information:**

[Using SmartTrace](#) (see page 195)

## Display Address Space Performance History

The Address Space History panel displays collected performance data and graphs of address space attributes. These attributes measure system resource usage and IP port traffic.

**Follow these steps:**

1. Enter **H** (Show Performance History) next to an ASMON entry on the IP Resource Monitor (**/IPMON**).

The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.

2. Enter *one* of the following actions beside an attribute for more details:

- D lists the samples
- S displays the Hourly Summary Graph
- H displays the Hourly Summary List
- DL displays the Daily Summary List
- W displays the Weekly Interval List

Press F5 (Overview) to compare this resource with others on the system.

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.



## Display Address Space IP Traffic

The Port Traffic Statistics panel shows the number of bytes and packets sent and received by the ports in 1-minute intervals over the last 5 minutes, and the percentage this represents of the total traffic for the stack.

**Note:** If a request from the generic server to a participating stack fails, the resource monitor shows the status of the ASMON class resource representing the server as DEGRADED. See the transient log for error messages.

### To display recent byte and packet counts for the IP ports associated with an address space

1. Enter **TRS** (Display IP Traffic Statistics) next to the ASMON class resource on the IP Resource Monitor (**/IPMON**).

The Port Traffic Statistics panel opens.

**Note:** You can display the statistics in 5-minute intervals over the last hour by pressing F12 (LastHour). If the address space is a generic server, traffic on all participating stacks appears.

**Note:** You can also view the IP traffic for all known address spaces on a system, not only the ones defined as ASMON. The TCP Application Activity List shows the traffic. You can access the list using the /ASMON.TC panel path. You can also view the address space traffic by stack, using the TC command for a STACK class resource.

### More information:

[Display Address Space Activities](#) (see page 125)

## 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.

**More information:**

[Managing Connections](#) (see page 73)

[Using SmartTrace](#) (see page 195)

[DRDA Packets](#) (see page 216)

# Chapter 15: Managing CSM Resources

---

This section contains the following topics:

[CSM Resources](#) (see page 179)

[Display CSM Usage](#) (see page 179)

[Display CSM Performance History](#) (see page 180)

## CSM Resources

The CSM (Communications Storage Manager) is a component of IBM's Communications Server. The component Authorized host applications use CSM to manage subsystem storage pools and to allow CSM users to share data without having to move the data physically.

You can use the IP Resource Monitor to display information about your CSM storage usage. CSM resources are shown as class CSM.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to a CSM resource](#) (see page 108) to perform various functions.

**Note:** To enable support for CSM, you define CSM to your TCP/IP management region. For information about defining CSM, see the *Implementation Guide*.

## Display CSM Usage

The CSM Usage by Buffer panel (or the CSM Usage by Job panel) provides information about the buffer usage of the CSM from the perspective of the selected region.

### To display the CSM Usage by Buffer (or by Job)

1. Enter **D** (Display CSM Usage) next to a CSM entry on the IP Resource Monitor (**/IPMON**)

The CSM Usage by Buffer panel appears.

**Note:** Use F4 to toggle between displays of usage by job and by buffer.

## Display CSM Performance History

The CSM History panel displays collected performance data and graphs of selected CSM attributes. You can view the total usage of CSM storage and the amount that individual tasks use.

**Follow these steps:**

1. Enter **H** (Show Performance History) next to a CSM entry on the IP Resource Monitor (**/IPMON**)

The list of monitored attributes appears. You can use the F6 function key to control whether the values are refreshed each time that a new sample is gathered.

**Note:** To expand or collapse the display of a listed qualifier, move the cursor to the qualifier and press Enter. To expand or collapse all qualifiers, press F4.

2. Enter *one* of the following actions next to an attribute for more details:
  - D lists the samples
  - S displays the Hourly Summary Graph
  - H displays the Hourly Summary List
  - DL displays the Daily Summary List
  - W displays the Weekly Interval List

**Note:** For more information, press F1 (Help).

**Note:** You can monitor other attributes. To monitor them, they must be added to the monitored list. For more information, see the *Implementation Guide*. If authorized, you can update the monitored list through the UM line command.

# Chapter 16: Managing CICS Resources

---

**Note:** The information here applies if CA NetMaster SM for CICS is configured in the region.

This section contains the following topics:

- [Diagnose Your CICS Resources](#) (see page 181)
- [List CICS Connections from a Socket Management Perspective](#) (see page 181)
- [Display Information About a CICMON Resource](#) (see page 182)
- [Stop and Restart CA NetMaster SM for CICS and CA CPT](#) (see page 182)
- [Stop and Restart the Command Server Interface](#) (see page 182)
- [Start a CICS Server](#) (see page 183)
- [Start CICS Transactions](#) (see page 183)
- [Monitor CICS Resource Performance](#) (see page 184)
- [Monitor CICS IP Traffic](#) (see page 184)

## Diagnose Your CICS Resources

You can use the IP Resource Monitor to display information about your CICS Socket Management resources.

CICS resources are shown as class CICMON.

To access the IP Resource Monitor, enter **/IPMON**.

From the monitor, you can [enter a command next to a CICMON resource](#) (see page 108) to perform various functions.

## List CICS Connections from a Socket Management Perspective

**To list CICS connections from a Socket Management perspective**

1. Enter **CL** (Connections List via SocketMgmt) next to a CICMON resource on the IP Resource Monitor.

The SocketMgmt : Connections List appears.

## Display Information About a CICMON Resource

### To display information about a CICMON resource

1. Enter **SQ** (SocketMgmt Query Display) next to a CICMON resource on the IP Resource Monitor.

The SocketMgmt : Information panel appears.

## Stop and Restart CA NetMaster SM for CICS and CA CPT

### To shut down and restart CA NetMaster SM for CICS and CA CPT inside the CICS environment

1. Enter **SR** (SocketMgmt and CPT Recycle) next to a CICMON resource on the IP Resource Monitor.

The SocketMgmt : Recycle Confirmation panel appears.

2. (Optional) Complete the following field:

#### **T09CONxx Startup Config Member Suffix**

Specifies an alternative startup configuration member for the recycle.

Press F6 (Confirm).

The region is recycled and the following message appears:

```
RMCALL25 'SR' COMMAND PROCESSING COMPLETE
```

## Stop and Restart the Command Server Interface

### To stop and restart the Socket Management for CICS command server interface:

1. Enter **SSR** (SocketMgmt CMD Server Recycle) next to a CICMON resource on the IP Resource Monitor.

The SocketMgmt : Recycle Confirmation panel appears.

Press F6 (Confirm).

The command server interface is recycled and the following message appears:

```
RMCALL25 'SSR' COMMAND PROCESSING COMPLETE
```

## Start a CICS Server

### To start a CICS server

1. Enter **SS** (CICS Server Start) next to a CICMON resource on the IP Resource Monitor.  
A confirmation panel appears.
2. Complete the following fields:

#### **Port**

Specifies the TCP/IP port number to use for the CICS server.

#### **(Optional) Transaction ID**

Specifies the CICS transaction name to use for the server.

#### **(Optional) Server Type**

Specifies the type of CICS server to start.

#### **(Optional) User ID**

Identifies the user to associate with the CICS server.

Press F6 (Confirm).

The CICS server starts.

## Start CICS Transactions

### To start a CICS transaction in a CICS environment:

1. Enter **TS** (CICS Transaction Start) next to a CICMON resource on the IP Resource Monitor.  
A confirmation panel appears.
2. Complete the following fields:

#### **Tran**

Specifies the CICS transaction to start for your server.

#### **Parms**

Specifies the names of any parameters that you want to apply to the CICS transaction.

Press F6 (Confirm).

The CICS transaction starts.

## Monitor CICS Resource Performance

The Monitor CICS Address Space Performance panel displays collected performance data and graphs of selected CICS attributes. You can view CICS attributes to ensure their services are available.

### To monitor CICS resource performance

1. Enter **H** (Show Performance History) next to a CICMON resource on the IP Resource Monitor.

The TCP/IP : Monitor CICS Address Space Performance panel appears.

## Monitor CICS IP Traffic

The TCP/IP : Port Traffic Statistics panel shows the number of bytes and packets sent and received by the ports in one-minute intervals over the last five minutes, and the percentage this represents of the total traffic for the stack. You can display the statistics in five-minute intervals over the last hour by pressing F12 (LastHour).

### To display recent byte and packet counts for the IP ports associated with a CICS environment

1. Enter **TRS** (Display IP Traffic Statistics) beside the CICMON class resource on the IP Resource Monitor.

The TCP/IP : Port Traffic Statistics panel appears.



# Chapter 17: Managing IP Security

---

This section contains the following topics:

[IP Network Security Center](#) (see page 185)

[IPSec Management](#) (see page 185)

[How You Access Management Functions](#) (see page 186)

[Limitations](#) (see page 186)

## 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.

### More information:

[Managing Connections](#) (see page 73)

[Using SmartTrace](#) (see page 195)

[IPSec Packets](#) (see page 217)

[TLS and SSL Handshake Packets](#) (see page 217)

## IPSec Management

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.

## How You Access Management Functions

You can access management functions for IPsec from either the IPsec menu using the /IPSEC panel shortcut or a STACK resource on the IP Resource Monitor using line commands. You can perform the following tasks:

- View a summary of the IPsec status, including the status of IP filters and statistics on tunnels.
- View the performance trend of IPsec attributes monitored by a STACK resource.
- List and view the details of the following objects:
  - IP filters
  - Internet Key Exchange (IKE) tunnels
  - Dynamic tunnels
  - Manual tunnels
- Identify the IP filters that affect the traffic between specified IP addresses.

**Note:** For more information about these functions, see the online help.

## Limitations

The following approximate limits apply to the retrieval of lists:

- 375 IP filters
- 400 IKE tunnels
- 400 dynamic tunnels
- 800 manual tunnels

If a list cannot be retrieved because of the limits, use the IPsec menu and use the available fields to restrict the list.

# Chapter 18: Diagnosing IP Networks

---

This section contains the following topics:

[Access Network Diagnosis Functions](#) (see page 187)

[How to Trace a TCP/IP Route](#) (see page 187)

[Browse MIBs](#) (see page 190)

[Browse System Information](#) (see page 190)

[Browse Host Interfaces](#) (see page 191)

[Display a Routing Table](#) (see page 191)

[Test Connectivity](#) (see page 193)

## Access Network Diagnosis Functions

**To display the network diagnosis functions menu**

1. Enter **/IPDIAG** at a prompt.

The Network Diagnosis Functions menu appears.

## How to Trace a TCP/IP Route

It is possible to obtain a hop-by-hop record of the route taken by a packet through a network, starting from the source host and finishing at the destination host.

You can perform a traceroute as follows:

- Directly from the TCP/IP : Network Diagnosis Functions menu
- Use the traceroute action against a host on a list or display; for example on a connection list or the IP Node Monitor
- Issue the TRACEROUTE command from the command line

## Perform a Traceroute From the Network Diagnosis Functions Menu

A traceroute attempts to trace the route from the issuing point through all hosts and routers to the destination host; otherwise it traces the route to the point at which a break in communication has occurred.

### To trace a route to a remote host

1. Enter **/IPDIAG** at the prompt.

The TCP/IP : Network Diagnosis Functions menu appears.

2. Select **TR** - Trace Route and complete the following field:

#### Host Name/Addr

Specifies the name or IP address of the remote host you want to access.

If you want to use a specific address of the local stack interface as the issuing point, select it in the Source Address field. If you want to trace the route through a specific physical interface, select it in the Interface field.

Press Enter.

The TCP/IP : Trace Route Result List panel appears.

## Use Traceroute Action

The Trace Route Result List panel displays the results of the traceroute action. This display is progressively updated as information arrives.

The most likely reason for performing a traceroute action is that a ping is unable to reach a remote host or it is indicating slow response times in the TCP/IP network.

If the host is unreachable, you can take the following actions:

- Perform a traceroute to find out where the failure is occurring.
- Review the Routing Table.

If the host is unreachable, a possible result is Hop Count Exceeded, Network Unreachable, or Host Unreachable.

If the hop count is exceeded and the IP address column on the last entry or entries is an \*, a device is not responding (possibly the destination host). If so, or if the network or host was unreachable, examine the Routing Table or Interfaces for the last listed hop. Apply **I** (Interfaces) or **R** (Routing Table) against the host or router that is recorded as the last hop on the list.

When using the Routing Table action, your TCP/IP management region uses masking. Masking ensures that the presented Routing Table contains only those addresses that are relevant to the path you are tracing. This mask is a network address mask that is based on the class of address being traced. For example, if you are tracing a route to the foreign host 192.168.2.66, your region inserts the mask 192.168.2.\*.

If the hop count is exceeded and the same number of hops is shown in the Hop Limit field, increase the hop limit and reissue the traceroute by pressing F6 (Action).

If the ping indicates a slow response, you can review the following information in your traceroute results:

- Review the Notes column to see if there are any outstanding alerts for the node. If the IP Node Monitor is monitoring the node, look for any alerts are outstanding.
- Review the trip times—these times usually increase at a steady rate the further along the route the packets are sent. A sudden and marked increase in the trip time for a particular hop along the route indicates a possible problem at that hop. To investigate further:
  - Apply the **I** (Interfaces) action to the host or router at the hop where the problem is occurring, and investigate the Interfaces for clues to the performance degradation.
  - Apply the **TN** (Telnet) action to start a Telnet connection to the host or router where the problem is occurring, and investigate the configuration or other possible causes.
- Review the hop list—if there is no evidence of slow trip times, look at the hop list for an unexpected route.

**Note:** To analyze response time problems, use the Transaction Path Analyzer facility.

If the traceroute does not return any abnormal results, use the reporting facility to look for large file transfers.

## Browse MIBs

To access further management information about IP hosts by browsing MIBs, you can access the MIBinsight browser direct from the Network Diagnosis Functions menu.

### To access the MIBinsight browser

1. Enter **/IPDIAG** at a prompt.

The Network Diagnosis Functions menu appears.

2. Type **MB** at the prompt, complete the Host Name/Addr field and any required optional fields, and press Enter.

The MIBinsight Loaded MIBs panel appears.

**Note:** The first time you select the MIBinsight browser function, you are redirected to the MIBinsight : User Security Details panel to enter your SNMP security details. This is the same panel that appears if you select option MS - MIBinsight User Security Details on the Network Diagnosis Functions menu.

3. Enter **S** beside a MIB to browse it.

The MIBinsight browser appears displaying the objects in the selected MIB.

### More information:

[Using MIBinsight](#) (see page 263)

## Browse System Information

### To browse system information for a selected IP host

1. Enter **/IPDIAG**.

The Network Diagnosis Functions menu appears.

2. Type **SI** at the prompt, complete the Name/Addr field and any required optional fields, and press Enter.

The System Information panel appears.

**Note:** The system information facility uses SNMP MIB-II technology, which is not supported by all hosts. SNMP must be supported on a router for you to be able to view system information about it.

## Browse Host Interfaces

### To view a list of interfaces for a selected IP host

1. Enter **/IPDIAG**.

The Network Diagnosis Functions menu appears.

2. Type **HI** at the prompt, complete the Name/Addr field and any required optional fields, and press Enter.

The Interface List panel appears.

**Note:** The interface list facility uses SNMP MIB-II technology that is not supported by all hosts.

## Display a Routing Table

A routing table holds a list of paths through which hosts can communicate with each other.

You may find that the number of entries in your Routing Table is such that it becomes unmanageable. If this is the case, you can reduce the list by entering a network address or network address mask and using the Refresh command (F6) to rebuild the list.

### To view the routing table for a device

1. Enter **/IPDIAG**.

The Network Diagnosis Functions menu appears.

2. Type **RT** at the prompt, complete the Name/Addr field and any required optional fields, and press Enter.

The Routing Table List panel appears.

**Note:** The routing table facility uses SNMP MIB-II technology, which is not supported by all hosts.

## Actions on the Routing Table

The following actions can be applied to routers appearing in the First Hop column of the routing table:

### **I (Interfaces)**

Presents the Interface List panel for the router listed in the First Hop column. To apply the Interfaces action, enter I to the left of the appropriate routing table entry on the list.

### **M (MIBinsight)**

Presents the MIBinsight browser for the router listed in the First Hop column. To apply the MIBinsight action, enter M to the left of the appropriate routing table entry on the list.

### **NL (NameLookup)**

Returns the full name of the router listed in the First Hop column.

### **P (Ping)**

Executes the PING command that tests whether the first hop address is reachable. To apply the Ping action, enter P to the left of the appropriate routing table entry on the list.

### **R (Routing Table)**

Presents the routing table for the router listed in the First Hop column. You can use the Net Address Mask field to limit the presented list.

### **S (System Information)**

Presents the TCP/IP : System Information panel for a selected first hop address. To apply the System Information action, enter S to the left of the appropriate routing table entry on the list.

### **TN (Telnet)**

Initiates a Telnet connection to the router listed in the First Hop column. You can use this connection to enter commands on that router to determine and alter its state.



## Test Connectivity

During problem diagnosis, you can use the PING command to do the following:

- Test whether a host is reachable through the network
- Determine the host name or IP address of a device
- Determine the network transit time for packets of varying sizes
- Determine whether all packets sent reached their destination

You can use a ping action in the following ways:

- Directly check the above information from the TCP/IP : Network Diagnosis Functions menu (/IPDIAG)
- Use the ping action against a host on a list or display; for example on a connection list
- Issue the PING command from the command line.

## Perform a Ping

Performing a ping sends an Internet Control Message Protocol (ICMP) echo request that tests whether the remote host is reachable through the network and how long a return trip takes.

### To test connectivity by sending a ping to a remote host

1. Enter **/IPDIAG** at the prompt.

The TCP/IP : Network Diagnosis Functions menu appears.

2. Type **P** at the prompt and complete the following field:

#### Host Name/Addr

Specifies the name or IP address of the remote host you want to access.

If you want to use a specific address of the local stack interface as the issuing point, select it in the Source Address field. If you want to trace the route through a specific physical interface, select it in the Interface field.

Press Enter.

The TCP/IP : Ping Result List appears.

## Interpret Responses to a Ping

A ping is an end-to-end transmission between your system and a nominated remote host. When a ping is issued, it returns one of the following results:

- Successful
- Packets Lost
- No Response

To determine where on the network, problems such as packet loss, slow response times, or breaks in communication are occurring, you can perform a traceroute.

If, for example, you are investigating poor end-user response times, packet loss or high trip times may indicate that:

- An unexpected route to the host is being used.
- Congestion exists on a link or router along the route to the destination host. For example, if a particular link or router has insufficient capacity, an unusually large file transfer can cause congestion.

The response to a ping appears on the TCP/IP : Ping Result List. The list can be scrolled.

### Example: Response to a Successful ping

The following shows an example of the response to a successful ping.

```

PROD----- TCP/IP : Ping Result list -----
Command ==>                                     Scroll ==> PAGE

Target Host Name .... mercury.dept.company.com
IP Address ... 192.168.2.66
Count ..... 3__
Timeout (seconds) ... 5_
Packet Size ..... 256_
Source Address .....+ _____
Interface .....+ _____
-----
Result ..... Successful
Min/Average/Max Time 10/12/14
Packets sent ..... 3
      received .... 3
      % lost ..... 0
Seq No.   Trip Time (ms)
  1       18
  2       14
  3        *
**END**

```

# Chapter 19: Using SmartTrace

---

This section contains the following topics:

- [SmartTrace](#) (see page 196)
- [SmartTrace Modes](#) (see page 196)
- [SmartTrace Line Command Mode](#) (see page 197)
- [SmartTrace OCS Mode](#) (see page 198)
- [SmartTrace Menu Mode](#) (see page 200)
- [Add a SmartTrace Definition](#) (see page 204)
- [Copy a SmartTrace Definition](#) (see page 205)
- [Activate a SmartTrace Definition](#) (see page 205)
- [Stop a SmartTrace Definition](#) (see page 206)
- [Delete a SmartTrace Definition](#) (see page 206)
- [List SmartTrace Definitions](#) (see page 207)
- [List Active SmartTrace Definitions](#) (see page 207)
- [View a Trace](#) (see page 208)
- [Save a Trace](#) (see page 226)
- [Export a Trace](#) (see page 226)
- [Import a Trace](#) (see page 228)
- [Print a Trace](#) (see page 228)
- [Generate Trace Reports](#) (see page 229)

## SmartTrace

Packet tracing is a valuable tool for troubleshooting network connectivity problems. SmartTrace is a real-time packet tracing facility.

SmartTrace enables you to do the following:

- Initiate a trace on demand (often while a problem is occurring and while you can still catch it), and view the results while the trace is running. You can have separate traces for different resources running at the same time.
- Define trace criteria using a panel interface. You can define a number of traces to wait on infrequent and difficult to capture network activity, and to pinpoint complex failure scenarios. You can also set criteria that cause a trace to stop when matched. Samples are provided to make it easier to define a trace that is relevant to your problem.
- Export trace data to libpcap or CTRACE format, enabling you to use the trace data with other packet trace viewers.
- Import trace data in libpcap format, enabling you to use CA NetMaster NM for TCP/IP to decode packets captured by other means.

CA NetMaster NM for TCP/IP also supports [IBM's Component Trace \(CTRACE\) facility](#) (see page 231).

## SmartTrace Modes

You can initiate a packet trace using one of the following modes. Typically, you use line commands from monitors to trace specific resources. You use menus and OCS for more advanced tracing.

### Line Command

You can initiate a trace by using a line command from the IP Node Monitor, IP Resource Monitor, or a connection list. Using line command is the easiest mode of initiating a trace because all the information required to define the trace is already present.

### OCS

You can schedule the activation of a SmartTrace definition by using timer commands.

### Menu

This mode provides flexibility for an advanced user to specify customized tracing criteria that is not available with line commands. You can use this mode when diagnosing complex problems.

## SmartTrace Line Command Mode

You can use the following line commands from the IP Node Monitor, IP Resource Monitor, and connection lists to manage simple traces:

### PT (Activate Packet Trace)

Starts a packet trace for the selected entry. In most cases, a panel appears for you to specify additional filter criteria.

**Note:** The SMARTTRACE parameter group determines the number of packets that are retained for a trace.

### PTI (Inactivate Packet Trace)

Stops the current packet trace for the selected entry. A stopped trace remains viewable for a time as specified in the SMARTTRACE parameter group.

### PTD (Inactivate and Delete Packet Trace)

Deletes the packet trace and all associated packet trace data for the selected entry.

### PTV (View Packet Trace)

Views the packets that the current packet trace collects.

### Example: Trace a Connection

You enter PT against an IP connection on a Connections panel to start a packet trace:

```
COMP44----- TCP/IP : Connections -----Stack: *MULTIPLE*
Command ==>                                     Scroll ==> CSR

Line 518 of 550                                Refresh Every ...      Seconds
          S=View I=Information CS=Statistics PT=Packet Trace Z=Drop ?=Actions
Foreign      Local
Host         Port Host         LPort TaskName Status      Idle
PT 172.31.122.204 1770 192.168.65.11 3001 COMP1 ESTABLISHED 0:09:41
   172.31.122.209 2676 192.168.65.11 3001 COMP1 ESTABLISHED 0:03:45
   172.31.122.209 2680 192.168.65.11 3001 COMP1 ESTABLISHED 3:39:49
```

After the trace has started (as indicated by \*PT\*), you can enter PTV against the connection to view the trace.

```
PTV 172.31.122.209 2676 192.168.65.11 3001 COMP1 ESTABLISHED *PT*
```

The following panel shows some of the traced packets:

```
COMP44----- SmartTrace : Connection Packet List -----
Command ==>                                         Scroll ==> CSR
                                                    S/V=View P=Print
Stack .... TCPIP11                                Total Traced 334
Local Host 192.168.65.11                          <--> Foreign Host 172.31.122.209
Local Port 3001                                    Foreign Port 2676
Protocol TCP

  Dir  +Time  Bytes  Summary Information
0001  -> <0.001    70  Ack Psh Win=32738 Seq=2044186642 Ack=1239670188
0002  <-   0.643    40  Ack Psh Win=32738 Seq=1239670188 Ack=2044186672
0003  <-   0.713    70  Ack Psh Win=32738 Seq=1239670188 Ack=2044186672
```

You can refresh the panel to see the latest packets, drill down to the individual packet detail, or go back to the connection list to stop the trace.

**More information:**

[View a Trace](#) (see page 208)

## SmartTrace OCS Mode

You can activate and inactivate a SmartTrace definition by using OCS commands.

## Schedule Tracing from OCS

You can schedule a trace from OCS or Command Entry by activating and stopping a trace definition at defined times.

To start a trace at a defined time, issue the following command in conjunction with the AT command:

TRCACT *name*

To stop a trace at a defined time, issue the following command in conjunction with the AT command:

TRCINACT *name*

***name***

Specifies the name of an existing SmartTrace definition.

### Example

To schedule a trace definition called Trace1 to activate at 22:00 and stop at 23:00, issue the following commands:

AT 22.00.00 ROUTE=SYS CMD=TRCACT Trace1

AT 23.00.00 ROUTE=SYS CMD=TRCINACT Trace1

## SmartTrace Menu Mode

Using SmartTrace in menu mode is slightly less simple than Line Command mode; but offers more comprehensive and powerful trace management. Although the PT line command provides the quickest way to start a packet trace, it has limited ability to select the packets to include. You can end up with too many packets. This behavior is important because the SMARTTRACE parameter group limits the number of packets in a PT trace. When the limit is exceeded, a new packet replaces the oldest packet.

In menu mode, you create your own custom trace definitions. The definitions provide the following features:

- Filter the packets to include in the trace.  
  
For example, you want to know if an unauthorized FTP server is being used in the network. You can define a TCP trace to include all packets containing FTP commands directed to a port number other than port 21.
- Stop a trace automatically when a known condition is satisfied.  
  
For example, the remote server is disconnecting a Telnet session. To disconnect a session, the remote server issues a TCP RST flag. You can define a TCP trace with a stop condition that scans for the TCP RST flag. Using this definition, packets are traced up to the moment the remote server issues a TCP RST flag.
- Specify the number of packets to include in the trace after a stop condition is satisfied.
- Stop a trace when a specified number of packets are captured.

All menu mode functions are accessed from the Packet Tracing Menu.

## Access Packet Tracing Menu

The Packet Tracing Menu enables you to manage and perform advanced packet tracing functions.

### To access the Packet Tracing Menu

1. Enter **/SMART** (or **/IPPKT**) from the prompt.

The Packet Tracing Menu appears.

**Note:** For information about the menu, press F1 (Help).



## Definition Types

The following definition types are available for you to create SmartTrace definitions:

### **TCP Trace**

Provides field criteria specific to the TCP protocol. This is commonly used for tracing TCP applications such as Telnet or FTP.

### **UDP Trace**

Provides field criteria specific to the UDP protocol. This is commonly used for tracing UDP applications such as SNMP.

### **ICMP Trace**

Provides field criteria specific to the ICMP protocol. ICMP generates error messages and conditions that are normally acted upon by the IP stack. ICMP is used by the PING and TRACERT commands.

### **General Trace**

Provides field criteria for general tracing.

### **Multiple TCP Connection Trace**

Provides field criteria for a special type of TCP trace. These definitions let you trace packets in specified TCP connections that are initiated after the trace is activated. This type of trace provides initial TCP handshake tracing for each connection and creates a separate trace entry per connection.

Trace definition samples are provided as templates for you to define traces. These definitions describe common network conditions and events that are worth tracing.

## Selection Criteria

Packet tracing often results in many packet entries, most of which are not relevant. SmartTrace provides the following types of selection criteria to help limit the trace output:

### Capture

Limits the captured packets based on the specified criteria.

### Stop

Stops a trace automatically based on the specified criteria and optionally performs a specified action. The stop criteria apply only to packets that pass the capture criteria.

### Connection

(Multiple TCP Connection trace only) Limits tracing to TCP packets that pass the specified connection selection criteria. The criteria applies only to new TCP connections initiated at the time the trace starts. The normal Capture and Stop criteria is then applied to each TCP packet.

### Example: Trace New Connections Between Specific Hosts

The following example selects only newly-initiated TCP connections with a local host of 172.31.255.255, local port of 1123, and a foreign host of 172.16.0.0.

```
PROD----- SmartTrace : Multiple TCP Connection Trace Details -----
Command ==>                                                                    Page 1 of 4

Name .....
Description .....

Trace Each Connection With:
  TCP/IP Stack .....+
  Local Host ..... 172.31.255.255
  Local Ports ..... 1123
  Foreign Host ..... 172.16.0.0
  Foreign Ports.....
```

### Example: Capture Packets with Specific Flags and Data

The following example selects only the TCP packets in the previous example that have a TCP flag of SYN, ACK, or PSH, and contains the string USER between positions 1 and 20 of the TCP data.

```

PROD----- SmartTrace : Multiple TCP Connection Trace Details -----
Command ==>                                                    Page 2 of 4

After the Initial Packets, Trace Packets with:
  TCP Flags .....+ SYN or ACK or PSH
                    (SYN,ACK,PSH,RST,URG,FIN or an expression e.g. SYN and not ACK)

. Packet Data (Following TCP Header) -----
|                                     |
| Oper  Data                        | Format  Start |
| 1 LIKE USER                      | ASCII   Pos.  Length |
|                                     |                                     |

```

### Example: Stop Tracing on the TCP RST Flag

The following example stops the trace when a captured packet has a TCP flag of RST.

```

PROD----- SmartTrace : Multiple TCP Connection Trace Details -----
Command ==>                                                    Page 3 of 4

Stop After Tracing a Packet with:
  TCP Flags .....+ RST
                    (SYN,ACK,PSH,RST,URG,FIN or an expression e.g. SYN and not ACK)
  TCP Window Size .....+

```

### Example: Stop Tracing After a Specified Number of Packets

The following example stops the trace when 2000 packets are captured.

```

PROD----- SmartTrace : Multiple TCP Connection Trace Details -----
Command ==>                                                    Page 4 of 4

Trace Options:
  Trace Limit ..... 2000 (Number of packets)
  Stop At Limit? ..... YES (Yes or No)

```

## Add a SmartTrace Definition

A SmartTrace definition sets up the criteria for a trace. You can have multiple definitions to capture different packets.

### To add a SmartTrace Definition

1. Enter **/SMART** (or **/IPPKT**) from the prompt.  
The Packet Tracing Menu appears.
2. (Optional) Complete the following field:  
**Link Name**  
Specifies the INMC link to the remote system where you want to perform the packet tracing functions.
3. Enter **A** (Add SmartTrace Definition) at the prompt.  
The SmartTrace : Definitions panel appears.
4. Enter **S** beside the definition type that you want to create.  
The relevant Trace Details panel appears.
5. Complete the fields, as required. Press F8 (Forward) to scroll through the panels. If you specify a stop condition on Page 3, you can also press F11 (StopAct) to specify an action for that condition.  
**Note:** For more information about the fields, press F1 (Help).  
**Note:** The default number of packets retained for a trace is determined by the SMARTTRACE parameter group. However, you can override this number in your definition through the Trace Limit field.  
Press F3 (File).  
The following message appears if the fields are completed correctly:  
IPPT8604 Press F3 to FILE; F6 to FILE and ACTIVATE; Enter to RESUME
6. Do *one* of the following:
  - Press F3 (File) to save the definition without activating.
  - Press F6 (Action) to save and activate the definition.
  - Press Enter to resume editing the definition.

## Copy a SmartTrace Definition

If you want to create a SmartTrace definition that is similar to another, it may be quicker to copy the existing definition and edit it accordingly.

### To copy a SmartTrace Definition

1. Enter **/SMART** (or **/IPPKT**) from the prompt.  
The Packet Tracing Menu appears.
2. Enter **L** (List all SmartTrace Definitions) at the prompt.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Enter **C** beside the definition that you want to copy.  
The relevant Trace Details panel appears.
4. Enter a new name in the Name field and edit the other fields, as required.

**Note:** Press F1 (Help) for more information about the fields.

Press F3 (File).

The following message appears if the fields are completed correctly:

IPPT8604 Press F3 to FILE; F6 to FILE and ACTIVATE; Enter to RESUME

5. Do *one* of the following:
  - Press F3 (File) to save the definition without activating.
  - Press F6 (Action) to save and activate the definition.
  - Press Enter to resume editing the definition.

## Activate a SmartTrace Definition

Using a SmartTrace definition, you can start a trace based on the specified criteria.

### To activate a SmartTrace definition

1. Enter **/SMART** (or **/IPPKT**) from the prompt.  
The Packet Tracing Menu appears.
2. Enter **L** (List all SmartTrace Definitions) at the prompt.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Enter **A** (Activate) beside the definition that you want to activate.  
A confirmation message appears.
4. Press Enter.  
The trace is activated, and the definition's status changes to ACTIVE.

## Stop a SmartTrace Definition

A SmartTrace definition with an ACTIVE status indicates that a trace is in progress using that definition. You can stop the trace by inactivating the definition.

**To stop a SmartTrace definition:**

1. Enter **/SMART** (or **/IPPKT**) from the prompt.  
The Packet Tracing Menu appears.
2. Enter **L** (List all SmartTrace Definitions) at the prompt.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Enter **I** (Inactivate) beside the definition that you want to stop.  
A confirmation message appears.
4. Press Enter.  
The trace is stopped, and the definition's status changes to INACTIVE.

## Delete a SmartTrace Definition

When a SmartTrace definition is no longer required, you can delete it.

**To delete a SmartTrace definition:**

1. Enter **/SMART** (or **/IPPKT**) from the prompt.  
The Packet Tracing Menu appears.
2. Enter **L** (List all SmartTrace Definitions) at the prompt.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Enter **D** (Delete) beside the definition that you want to delete.  
The definition and all subentries are removed from the list.

## List SmartTrace Definitions

You can list all SmartTrace definitions and then manage the traces using line commands.

**Note:** This option does not list SmartTrace definitions implicitly created using the line commands from the IP Resource Monitor, IP Node Monitor, and connection lists.

### To list all SmartTrace definitions

1. Enter **/SMART** (or **/IPPKT**) from the prompt.

The Packet Tracing Menu appears.

2. Enter **L** (List All SmartTrace Definitions).

The SmartTrace : Packet Trace Definitions panel appears listing all SmartTrace definitions.

**Note:** Use the **VIEW** command to specify the types of traces listed. For more information, see the online help.

## List Active SmartTrace Definitions

You can list all active SmartTrace definitions and then manage the trace using line commands.

**Note:** This option does not list SmartTrace definitions implicitly created using the line commands from the IP Resource Monitor, IP Node Monitor, and connection lists.

### To list all active SmartTrace definitions

1. Enter **/SMART** (or **/IPPKT**) from the prompt.

The Packet Tracing Menu appears.

2. Enter **LA** (List Active SmartTrace Definitions).

The SmartTrace : Packet Trace Definitions panel appears listing:

- Active SmartTrace definitions.
- Inactive definitions that currently have traces.
- Saved traces that do not have associated definitions.

## View a Trace

You can view a packet trace from the following locations:

- From the IP Resource Monitor, IP Node Monitor, or connection list (after activating a trace with the PT command)
- From the Packet Tracing Menu through a list of packet tracing definitions

The trace provides information about the flow of packets and helps you diagnose network problems.

**Note:** The data displayed depends on your security access. For more information, see your Security Administrator.

The following examples show how traces can help you identify conditions that can contribute to poor response time.

### Example: Packet Fragmentation

If a packet is too large and becomes fragmented, it needs to be reassembled at the destination. The process of fragmentation and reassembly can contribute to poor response time.

If a packet has been fragmented, it is indicated under the Summary Information column on the Packet List panel.

```

PROD----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR
                                                S/V=View P=Print

Definition UDP2
Stack .... TCPIP11
Local Port 8011
Protocol  UDP

Total Traced 32

   Local Host   Dir Foreign Host   Port   +Time  Bytes  Summary Infor
0008 192.168.65.11 -> 192.168.65.31 32317 <0.001 1492  (Frag)
0009 192.168.65.11 <- 192.168.65.31 32317 4.005 1492  (Frag)
0010 192.168.65.11 -> 192.168.65.31 32317 <0.001 1492  (Frag)

```



### Example: Retransmissions

When packets are lost, the lost segment or segments are retransmitted. Retransmissions can contribute to poor response time.

One way that TCP detects packet loss relies on the fact that when an out-of-order segment is received, the receiver generates a duplicate acknowledgement for the highest in-order data byte received. A single duplicate acknowledgement is not a reliable indicator of packet loss because the packets may have been delivered, but not in the original order. TCP distinguishes between these cases by using three duplicate acknowledgements as an indicator of packet loss. When the sending TCP receives the third duplicate acknowledgement, it retransmits the segment referenced by the duplicate ACK number. This is referred to as fast retransmission.

In the following example, the segment with relative sequence number (RelSeq) 1419406 was lost. Packet numbers 1522 through 1524 are duplicate acknowledgements of all data up to the segment with relative sequence number 1419406. Packet number 1524, being the third duplicate acknowledgement, triggers fast retransmission, and packet number 1525 is the retransmission of the segment.

```

PROD----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR
                                           S/V=View P=Print

Definition FTP
Stack .... TCPIP11
Local Host 192.168.65.11
Local Port 20
Protocol TCP

Total Traced 1697
<--> Foreign Host 192.168.135.39
Foreign Port 4177

  Dir  +Time  Bytes  Summary Information
1520  -> <0.001  1492  Ack Psh Win=32768 RelSeq=1482061 RelAck=1 TimeStamp
1521  <-  0.043    52  Ack Win=64095 RelSeq=1 RelAck=1419406 TimeStamp
1522  <-  0.007    52  Ack Win=64095 RelSeq=1 RelAck=1419406 TimeStamp
1523  <-  0.007    52  Ack Win=64095 RelSeq=1 RelAck=1419406 TimeStamp
1524  <-  0.008    52  Ack Win=64095 RelSeq=1 RelAck=1419406 TimeStamp
1525  -> <0.001  1492  Ack Psh Win=32768 RelSeq=1419406 RelAck=1 TimeStamp

```

### Example: Window Size to Receive Data

Each end of a TCP connection advertises a window size that specifies the size of the buffer that is available to receive data. The size changes as data is moved into or out of the buffer. If the receiver advertises a window size of 0 (a closed window), it stops the data transfer. Closed windows can contribute to poor response time.

When a window is closed, a subsequent TCP segment must be sent to open the window by advertising a nonzero window size.

In the following example, the local end of the connection advertises a window size of 4096 in packet number 0309. After receiving three data packets (0312 through 0314) with a total of 4096 data bytes (excluding the headers), it closes the window with packet number 0315. After a short delay, the local application apparently received 2048 bytes of data, freeing up some local buffer space. The window is reopened with packet number 0317 that advertises a window size of 2048.

```
PROD----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR
                                           S/V=View P=Print

Definition TCP1
Stack .... TCPIP11                               Total Traced 334
Local Host 192.168.65.11
Local Port 8011
Protocol   TCP

   Dir Foreign Host    Port  +Time  Bytes  Summary Information
0309 -> 192.168.65.31   3375  <0.001   52  Ack Psh Win=4096 Seq=25131163
0310 <- 192.168.65.31   3375   0.001   52  Ack Psh Win=6144 Seq=56108795
0311 <- 192.168.65.31   3375  <0.001   52  Ack Psh Win=8192 Seq=56108795
0312 <- 192.168.65.31   3375  <0.001  1492  Ack      Win=8192 Seq=56108795
0313 <- 192.168.65.31   3375  <0.001  1492  Ack      Win=8192 Seq=56108939
0314 <- 192.168.65.31   3375  <0.001  1268  Ack Psh Win=8192 Seq=56109083
0315 -> 192.168.65.31   3375  <0.001   52  Ack Psh Win=0 Seq=2513116335
0316 -> 192.168.65.31   3375  <0.001  1076  Ack Psh Win=0 Seq=2513116335
0317 -> 192.168.65.31   3375  <0.001  1076  Ack Psh Win=2048 Seq=25131173
```

## View a Trace from a Resource or a Connection

After you have started a trace, you can view the traced packets.

To view a trace from a resource or a connection, enter **PTV** next to the resource or connection.

The SmartTrace : Packet List appears.

## View a Trace from the Packet Tracing Menu

The Packet Tracing Menu lets you list running or saved traces, which you can view.

### To view a trace from the Packet Tracing Menu

1. Enter **/IPPKT** at the prompt.  
The Packet Tracing Menu appears.
2. Select the option for the type of definitions that you want to display.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Position your cursor next to the definition for the packet trace you want to view, and press Enter.  
The definition expands to list the packet traces.
4. Enter **V** (View) or **S** next to the packet trace.  
The SmartTrace : Packet List appears, listing the packets in the trace.  
**Note:** If authorized, you can enter the EE command at the Command prompt to view UDP packets as EE packets.
5. (Optional) Enter **PRINTLIST** at the Command prompt to print the packets list.

## Locate Packet Data

On a Packet List panel, you can tag packets that contain the data you want to find. You use the TAG command to specify the data you want to locate. The command searches the content of the packets (excluding the IP header) for the specified data. The packets in which the data is located are identified by a TAG flag. You can then use the FIND command to find these flags to locate those packets.

### To locate packet data in the listed packets

1. Enter **TAG**.

The TAG Command Prompt panel appears.

2. Specify the data you want to locate, and then press F6 (Action).

Packets that contain the specified data are tagged, for example:

|      |               |      |    |                |      |        |      |     |     |
|------|---------------|------|----|----------------|------|--------|------|-----|-----|
| 0003 | 192.168.65.11 | 2859 | <- | 192.168.65.61  | 1817 | 0.001  | 82   | Ack | Psh |
| 0004 | 192.168.65.11 | 3001 | <- | 172.24.122.222 | 4607 | 0.009  | 50   | Ack | Psh |
| TAG* | 192.168.65.11 | 3001 | -> | 172.24.122.222 | 4607 | 0.009  | 1492 | Ack |     |
| TAG2 | 192.168.65.11 | 3001 | -> | 172.24.122.222 | 4607 | <0.001 | 1456 | Ack | Psh |
| 0007 | 192.168.65.11 | 7005 | <- | 172.31.9.182   | 2347 | 0.147  | 48   | Syn |     |

3. Use the FIND command to find the tags:

#### **TAGn**

Indicates that the packet contains the data string specified by the *n*th tag.

#### **TAG+**

Indicates that the packet contains *some* of the data strings to be located.

#### **TAG\***

Indicates that the packet contains all the data strings to be located.

To clear selected tags, enter **TAGCLR** and select the tags to clear.

To clear all tags, enter **TAGCLR ALL** or press F3 (Exit) to exit the Packet List panel.

## Decode Packet Data for Specific Protocols and Ports

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 (OSPF/IGP)
- Transport Layer Security (TLS) and Secure Sockets Layer (SSL) handshake
- User Datagram Protocol (UDP) (for Enterprise Extender data only)

**Note:** Only data packets with header information are decoded. If the data spans multiple packets, only the first packet is decoded.

**To decode packet data for other ports**

1. Enter **DECODE**.  
The DECODE Command Prompt panel appears.
2. Specify the port number for the ports you want to decode, and press F6 (Action).  
A message appears, indicating that ports are defined for decoding. Part of the decoded information appears under Summary Information.
3. Enter **S** next to a decoded packet to view all the decoded information.  
The Formatted Packet Display panel appears, showing the decoded information.

After you specify the decoding of certain ports, you can disable their decoding for the currently listed packets by server port type.

To disable the decoding of user-specified ports for a server type, enter **DECODE *server\_port\_type* OFF**.

**Note:** For more information about the syntax of the command, see the online help.

### Example: Decoding of Packets on Port 21

The following example shows the decoding of Port 21:

|                    |               |       |     |                         |      |        |       |         |
|--------------------|---------------|-------|-----|-------------------------|------|--------|-------|---------|
| Definition FTP31   |               |       |     | Description USER001 FTP |      |        |       |         |
| Stack .... TCPIP11 |               |       |     |                         |      |        |       |         |
| Protocol TCP       |               |       |     |                         |      |        |       |         |
|                    | Local Host    | LPort | Dir | Foreign Host            | Port | +Time  | Bytes | Summary |
| 0001               | 192.168.65.11 | 1433  | ->  | 192.168.65.31           | 21   | -      | 78    | Req: P0 |
| 0002               | 192.168.65.11 | 1433  | <-  | 192.168.65.31           | 21   | <0.001 | 74    | Rsp: 20 |
| 0003               | 192.168.65.11 | 1433  | ->  | 192.168.65.31           | 21   | <0.001 | 58    | Req: NL |
| 0004               | 192.168.65.11 | 1471  | <-  | 192.168.65.31           | 20   | 0.092  | 60    | Syn     |
| 0005               | 192.168.65.11 | 1471  | ->  | 192.168.65.31           | 20   | <0.001 | 60    | Ack Syn |
| 0006               | 192.168.65.11 | 1471  | <-  | 192.168.65.31           | 20   | <0.001 | 52    | Ack     |
| 0007               | 192.168.65.11 | 1433  | <-  | 192.168.65.31           | 21   | <0.001 | 73    | Rsp: 12 |
| 0008               | 192.168.65.11 | 1471  | <-  | 192.168.65.31           | 20   | <0.001 | 84    | Ack Psh |
| 0009               | 192.168.65.11 | 1471  | <-  | 192.168.65.31           | 20   | <0.001 | 52    | Ack Psh |
| 0010               | 192.168.65.11 | 1471  | ->  | 192.168.65.31           | 20   | <0.001 | 52    | Ack     |
| 0011               | 192.168.65.11 | 1471  | ->  | 192.168.65.31           | 20   | <0.001 | 52    | Ack Psh |
| 0012               | 192.168.65.11 | 1471  | <-  | 192.168.65.31           | 20   | <0.001 | 52    | Ack Psh |
| 0013               | 192.168.65.11 | 1433  | ->  | 192.168.65.31           | 21   | 0.214  | 52    | Ack Psh |

**Summary Information**

0001 Req: PORT 141,202,65,11,5,191

0002 Rsp: 200 Port request OK.

0003 Req: NLST

0004 Syn Win=65535 Seq=3986067402 MaxSeg=1452 WScale=3 TimeStamp

0005 Ack Syn Win=65535 Seq=1354158791 Ack=3986067403 MaxSeg=1452 WScale=3

0006 Ack Win=32768 Seq=3986067403 Ack=1354158792 TimeStamp

0007 Rsp: 125 List started OK

0008 Ack Psh Win=32768 Seq=3986067403 Ack=1354158792 TimeStamp

0009 Ack Psh Fin Win=32768 Seq=3986067435 Ack=1354158792 TimeStamp

0010 Ack Win=32768 Seq=1354158792 Ack=3986067436 TimeStamp

0011 Ack Psh Fin Win=32768 Seq=1354158792 Ack=3986067436 TimeStamp

0012 Ack Psh Win=32768 Seq=3986067436 Ack=1354158793 TimeStamp

0013 Ack Psh Win=32747 Seq=1351125108 Ack=3978318867 TimeStamp

Packets 1 through 3 and 7, which use Port 21, are decoded.

Packets 4 through 6 and 8 through 12, which do not use Port 21, are not decoded.

Packet 13, which uses Port 21, is not decoded because it contains no data.

## DRDA Packets

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.

```

PROD17----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR

Stack .... TCP/IP31                               Description db2 connection
Local Host 192.168.65.31                          <--> Foreign Host 192.168.65.31
Local Port 5058                                    Foreign Port 33242
Protocol   TCP

Summary Information
-----
00001 Ack Psh Win=32502 Seq=241242201 Ack=221029324 TimeStamp
00002 SQL-Cmd: 1(PREPARE; SELECT 'T'...) 2(OPEN)
00003 SQL-Rsp: 2(100(02000))
00004 SQL-Cmd: 1(PREPARE; UPDATE esp_jhr_b3...) 2(EXECUTE/ine... ) trune.
00005 DDM-Rsp: End Unit of Work Condition (Sev=4)
00006 SQL-Cmd: 1(PREPARE; SELECT 'T'...) 2(OPEN)
00007 SQL-Rsp: 2(100(02000))
00008 SQL-Cmd: 1(COMMIT)
00009 DDM-Rsp: End Unit of Work Condition (Sev=4)
00010 SQL-Cmd: 1(PREPARE; INSERT INTO...) 2(EXECUTE/ine... ) trune.
00011 DDM-Rsp: End Unit of Work Condition (Sev=4)
00012 Ack Psh Win=32502 Seq=241242206 Ack=221029333 TimeStamp

```

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:

```

PROD17----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR

Stack .... TCP/IP31                               Description db2 connection
Local Host 192.168.65.31                          <--> Foreign Host 192.168.65.31
Local Port 5058                                    Foreign Port 33242
Protocol   TCP

Summary Information
-----
00001 Ack Psh Win=32502 Seq=241242201 Ack=221029324 TimeStamp
00002 Req: 1(PRPSQLSTT SQLATTR SQLSTT) 2(OPNQRY SQLDTA)
00003 Rsp: End of Query (Sev=4)
00004 Req: 1(PRPSQLSTT SQLSTT) 2(EXCSQLSTT SQLDTA/ine ... ) trune.
00005 Rsp: End Unit of Work Condition (Sev=4)
00006 Req: 1(PRPSQLSTT SQLATTR SQLSTT) 2(OPNQRY SQLDTA)
00007 Rsp: End of Query (Sev=4)
00008 Req: 1(RDBCMM)
00009 Rsp: End Unit of Work Condition (Sev=4)
00010 Req: 1(PRPSQLSTT SQLSTT) 2(EXCSQLSTT SQLDTA/ine ... ) trune.
00011 Rsp: End Unit of Work Condition (Sev=4)
00012 Ack Psh Win=32502 Seq=241242206 Ack=221029333 TimeStamp

```



## IPSec Packets

Decoded IPSec packets help network analysts diagnose IPSec problems, for example, error during IKE negotiations.

The following example shows IKE negotiations during the establishment of an Enterprise Extender (EE) connection:

```

PROD17----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR
                                           S/V=View P=Print
Resource   TCP/IP31V                               Class ..... STACK
Stack .... TCP/IP31V                               Description  IPSEC - connected/fail
Local Host *                                     <--> Foreign Host 192.168.66.12

Summary Information
-----
00060 IKEv1 Quick: (Encrypted, Next Payload - HASH)
00061 IKEv1 Informational: (Encrypted, Next Payload - HASH)
00062 TEST Are you there? (local)
00063 IKEv1 Quick: (Encrypted, Next Payload - HASH)
00064 IKEv1 Informational: (Encrypted, Next Payload - HASH)
00065 XDP3 T4 prenegotiation Role=neg CP=SERVER01.A31X99 Link=PUC011 TG=3
00066 IKEv1 Quick: (Encrypted, Next Payload - HASH)

```

## TLS and SSL Handshake Packets

Decoded TLS and SSL handshake packets help network analysts diagnose problems during the negotiations between two applications to establish connection.

The following example shows a typical negotiation:

```

Summary Information
-----
00001 Syn      Win=32767 Seq=2022455702 MaxSeg=16396 WScale=0 Sack-P Time...
00002 Ack Syn  Win=32767 Seq=2026185944 Ack=2022455703 MaxSeg=16396 WScale...
00003 Ack      Win=32767 Seq=2022455703 Ack=2026185945 TimeStamp
00004 SSL2: HSK( CLIENT_HELLO )
00005 Ack      Win=32767 Seq=2026185945 Ack=2022455808 TimeStamp
00006 SSL3: HSK( SERVER_HELLO CERTIFICATE SERVER_HELLO_DONE )
00007 Ack      Win=32767 Seq=2022455808 Ack=2026186974 TimeStamp
00008 SSL3: HSK( CLIENT_KEY_EXCHANGE ) CHANGE_CIPHER HSK( Encrypted )
00009 SSL3: CHANGE_CIPHER HSK( Encrypted )
00010 Ack      Win=32767 Seq=2022456020 Ack=2026186949 TimeStamp
00011 SSL3: APPLICATION_DATA
00012 Ack      Win=32767 Seq=2026186949 Ack=2022456457 TimeStamp
00013 SSL3: HSK( Encrypted )
00014 SSL3: HSK( Encrypted )

```

## SOAP Packets

Decoded SOAP packets help network analysts diagnose problems. By reviewing the decoded data, you can easily identify requests that have failed and gain understanding of the data flow that transpires during a web service exchange.

Decoding is limited to HTTP as the underlying protocol for transporting SOAP messages.

The following example shows an error condition:

```
PROD17----- SmartTrace : Packet List -----
Command ==>                                     Scroll ==> CSR
                                           S/V=View P=Print

Resource   WRKAUTO2                               Class ..... ASMON
Stack .... TCP/IP31                             Description  SOAP workload auto web
Local Host 192.168.65.31                         <--> Foreign Host 172.24.4.36
Local Port 8940                                  Foreign Port 3680
Protocol   TCP

Summary Information
Initial packets for connection:
-----
00001 Syn      Win=16384 RelSeq=0 MaxSeg=1460 Sack=P
00002 Ack Syn  Win=32768 RelSeq=0 RelAck=1 MaxSeg=1462
00003 Ack      Win=17424 RelSeq=1 RelAck=1
00004 SOAP-Req: <Body> <startWork>
00005 Ack      Win=31864 RelSeq=1 RelAck=905
00006 SOAP-Rsp: <Fault> <faultcode>soapenv:WACA71010E Call to CA 7 failed <
00007 Ack Psh  Fin Win=31864 RelSeq=937 RelAck=905
00008 Ack      Win=16488 RelSeq=905 RelAck=938
00009 Ack Fin  Win=16488 RelSeq=905 RelAck=938
00010 Ack Psh  Win=31864 RelSeq=938 RelAck=905
***** Bottom of data *****
```

Typically, SOAP packets are segmented. You can view the reassembled packets using data flow reports.

## Hide Decoded Information from the Packet List

During diagnosis, you may want to see the summary information about TCP instead of the decoded FTP, HTTP, and Telnet ports. For example, you may want to find out about the window sizes and sequence numbers across a number of packets. The TCPSUMM command lets you hide any decoded information temporarily on the Packet List panel.

To hide decoded information from the packet list, enter **TCPSUMM** at the Command prompt.

To redisplay the decoded information, press F6 (Refresh).

## View Packet Data

From Packet List, you can view the details of a packet. You can view the details in different formats.

### To view the packet data

1. Enter **V** (View) or **S** beside the packet that you want to view.

The details appear.

**Note:** To view the actual data in a packet, you must have authority.

2. (Optional) Press F6 (Format) to cycle through the formats.

The format of the displayed details changes.

## Formatted Packet Display

The contents of the Formatted Packet Display vary according to the type of packet and its contents. There are three display formats for the Formatted Packet Display. You can move between the three display formats by pressing F6 (Format).

### Format A

```

PROD----- TCP/IP : Formatted Packet Display -----Columns 001 079
Command ==>                                         Scroll ==> PAGE

***** TOP OF DATA *****
PKT  Packet # ..... 00000002   Direction ..... Recv
     Date ..... 19-SEP-2006   Time ..... 10:16:58.408203
     Link Name .... OSATRO

IP   Source Addr ..... 10.16.91.126   Destination Addr ... 10.16.77.25
     IP Version ..... 4               Header Length ..... 5
     Type of Service . B'00000000'    Total Length ..... 40
     Identification .. 47203          Flags ..... B'010'
     Frag Offset ..... 0              Time To Live ..... 125
     Protocol ..... TCP               Header Chksum ..... X'0BD4'

TCP  Src Port ..... 2336             Dest Port ... TELNET
     Seq Number ..... X'F9F3F6F5'    Ack Number .. X'F6F8F3F4'
     Data Offset ..... 20             Flags ..... ACK
     Window ..... 8638                Checksum .... X'C06C'
     Urgent Pointer .. 0

```

## Format B

```

PROD----- TCP/IP : Formatted Packet Display -----Columns 001 079
Command ==>                                         Scroll ==> PAGE

***** TOP OF DATA *****
PKT  Packet # .... 00000002   Direction ..... Recv
     Date ..... 19-SEP-2006   Time ..... 10:16:58.408203
     Link Name .... OSATR0

IP   Source Addr ..... 10.16.91.126   Destination Addr ... 10.16.77.25
     IP Version ..... 4               Header Length ..... 5
     Type of Service . B'00000000'    Total Length ..... 40
     Identification .. 47203          Flags ..... B'010'
     Frag Offset ..... 0              Time To Live ..... 125
     Protocol ..... TCP               Header Chksum ..... X'0BD4'

           +----- IP Header -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 45000028 B8634000 7D060BD4 C7005B7E      ' MG $= E ( c@ } ~
+0010 C7005019                                G &                               P

TCP  Src Port ..... 2336             Dest Port ... TELNET
     Seq Number ..... X'F9F3F6F5'    Ack Number .. X'F6F8F3F4'
     Data Offset ..... 20             Flags ..... ACK

```

## Format C

```

***** TOP OF DATA *****
PKT  Packet # .... 00000002   Direction ..... Recv
     Date ..... 19-SEP-2006   Time ..... 10:16:58.408203
     Link Name .... OSATR0

           +----- IP Header Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 45000028 B8634000 7D060BD4 C7005B7E      ' MG $= E ( c@ } ~
+0010 C7005019                                G &                               P

           +----- IP Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 09200017 28BCF407 37D33643 501021BE      4 L & ( 7 6CP !
+0010 C06C0000                                { %                               l
***** BOTTOM OF DATA *****

```

**Note:** For more information about the information displayed, see the *Request for Comments* (RFC) for the protocol being used:

- RFC 791 for IP
- RFC 793, RFC 1323, and RFC 2018 for TCP
- RFC 768 for UDP
- RFC 792 for ICMP

The Formatted Packet Display shows several groups of data. Some of these groups of data are displayed in only one format of the panel; others are displayed in two or three of the formats.

Each group of data relates to one of the following:

- The packet as a whole
- IP
- The related protocol (TCP, UDP, or ICMP)

The following table identifies the groups of data displayed in the different formats:

| Format | Data Displayed   |
|--------|--|
| A      | Packet details<br>IP header fields<br>IP options<br>Protocol header fields<br>Protocol data                                      |
| B      | Packet details<br>IP header fields<br>IP options<br>IP header<br>Protocol header fields<br>Protocol header data<br>Protocol data |
| C      | Packet details<br>IP header<br>IP data   |

## Packet Details on the Formatted Packet Display

Packet details are displayed in all three formats of the Formatted Packet Display.

|     |                 |             |                 |                 |
|-----|-----------------|-------------|-----------------|-----------------|
| PKT | Packet # .....  | 00000002    | Direction ..... | Send            |
|     | Date .....      | 12-Mar-2006 | Time .....      | 15:32:09.456064 |
|     | Link Name ..... | IUCVLNK     |                 |                 |

## IP Header Fields on the Formatted Packet Display

The IP header fields for the packet are displayed in Format A and Format B of the Formatted Packet Display.

|                   |             |                     |         |
|-------------------|-------------|---------------------|---------|
| IP Version .....  | 4           | Header Length ..... | 5       |
| Type of Service . | B'00000000' | Total Length .....  | 472     |
| Identification .. | 22900       | Flags .....         | B'000'  |
| Frag Offset ..... | 0           | Time To Live .....  | 60      |
| Protocol .....    | UDP         | Header Chksum ..... | X'D555' |

## IP Options on the Formatted Packet Display

For some packets, there is a group of items displayed as IP options in Format A of the Formatted Packet Display.

```
OPTION=COPY  CONTROL  LOOSE_SRC  LEN=11  PTR=4
      1.2.3.4
      5.6.7.8
OPTION=NOCOPY CONTROL  END_LIST
```

**Note:** For more information about IP options, see *RFC 791*.

## Protocol Header Fields on the Formatted Packet Display

Protocol header fields are displayed in Format A and Format B of the Formatted Packet Display. The header displayed depends on the protocol: TCP, UDP, or ICMP.

### TCP Header Fields on the Formatted Packet Display

```
TCP  Src Port ..... TELNET           Dest Port ... 3355
      Seq Number ..... X'F9F3F6F5'      Ack Number .. X'F6F8F3F4'
      Data Offset ..... 20              Flags ..... ACK PSH
      Window ..... 1853                Checksum .... X'6981'
      Urgent Pointer .. 0
```

### UDP Header Fields on the Formatted Packet Display

```
UDP  Src Port ..... 53                Dest Port ... 1173
      Length ..... 94                  Checksum .... X'BE47'
```

### ICMP Header Fields on the Formatted Packet Display

```
ICMP Msg Type ..... Echo Request
      Code ..... 0
      Checksum ..... X'7A94'
      Identifier ..... 12
      Sequence Number ..... 0
```

## TCP Options on the Formatted Packet Display

For some packets, there is a group of items displayed as TCP options in Format A of the Formatted Packet Display.

| TCP Option           | Value |
|----------------------|-------|
| -----                | ----- |
| Maximum Segment Size | 255   |
| No Operation         |       |
| End Of Options List  |       |

## Protocol Data on the Formatted Packet Display

Protocol data appears in Format A and Format B of the Formatted Packet Display. Protocol header data appears in Format B only.

The details displayed depend on the protocol: TCP, UDP, or ICMP. The packet's data is displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

### TCP Data on the Formatted Packet Display

```

+----- TCP Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 3C404000 13114040 2902C0E8 42F5E2E3      {Y 5ST <@@ (@@) B
+0010 D5D4F13C 40616029 02C0E842 F5E2A385 AB1 /- {Y 5Abc <(@a) B
+0020 8740E296 12A3A456 12345678 C0E842F5 g Software {Y 5 @ ) B
+0030 3CC15060 11C15029 02C0E842 F23CC260 A&- A& {Y 2 B- < P P) B <
+0040 4011C260 2902C0F0 42F43CC2 E6402902 B- {0 4 BW @ ) B < @)
+0050 C0E842F7 4E3CC27D 604E3CC3 12345678 {Y 7+ B'-+ C- B N< }< @)
+0060 C0F042F4 D3E44040 12345678 C0E842F7 {0 4LU {Y 7 B @@@@) B
+0070 D5D5D5D5 D5F0F0F2 11C3F029 02C0F042 aaaaa002 C0 {0 ) B
+0080 F43CC3F6 402902C0 E842F74F 3CC4C67E 4 C6 {Y 7| DF= < @) B 0< ~
+0090 3CC44D40 4F3CC4D6 402902C0 F042F1D6 D( | D0 {0 10 < M@0< @) B
+00A0 2902C0E8 42F7D629 02C0E842 F2D62902 {Y 70 {Y 20 ) B ) B )

```

### TCP Header Data on the Formatted Packet Display

```

+----- TCP Header Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 00170D1B 0DBC6D44 0DA807C4 5018073D      - y D& mD P =
+0010 69810000                                a i

```

### UDP Data on the Formatted Packet Display

```

+----- UDP Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 00018580 00010001 00000000 02353302      e 53
+0010 12345678 12345678 07696E2D 61646472      > / 90 0 192 in-addr
+0020 04617270 6100000C 0001C00C 000C0001      / / { arpa
+0030 0000D141 12345678 616E796D 65646502      J /> A ganymede
+0040 12345678 03313939 07696E2D 61646472      > / 90 0 192 in-addr
+0050 04617270 6100      / / arpa

```

## UDP Header Data on the Formatted Packet Display

```

+----- UDP Header -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 00350495 005EBE47          n ;          5      G

```

## ICMP Data on the Formatted Packet Display

```

+----- ICMP Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 48B63B8B 1A1F56FF 10111213 14151617          H ; V
+0010 18191A1B 1C1D1E1F 20212223 24252627          !"#$%&'
+0020 28292A2B 2C2D2E2F 30313233 34353637          ()*+,-./01234567
+0030 38393A3B 3C3D3E3F 40414243 44454647          89:;<=>?@ABCDEFGH
+0040 48494A4B 4C4D4E4F 50515253 54555657      ¢.<(+|&      HIJKLMNPOQRSTUVWXYZ
+0050 58595A5B 5C5D5E5F 60616263 64656667      !$*);-/_      XYZ
+0060 68696A6B 6C6D6E6F 70717273 74757677      <x:ad>,%_>?  hijklmnopqrstuvw
+0070 78797A7B 7C7D7E7F 80818283 84858687      :#@'=" abcdefg xyz{<x:ad>}~
+0080 88898A8B 8C8D8E8F 90919293 94959697      hi          jklmnop
+0090 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7      qr          ~stuvw
+00A0 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7      yz

```

## ICMP Header Data on the Formatted Packet Display

```

+----- ICMP Header -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 08007A94 000C0000          :m          z

```

## IP Data on the Formatted Packet Display

```

+----- IP Data -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 00170D1B 0DBC6D44 0DA807C4 5018073D          y D&      mD P =
+0010 12345678 01C21140 40290142 F4114040      a B-      4 i      @a) B @@
+0020 3C404000 12345678 2902C0E8 42F5E2E3          {Y 5ST <@@      @a) B
+0030 D5D4F13C 12345678 02C0E842 F5E2A385      XX1 /- {Y 5Abc      <a) B
+0040 12345678 8740E296 86A3A681 12345678      defgh Software      @      )
+0050 C0E842F5 3CC15060 11C15029 02C0E842      {Y 5 A&- A& {Y      B < P P) B
+0060 F23CC260 4011C260 2902C0F0 42F43CC2      2 B- B- {0 4 B < @      ) B <
+0070 E6402902 C0E842F7 4E3CC27D 604E3CC3      W {Y 7+ B'-+ C @      ) B N< }<
+0080 60402902 C0F042F4 D3E44040 40402902      - {0 4LU      @      ) B @@@@
+0090 C1E234F5 D5D5D5D5 D5F0F0F2 11C3F029      {Y 7aaaaa002 C0      B      )
+00A0 02C0F042 F43CC3F6 402902C0 E842F74F      {0 4 C6 {Y 7      B < @      ) B 0

```

## IP Header Data on the Formatted Packet Display

```

+----- IP Header -----+ +--- EBCDIC ---+ +--- ASCII ---+
+0000 450004D8 721C0000 3C06A9AB C7005019      Q      z G & E r < P
+0010 C700803E          G          >

```



## Print Packet Data

Both the Packet List panel and the Formatted Packet Display panel let you print the data in a packet..

### To print packet data from Packet List

1. Enter **P** (Print) beside the packet that you want to print.  
The Confirm Printer panel appears.
2. Specify your printing requirements, and press F6 (Confirm).  
The packet details are printed.

### To print packet data from Formatted Packet Display

1. Enter **PRINT** at the Command prompt.  
The Confirm Printer panel appears.
2. Specify your printing requirements, and press F6 (Confirm).  
The packet details are printed.

## Save a Trace

A trace can be in *one* of the following states:

### Running

The trace is currently active.

### Ended

The trace has stopped.

### Saved

The Trace is saved to IPFILE.

**Important!** A trace expires after a period. Also, when a trace is Running or Ended, the trace is deleted if SOLVE SSI terminates. *If you want to retain a trace, you must save it.*

### To save a trace

1. Enter **/IPPKT** from the prompt.

The Packet Tracing Menu appears.

2. Select the option to display the trace that you want to save.

The SmartTrace : Packet Trace Definitions panel appears.

3. Position your cursor beside the SmartTrace definition that you want to save and press Enter.

The packet traces appears.

4. Enter **SAV** beside the packet trace that you want to save.

The SmartTrace : Save Packet Trace dialog appears.

5. Enter a description in the Description field.

The SmartTrace : Packet Trace Definitions panel appears. The trace is saved and the state of the trace is SAVED.

## Export a Trace

You can export a trace to a physical sequential (PS) data set or a z/OS UNIX file. The file can then be viewed by another external application.

If you plan to export to a data set, you must allocate it first with the following requirements:

- **Organization**—PS
- **Record length**—2056 bytes minimum (for libpcap output format) or 27994 bytes minimum (for CTRACE output format)
- **Block size**—(record\_length + 4 bytes) to 32760 bytes
- **Record format**—VB

#### To export a SmartTrace trace

1. Enter **/IPPKT** (or **/SMART**) from the prompt.  
The Packet Tracing Menu appears.
2. Select the option for the type of definitions or traces you want to display.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Position your cursor next to the packet trace that you want to export and press Enter.  
The packet trace details appear.
4. Enter **EX** next to the packet trace that you want to export.  
The Export Packet Trace panel appears.
5. Complete the following fields:

##### **Dataset or HFS File**

Specifies the name of the output file into which the trace is saved. This output can be a PS data set or a z/OS UNIX file.

**Important!** If you are exporting to CTRACE, you must use a PS data set.

##### **Adjust Time By**

Specifies the adjustment value to apply to the timestamp associated with each packet during the export operation. For example, if SmartTrace captured the trace on a mainframe running with TOD clock set to GMT and the trace is viewed on a workstation in the +11:00 time zone, an adjustment of +11:00 is required to make the packet timestamps appear unchanged.

##### **Output Format**

Specifies the format in which the output file is written. Valid values are CTRACE and libpcap.

Press F6 (Action).

The trace is exported.

**Note:** If you FTP this file to a PC to view using a trace application there, ensure that you use an FTP transfer mode of binary.

## Import a Trace

The Packet Tracing Menu contains an option that lets you import a trace file that is in libpcap format. After the file is imported, you can use the SmartTrace features to analyze the trace. The file can be a data set or a z/OS UNIX file (up to 64 KB).

### To import a libpcap trace file

1. Enter the **/LIBPCAP** panel shortcut.  
A panel prompts you for the file.
2. Specify a description for the imported file and the name of the file being imported, and then press F6 (Action).  
The file is imported. You can view the imported file on the Saved Traces List panel.

## Print a Trace

You can print your trace in one of the following formats:

- The entire packet trace
- The list of packets in summary format

### To print a trace

1. Enter **/IPPKT** from the prompt.  
The Packet Tracing Menu appears.
2. Select the option for the type of definitions that you want to display.  
The SmartTrace : Packet Trace Definitions panel appears.
3. Position your cursor next to the packet trace that you want to print and press Enter.  
The packet trace details appear.
4. Position your cursor beside the packet trace that you want to print and do *one* of the following:
  - Enter **P** to print the entire packet trace.
  - Enter **PL** to print the list of packets in summary format.A confirmation dialog appears.
5. Press Enter.  
The PSM : Confirm Printer dialog appears.
6. Complete the details of your printer and press F6 (Confirm).  
The trace is printed.

## Generate Trace Reports

You can generate IPCS reports for a SmartTrace packet trace. The reports generated depend on the contents of the trace and fall into the following categories:

- DRDA Distributed Data Management (DDM) summary reports for connection establishment information between servers
- Data flow reports for TCP sessions (if you are authorized to view data)—The reports shows the data exchanged between TCP peer applications. If the data is segmented, the data is reassembled.
- Session reports for general information about sessions (for example, between two hosts)
- Statistics reports for statistical information about the trace (for example, the number of packets transferred for each protocol used)

You can generate the reports either through the GR action against a trace or through the REPORTS command on a Packet List panel.

### To generate IPCS reports for a packet trace

1. Enter **GR** next to a trace, or enter **REPORTS** on a Packet List panel.

A panel is displayed to show you the progress of the report generation. On completion, it lists the reports. A report name that has a number (in parenthesis) following contains multiple reports.

2. Enter **S** next to a report to view it.

The report is displayed. If the report name indicates multiple reports, it is expanded to list those reports.

You can also print or save a report.



# Chapter 20: Using CTRACE

---

This section contains the following topics:

[CTRACE](#) (see page 231)

[Display CTRACE Packet Tracing Menu](#) (see page 231)

[How to Perform a Trace and Save Data](#) (see page 232)

[View the Saved Packet Trace](#) (see page 234)

[Errors in Packets](#) (see page 241)

[Export a Trace](#) (see page 243)

## CTRACE

CTRACE is an MVS diagnostic service aid. Your region uses it to obtain traces of IP packets flowing to and from a TCP/IP stack on a z/OS Communications Server host.

The CTRACE packet tracing facility includes the following features:

- Ability to start and stop CTRACE (Component Trace)
- Ability to trace IP packets with specified criteria
- A trace format and display facility
- Ability to display active traces
- An archive of trace information
- Ability to export traces to a PS data set or an HFS file in either CTRACE or libpcap format

## Display CTRACE Packet Tracing Menu

The CTRACE Packet Tracing Menu lets you control tracing and list the traces.

### To display the CTRACE Packet Tracing Menu

1. Enter **/CTRACE** at a prompt.

The CTRACE Packet Tracing Menu appears. The options on the menu are listed in the order in which you would normally use them. If you already have a CTRACE data set that contains a TCP/IP packet trace, you can view the trace by firstly saving the trace data using Option SV and then using Option L to list the saved traces.

## How to Perform a Trace and Save Data

### To perform a trace and save the trace data

1. Start trace, which prompts you to start CTRACE if it is inactive.
2. Reproduce the problem you are tracing.
3. Stop trace, which stops CTRACE.
4. Save the packet trace data.

You can also see which traces are currently running, and view saved trace data.

## Start a Trace

Before you can begin tracing packets, you need to start CTRACE (Component Trace). If CTRACE is inactive, you are prompted to start CTRACE. The Start CTRACE panel appears. You can also start CTRACE from the CTRACE Packet Tracing Menu.

**Note:** To trace TCP/IP packets, CTRACE must be started with an external writer. For information about how to create the external writer, see the *Administration Guide*.

### To start a trace

1. Enter **/CTRACE** at the prompt.  
The CTRACE Packet Tracing Menu appears.
2. Select option **PT** (Start Packet Tracing).  
(Optional) Complete the fields to limit your trace.  
Press Enter.  
The Start CTRACE panel appears.
3. (Optional) Change the stack for which you want to start the trace or the contents of the Command to Start CTRACE field.  
The trace is ready to be started with your requirements.
4. Press F6 (Action).  
CTRACE starts, and the trace job values are saved. These saved options are then used as defaults next time you use this panel.  
CA NetMaster NM for TCP/IP issues the command specified in the command field for the specified stack. It then automatically responds to the WTOR messages written to the console during CTRACE start processing.

**Note:** If any errors are encountered when starting CTRACE, error information may be written to the activity log. To view this log, enter **/LOG** at the prompt.



## List Active Traces

To find out what traces you have started, you can list active traces whenever any are running.

### To list active traces

1. Enter **/CTRACE** at the prompt.

The CTRACE Packet Tracing Menu appears.

2. Enter **LA** (List Active Traces).

(Optional) Enter the name of the INMC link to that region in the Link Name field if you want to list active packet traces on a remote region.

Press Enter.

The Active Packet Trace List appears.

## Stop a Trace

Before you can save your trace data, you must stop tracing packets, which also stops CTRACE.

### To stop a trace

1. Enter **/CTRACE** at the prompt.

The CTRACE Packet Tracing Menu appears.

2. Enter **PTC** (Clear Traces).

(Optional) If you want to stop traces on a remote region, specify the name of the INMC link to that region in the Link Name field.

Press Enter.

The Confirm Trace Stop panel appears.

3. Press F6 (Confirm).

The Packet Tracing Menu appears with a message confirming that the trace has been stopped.

## Save CTRACE Data

When you have stopped tracing, you can save the CTRACE records. You need to do this so that you can view the traced packets.

### To save your trace data

1. Enter **/CTRACE** at the prompt.

The CTRACE Packet Tracing Menu appears.

2. Select option **SV** (Save Trace Data).

The Save Trace Data panel appears.

3. Press F6 (Action).

The CTRACE Packet Tracing Menu appears, with a message indicating:

- How many IP packets were saved
- How many IP packets were in error

## View the Saved Packet Trace

After you have saved the packet trace data, you can view it. You can view the following levels of detail:

- The list of saved traces
- IP addresses in a selected trace
- All connections in a trace
- The list of packets in a selected trace
- Data for a selected packet

## List IP Addresses in a Trace

The Packet Trace IP Address List displays a number of IP addresses (sorted in chronological order) in a selected trace. The number of IP addresses listed is the number of IP addresses that can be stored in the packet trace header record. If there are more IP addresses than those listed, a > symbol appears beside that IP address count on the Saved Trace List to indicate this.

### To list IP addresses in a trace

1. Enter **I** (IP Address List) beside an entry on the Saved Trace List.

The IP addresses are displayed.

**Note:** You can access a connection list or a packet list from this panel.

## Sort IP Addresses

The SORT command lets you display the Packet Trace IP Address List in a sort order other than the default chronological order.

The operand values for the command are associated with the column heading of the column you want to sort by. For example, enter **SORT BYTES** to sort the list by the number of bytes.

## SORT Operands

The SORT operands are as follows:

**?**

Displays the available sort values for the list.

**TIME**

Sorts by time of first occurrence of a packet for the address in the trace.

**BYTES**

Sorts by the number of bytes in all packets for the address.

**PKTCOUNT**

Sorts by the number or frequency of packets for the address.

**IPADDR**

Sorts by IP addresses.

### To sort the list

1. Enter **SORT ?** at the prompt.

The Sort Values List appears.

2. Select the sort value you want and press Enter.

The Packet Trace IP Address List appears sorted in the specified order.

**Note:** Alternatively, to change the sort order, issue the SORT xxx command (where xxx is a valid name, for a sort field, that consists of the minimum number of characters (for uniqueness) from the sort column heading). For example, to sort by number of bytes, issue the SORT B command.

## Locate IP Addresses

You can use the LOCATE command to position a particular row at the top of the list.

This command is available only when the IP address list is sorted using the SORT command to change the default sort order.

The value you specify after the LOCATE command applies to the sort value that has been issued on the list. It does not necessarily apply to the first column of the list unless you have sorted by the first column.

### Example

If you have sorted by time (the default sort order), and you issue the L 11:25:00 command, you are positioned at (the line before) the first time that starts with 11:25:00.

## List Saved Traces

The Saved Trace List provides information about the trace, including:

- Save start date
- Save start time
- Save end time
- Save user ID
- A short description of the trace
- Packet count
- Number of IP addresses in the trace

If there are more IP addresses in this trace than can be incorporated into the IPFILE packet trace header record, a > symbol appears beside that IP address count to indicate this.

- The most common IP addresses
- A complete list of IP addresses, if you select a particular trace

### To list the traces saved by your packet trace

1. Enter **/CTRACE** at the prompt.

The CTRACE Packet Tracing Menu appears.

2. Enter **L** (List Saved Traces).

(Optional) If you want to list saved traces on a remote region, specify the name of the INMC link to that region in the Link Name field.

Press Enter.

The Saved Trace List appears.

The Saved Trace List displays a list of traces that were captured and loaded from CTRACE. The list is sorted (in reverse save-date and time chronological order) to show the most recent trace first.

## Update Packet Trace Description

The Packet Trace Description Update panel lets you update the short description of the saved trace displayed on the Saved Trace List.

It also displays the following key information from the Saved Trace List about the trace:

- Saved date and time
- User ID
- IP address count
- Packet count

### To access the Packet Trace Description Update panel

1. Enter **U** (Update) beside an entry on the Saved Trace List.

The Packet Trace Description Update panel appears.

## List Connections in a Trace

The Packet Trace Connection List displays connections (sorted into chronological order) in a selected trace.

This list has a header that displays some trace record information.

### To access the connections in a trace

1. Enter **C** (Connection List) beside an entry on the Saved Trace List or the Packet Trace IP Address List.

The connections are displayed.

## Sort Connections

The SORT command lets you display the Packet Trace Connection List in a sort order other than the default order of date and time.

The operand values for the command are associated with the column heading of the column (except the Connect Count column) that you want to sort by. For example, enter **SORT BYTES** to sort the list by the number of bytes.

## **SORT Operands**

The SORT operands are as follows:

**?**

Displays the available sort values for the list.

**TIME**

Sort by time of first occurrence of the packet trace.

**BYTES**

Sorts by the number of bytes in a packet.

**PKTCOUNT**

Sorts by the number or frequency of packets.

**FHOST**

Sorts by IP addresses of the foreign hosts.

**FPORT**

Sorts by port numbers of foreign ports.

**LHOST**

Sorts by IP addresses of the local hosts.

**LPORT**

Sorts by port numbers of local ports.

## **Locate Connections**

You can use the LOCATE command to position a particular row at the top of the list.

This command is available only when the connection list is sorted using the SORT command to change the default sort order.

The value you specify after the LOCATE command applies to the sort value that has been issued on the list. It does not necessarily apply to the first column of the list unless you have sorted by the first column.

## List Packets in a Selected Trace

The Packet List displays all packets (sorted into chronological order) in a selected trace, optionally filtered for a specific IP address or connection. This list has a header that displays some trace record information.

### To list the packets in a selected trace

1. Enter **P** (Packet List) beside the trace that you want to view on the Saved Trace List.

**Note:** If you just saved it, then it is at the top of the list.

The details of the packets that were traced are displayed.

## Errors Displayed on the Packet List

If the save processing found major errors (such as missing records or invalid packet headers) when reading packets from the CTRACE file, then the warning message for each packet in error appears as the entry for that packet on the Packet List.

The following are possible reasons for packets being in error:

- The IP version is not supported.
- The IP header length has a value less than 5.
- The IP header length exceeds the IP packet length.
- The IP header total length does not match the actual length of the datagram.

To view a Formatted Packet Display of a packet in error, enter **S** or **F** next to an error entry.

## View Data for a Selected Packet

### To view the contents of a packet from the Packet List

1. Enter **F** or **S** (Format) beside the packet that you want to view.

The Formatted Packet Display appears.

2. (Optional) Press F6 (Format) repeatedly to cycle through the formats.

The format of the displayed details changes.



## Print Formatted Packet Details

### To print formatted packet details

1. Press F4 (Print) from the Formatted Packet Display.

The PSM : Confirm Printer panel appears.

2. Complete the following fields:

#### Printer Name

Specifies the name of the printer on which to print the report.

#### Copies

Specifies the number of copies to print.

**Limits:** 255

#### Hold?

Specifies whether to hold the request on the spool or print immediately.

#### Keep?

Specifies whether to delete the request from the spool when printed.

Press F6 (Confirm).

The report is printed.

## Errors in Packets

Sometimes during the formatting of a packet trace, errors are found, such as invalid field values in packet headers. The Packet Trace facility cannot analyze these headers. It displays warning messages, in red, on the Packet List panel to inform you of these errors.

The warning messages relate to such things as:

- Incorrect lengths
- Invalid use of flags
- Invalid field values
- Reserved fields being used
- Invalid IP and TCP options
- Invalid checksums

## View Packets in Error

### To view packets in error for a trace

1. Enter **/CTTRACE.L** at a prompt.  
The Saved Trace List appears.
2. Enter **PE** (IP Packets in Error) next to the trace entry you want to view.  
The IP Packets in Error List appears.
3. Enter **S** or **D** next to an error entry.  
A Formatted Packet Display of the packet in error appears.

## Deal with Errors in Packets

If there are errors in the traced packets, do the following:

- See the appropriate RFC to determine the correct usage of fields in the protocol.
- Identify the device/program that is sending the invalid packets.
- Identify other IP devices that the packet traversed, as they may be corrupting the packet.
- Rectify the problem.

## Export a Trace

After you have saved a trace, you can export it to a physical sequential (PS) data set or an HFS file.

If you plan to export to a data set, you must allocate it first with the following requirements:

- **Organization**—PS
- **Record length**—2056 bytes minimum (for libpcap output format) or 27994 bytes minimum (for CTRACE output format)
- **Block size**—(record\_length + 4 bytes) to 32760 bytes
- **Record format**—VB

### To export a trace

1. Enter **/CTRACE** at the prompt.  
The CTRACE Packet Tracing Menu appears.
2. Enter **L** (List Saved Traces).  
(Optional) If you want to list saved traces on a remote region, specify the name of the INMC link to that region in the Link Name field.  
Press Enter.  
The Saved Trace List appears.
3. Enter **EX** (Export) beside the trace that you want to export.  
The Export CTRACE Trace panel appears.
4. Complete the fields, and then press F6 (Action).  
The trace is exported.



# Chapter 21: Using Telnet

---

This section contains the following topics:

[Use Telnet to Connect to Remote Hosts](#) (see page 245)

[Start Telnet Connections](#) (see page 246)

[Telnet Display](#) (see page 247)

[Manage Your Telnet Connection](#) (see page 249)

[Use Line Commands to Connect to a Remote Host](#) (see page 254)

[Send Control Codes or Special Characters to the Remote Host](#) (see page 258)

## Use Telnet to Connect to Remote Hosts

The Telnet protocol can be used to do the following:

- Connect to remote hosts (this could be a channel card, a router, or a UNIX system).
- Connect to network management platforms from where you can issue commands.

For example, you may want to view the status of a router's interfaces, or update its configuration.

You can establish a Telnet connection to a remote host in the following modes:

- Full screen mode
- OCS takeover mode
- Line mode

## Connect in Full Screen Mode

Full screen mode uses a full screen of the 3270 to display the Telnet connection line by line. The Telnet function supports simple line-by-line access to the remote system. It emulates a line-by-line terminal. The Telnet protocol calls this a network virtual terminal (NVT).

This support allows rapid problem diagnosis when used from other TCP/IP management displays such as the traceroute display. The Telnet function does not provide access to remote facilities that use more advanced terminal facilities, for example, full-screen editors.

## Connect in OCS Takeover Mode or Line Mode

When you start a Telnet connection in OCS takeover mode or line mode, you can issue Telnet and system commands from the same command entry point at the same time.

## Start Telnet Connections

### To start a Telnet connection to a remote host

1. Enter **/IPDIAG** at the prompt.  
The Network Diagnosis Functions menu appears.
2. Enter **TN** - Start a Telnet Connection, and complete the following fields:

#### Host Name/Address

Specifies the name or IP address of the remote host to which you want to start a Telnet connection.

#### Port Number

Specifies the port number used for the Telnet connection.

Press Enter.

The TCP/IP: Telnet panel appears.

## Other Methods of Starting Full-Screen Telnet Connections

You can start a full-screen (FS) Telnet connection as follows:

- By entering **TN** against a CIP resource on the IP Resource Monitor
- By entering **TN** against a node on the IP Node Monitor
- By applying the **TN** (Telnet) action against a host or router on the Trace Route Result List
- By applying the **TN** (Telnet) action against a router on the Routing Table
- From an OCS window by using the command:  
`TELNET host_name|IP_address MODE=FS`
- By pressing F4 (Telnet) from many panels such as channel card panels.

## Telnet Display

From the Telnet display, you can issue commands and pass data to the remote host to which the connection has been made—the IP address or host name of this connection appears in the title line.

All data resulting from any processing you do on the remote host is held in a buffer. The size of the buffer and the number of the first line displayed are shown on the right of the title line.

**Note:** Commands entered in the command line of the Telnet display are sent directly for processing on the remote host.

## Telnet Function Key Assignments

The Telnet display contains the following function key assignments exclusive to the Telnet display:

### **Function (F4)**

Presents the Telnet Functions menu from where you can select the options to manage your Telnet connection

### **Hide (F5)**

Suppresses the display of the characters being typed as you enter your password when logging on to a Telnet connection on a remote host—this also suppresses data from going into the command stack used by Retrieve (F6) as well as that resulting from tracing.

### **Retrieve (F6)**

Retrieves previously issued commands from the command stack, starting with the most recent. When the cursor is positioned on a line in the display, then that line is retrieved.

## Edit Text on the Telnet Display

If you want to reformat the data on your Telnet display before printing it, or if you want to use particular data or messages as input—for example, to a problem record—ensure that the Edit field on the Telnet display is set to ON. When Edit is set to ON, the display is presented in Edit mode. This is an ISPF-like interface and supports most of the standard ISPF editing commands.

Some simple editing commands are as follows:

### **D or DD (Delete)**

Deletes one line of text, type the **D** command in the first column to the left on the line you want to remove and press Enter. To delete more than one line, enter **DD** at the first and last lines of the block you want to remove.

### **N or NN (Notepad)**

Copies one line of text to the Notepad, type the **N** command in the first column to the left on the line you want to copy to the Notepad and press Enter. To copy more than one line, enter **NN** at the first and last lines of the block you want to copy.

**Note:** For more information about editing commands, see the *Managed Object Development Services Programmer and Developer Guide*.



## Manage Your Telnet Connection

The following functions are provided to help you manage your Telnet connection:

### **Find**

Specifies a string of text and search for it in the buffer.

### **Print**

Prints the contents of the buffer.

### **Options**

Sets up or alters your Telnet connection.

### **Telnet Commands**

Issues any of four standard Telnet commands.

### **Clear Buffer**

Clears the buffer of all existing data.

### **Keys Off/On**

Hides or shows the function key display.

### **Connection Details**

Provides statistical information about the current connection.

### **Disconnect/Reconnect**

Exits from the current connection or, if currently disconnected, lets you reconnect.

## Search Data on the Telnet Display

A search facility is provided to enable you to find occurrences of text that match a specified string.

### **To find a particular text string in the buffer**

1. Enter **1** on the Functions menu.

The Find window appears.

2. Specify the text string you want to find and press Enter.

The cursor is placed at the first character of the found text.

3. To locate further instances of the text string, continue to press Enter.

When there are no more instances of text that match the search string, a message appears informing you that the bottom of the data has been reached.

Press Enter again to return to the top of the data and continue the search.

## Print from the Telnet Display

You can print the contents of the Telnet buffer to any printer defined in the Print Services Manager (PSM).

### To print the contents of the Telnet buffer

1. Enter **2** on the Functions menu.

The Print window appears.

2. Complete the following fields:

#### Printer

Specifies the name of the printer to which you want to send the output.

**Note:** Type **?** in the Printer field and press Enter to display a list of printers.

#### Copies

Specifies the number of copies you want to produce.

#### Hold

Specifies whether to hold the output or print it immediately.

#### Keep

Specifies whether to remove the print job from the spool immediately after printing.

Press F6 (Confirm).

The output is sent to the spool and held in the queue or printed immediately.

### More information:

[Using Print Services](#) (see page 355)

## Set Your Telnet Options

You can configure your Telnet connection to suit your particular requirements.

### To change the Telnet options

1. Enter **3** on the Functions menu.

The Options window appears.

2. Complete the fields, as required, and press Enter.

**Note:** Press F1 (Help) for a description of the fields.

The changes are saved.

**Note:** If you change any of the options while your Telnet display has a status of Disconnected, an attempt is made to reconnect you with the new options. If the attempted reconnect fails (for example, you might have specified an unsupported port), an appropriate message appears and the status of the Telnet display changes to Error.

## Issue Telnet Commands

A set of four standard Telnet commands is implemented. When issued, these commands are sent to the remote host, which processes them accordingly. The following is a brief description of each of these commands:

### To issue Telnet commands

1. Enter **4** on the Functions menu.

The CAS : Valid Value List for the Telnet Commands appears.

2. Complete the following fields, as required:

#### **Abort Output**

Allows a process that is generating output to run to completion, but without sending the output to your terminal.

#### **Are You There**

Sends a request to provide visible evidence that this connection is still active; for example, this command might be used if the system has been unexpectedly *silent* for an extended period of time.

#### **Break**

Simulates a Break key or Attention key.

#### **Interrupt Process**

Suspends, interrupts, aborts, or terminates the process to which you are connected.

Press Enter.

The command is issued.

## Clear the Buffer

### To remove all of the data in the buffer

1. Enter **5** on the Functions menu.

The data is removed.

## Hide or Display the Function Key Assignments

**To hide the function key assignments that are displayed at the bottom of the Telnet panel**

1. Enter **6** on the Functions menu.

The function key assignments are hidden.

Alternatively, if the function key assignments are already hidden, this option appears in the Functions menu as Keys On and can be selected when you want them to be displayed.

## Display Telnet Connection Details

**To display information about your current Telnet session**

1. Enter **7** on the Functions menu.

The Connection Details window appears.

## End Your Telnet Connection

The most direct way to end your session on the remote host and exit is to press F3 (Exit); however, this function is useful if you want to change any of your connection's option settings, while retaining access to the Telnet display and its Functions menu after disconnecting.

**To end your session on the remote host and remain in the Telnet display**

1. Enter **8** on the Functions menu.

The session ends and the Status field now contains the value of Disconnected.

**Note:** You can re-establish the connection through the Functions menu.

## Use Line Commands to Connect to a Remote Host

A benefit of using the TELNET command to establish a connection from an OCS window or from the Command Entry panel is that you can issue both Telnet and product commands from the same command entry point at the same time.

The TELNET command can be used in the following ways:

- OCS takeover mode
- Line mode
- As part of an NCL procedure

Regardless of the way in which you use the TELNET command to establish a connection, you may need to occasionally send special characters to the remote host.

### TELNET Command: Start a Telnet Connection

Use the TELNET command to start a Telnet connection.

This command has the following format:

TELNET *ip\_address*|*host\_name*

**ip\_address**

Specifies the IP address of the host to which you want to connect.

**host\_name**

Specifies the name of the host to which you want to connect.

To start a connection with a configuration other than the default (for example, to connect to the remote host *mercury* on a port other than the default port 23), you should enter the command as follows:

TELNET *mercury* PORT=1976

**PORT**

Specifies the port number on the remote host.

## Use Telnet in OCS Takeover Mode

You can turn your OCS window into a virtual terminal for a nominated remote host by using the OCS takeover mode. In takeover mode, you retain the ability to issue product commands and receive unsolicited notifications, but you can also issue commands directly to the remote host by typing the command and pressing Enter.

To start a Telnet connection to the remote host, *mercury*, in takeover mode, use the TELNET command in the following form:

```
TELNET mercury MODE=OCS
```

**Note:** MODE=OCS is the default when you are in OCS.

When you establish a connection in OCS takeover mode, the name of the remote host to which you are connected appears to the right on the line immediately above the command entry line.

When you press the Enter key in takeover mode, the data you have entered at the command line is passed to the remote host.

When you start a Telnet connection in takeover mode it overrides the following function key assignments in your OCS window:

**F3**

Becomes Disconnect—this is used to end your current Telnet connection and reinstate normal function key assignments.

**F12**

Becomes the OCS Enter key—this is used to issue Management Services commands in the OCS environment.

**Enter**

Becomes the Telnet Enter key—this is used to issue commands to the remote host.

## Use Telnet in Line Mode

In line mode, you retain normal OCS operation and must issue a new command each time you want to communicate with the host.

For example, to start a Telnet connection to the host, *mercury*, in line mode, use the following command form:

```
TELNET mercury MODE=LINE
```

To send data to the remote host use the TNSEND command and the identifier of the connection (usually the host name). For example if the host, *mercury*, prompts you for your login ID on starting a connection, you would enter:

```
TNSEND mercury user01
```

To reduce the amount of typing required, you can set up your own equate. For example, you might want to assign the period (.) as an equate to send data to the host, *mercury*. To do this, enter the following OCS command:

```
EQ . -START $TNCALL COMMAND=TNSEND ID=mercury DATA=
```

The above equate means that to send data (for example, the login ID requested in the earlier example), you need only enter:

```
.user01
```

**Note:** The TNSEND command is itself an equate which is set up as follows:

```
EQUATE TNSEND+ -START $TNCALL COMMAND=TNSEND ID=
```



## Automate Commands Issued to Remote Hosts

You can use an NCL procedure to automate the starting of a connection and the issuing of commands to the remote host to which the connection was made.

### Example

You may want to create a procedure that logs on to Router1 and checks its interfaces. The following example shows how you can do this.

```
.  
. .  
. .  
-* Start the connection  
_*  
&INTCMD TELNET Router1 MODE=LINE  
. .  
. .  
_*  
-* Receive messages from the router  
_*  
&INTREAD SET  
. .  
. .  
_*  
-* Send the SHOW INTERFACES command to the router  
_*  
&INTCMD TSEND Router1 SHOW INTERFACES
```

You could then process the results of the SHOW INTERFACES command and reformat the display for an operator or you could send a monitor message if an error situation is detected.

**Note:** Issuing &INTCLEAR TYPE=ALL causes the connection to be terminated. Use &INTCLEAR TYPE=ANY to clear any queued messages and continue processing.

For information about using NCL procedures and product commands, see the *Network Control Language Programming Guide* and the online help.

## End a Telnet Connection in Line Mode or OCS Take-over Mode

Depending on the type of host to which you are connected, it is likely that you will be disconnected when you issue the logoff command appropriate to that host. If this is not the case, use the TNDISC command (or, in OCS takeover mode, the F3 (Disconnect)) to end the connection.

## Send Control Codes or Special Characters to the Remote Host

It is likely that you will occasionally need to send control codes such as Ctrl-C, or special characters such as [ to the remote host; for example, Ctrl-D to log off from the host.

The control character is used to do this and it is specified when you start a Telnet connection. The default control character is the cent (¢), but you can change this by using the CTRL operand of the TELNET command.

The control character has the following distinct purposes:

- To simulate the Ctrl key; for example, ¢C becomes Ctrl-C.
- To send characters that are otherwise not supported on 3270 keyboards:

| To send...  | Enter... |
|-------------|----------|
| [           | ¢{       |
| ]           | ¢}       |
| Del (X'7F') | ¢#       |
| NUL (X'00') | ¢0       |
| Esc (X'1B') | ¢2       |
| X'1C'-X'1F' | ¢3-¢6    |

### Using the ---more--- Prompt

You can send a string of text without the usual Enter character (CRLF or CR) by ending the string with ¢ and the Enter key. For example, you might want to send a single space in response to a --more-- prompt. To do this, press the space bar, type ¢ and press Enter.

**Note:** Cisco routers support the command: `TERMINAL LENGTH 0`, which prevents them from using the --more-- prompt.

# Chapter 22: Diagnosing Line Printers

---

This section contains the following topics:

[Line Printer Diagnostics Panel](#) (see page 259)

## Line Printer Diagnostics Panel

```
PROD----- TCP/IP : Line Printer (LPD) Diagnostics -----/LPD
Select Option ==>

  Q  - Query Print Queue
  D  - Delete a Job from the Print Queue
  PR - Send a Test Print to a Printer
  X  - Exit

Host Name/Addr ..                ( Required ALL )
Printer Name ....                ( Required ALL )
Job Number .....                ( Required D  )
User Name ..... USER01         ( Required D  )
Link Name .....+                ( Optional ALL )
```

The TCP/IP : Line Printer Diagnostics panel helps you to determine if there are printer problems on the network.

This panel contains the following options:

### **Q - Query Print Queue**

Displays a print queue to determine if there are problems on the network.

### **D - Delete a Job from the Print Queue**

Deletes a job from the print queue.

### **PR - Send a Test Print to the Printer**

Sends a test print to the selected printer.

This panel contains the following fields:

**Host Name/Addr**

Specifies the name or the IP address of the host that owns the target printer.

**Printer Name**

Specifies the name of the target printer.

**Job Number**

Specifies the job number of the printer queue entry to delete.

**User Name**

Specifies the name of the owner of the print queue entry to delete.

**Link Name**

Specifies the name of the INMC link to a remote system. You can invoke line print functions on a remote system by specifying the name of the INMC link to that system.

## Access Line Printer Diagnostics Panel

**To access the line printer diagnostics**

1. Enter **/LPD** at a prompt.  
The Line Printer Diagnostics panel appears.

## Query Printer Status

**To display a printer queue**

1. Enter **Q** at the prompt on the TCP/IP : Line Printer (LPD) Diagnostics Menu, complete any required fields on the panel, and press Enter.

The printer status panel appears.

**Note:** The contents of this panel depend on the remote LPD implementation. If your region receives an error return code instead of the printer status display, it automatically pings the IP address of the printer's host to determine the cause of the failure. If the ping is successful, it proves that the host can be contacted, but the printer cannot be, or that the printer daemon resident in the host is not active.

## Delete an Entry in the Print Queue

### To delete a job from the print queue

1. Enter **D** - Delete a Job at the prompt on the Print Queue from the TCP/IP : Line Printer (LPD) Diagnostics Menu, complete the details of the job you want to delete, and press Enter.

**Note:** If the print job you want to delete is not yours, change the user ID in the User Name field to that of the owner of the print job.

The print job is deleted from the print queue.

**Note:** Security considerations on the remote host could prevent users from deleting any or all entries on a print queue. For example, on Windows NT, the Security tab of the printer's Properties controls authorizations for user access to the printer and its queue. On some UNIX systems, a user name of ROOT is required to delete entries of the printer queue.

## Send a Test Print

### To send a test print to a target printer

1. Enter **PR** - Send a Test Print to a Printer at the prompt on the TCP/IP : Line Printer (LPD) Diagnostics Menu, complete any required fields on the panel, and press Enter.

The test print is printed at the specified printer.



# Chapter 23: Using MIBinsight

---

This section contains the following topics:

- [MIBinsight](#) (see page 263)
- [MIBinsight Browser](#) (see page 264)
- [SNMP Tree](#) (see page 265)
- [Add MIB Definition](#) (see page 267)
- [Delete MIB Definition](#) (see page 267)
- [Sort MIB Objects](#) (see page 268)
- [Display the Value of a Selected MIB Object](#) (see page 269)
- [Display the Values of the Next n MIB Objects](#) (see page 270)
- [Skip a Table or Group](#) (see page 270)
- [Walk the MIB](#) (see page 270)
- [Browse the Value of MIB Objects](#) (see page 270)
- [Display the Object Values of a Selected MIB Table](#) (see page 271)
- [Update the Value of MIB Objects](#) (see page 272)
- [Reformat Octet String Object Values](#) (see page 272)
- [Delete Objects from the MIBinsight Browser](#) (see page 273)
- [Add an OID](#) (see page 273)
- [Get First OID](#) (see page 273)
- [Print MIB](#) (see page 274)
- [Maintain Your User Security Details for MIBinsight](#) (see page 274)

## MIBinsight

MIBinsight is a component that lets you manage SNMP Management Information Bases (MIBs). MIBinsight comprises a MIB maintenance facility, a browser, and the ability to monitor MIB attributes.

To browse or monitor a MIB attribute of an IP resource, you normally need to specify a unique Object Identifier (OID). OIDs are a string of numbers (usually very long); they are not very user-friendly. MIBinsight translates these numbers into a more intelligible, human-readable format and lets you view the knowledge of the resource in a user-friendly way.

This chapter describes how to browse MIBs using the MIBinsight browser.

**Note:** For information about compiling, administering, and loading MIBs using the MIBinsight compiler, see the *Administration Guide*.

## MIBinsight Browser

The MIBinsight browser displays MIB details for an IP device. You can browse and update these details, depending on your level of authority.

The MIBinsight browser displays the structure of a device's MIB as a tree. The MIBinsight browser supports the maximum screen width available, which means that more of the OID values can be displayed.

Objects and their values are dynamically added to this display as you browse through a MIB.

## Access MIBinsight Browser

### To access the MIBinsight browser

1. Enter **/IPDIAG** at the prompt.

The TCP/IP : Network Diagnosis Functions menu appears.

2. Type **MB** at the prompt and complete the following fields:

#### **Host Name/Addr**

Specifies the IP address or host name of the host you want to investigate.

#### **(Optional) Object ID**

Specifies the OID that you want to display.

Press Enter.

The MIBinsight : [User Security Details](#) (see page 274) panel appears.

3. Press F3 (File).

The system saves your changes.

If you did not provide an initial OID, the MIBinsight : Loaded MIBs panel appears.

4. Enter **S** beside the MIB that you want to display.

The MIBinsight browser appears, with the selected (or default) object definitions listed.

**Note:** Select only MIBs that are relevant to the MIB that you are browsing. For example, it is futile to prime your browser with a Cisco MIB if you are browsing an IBM stack.

**Note:** You can also access the MIBinsight browser from the IP Node Monitor and the IP Resource Monitor by using the MIB command.



## SNMP Tree

The SNMP tree has two viewing modes. Whichever mode you choose is retained in your user profile and used the next time you use the MIBinsight browser.

The modes for viewing the SNMP tree are as follows:

### Flat

Displays a flat list of OIDs with only table entries, index, and attribute groupings, with contained entries indented. This is the default mode.

### Example

```

PROD1531----- MIBinsight : Browser -----Line 1 of 113
Command ==> _                               Scroll ==> PAGE

IP Address ..... 172.16.0.0
Host Name ..... ca3
GetNext Amount ... 100
S/=Browse G=Get N=GetNext U=Update E=Expand C=Collapse T=GetTable K=Skip D=Delete X=Text O=Octet B=Binary ?=List Cmds
----- MIB Layout / Object Name ----- Value
├── sysDescr
├── sysObjectID
├── sysUpTime
├── sysContact
├── sysName
├── sysLocation
├── sysServices
├── atmInterfaceConfTable
│   └── atmInterfaceConfEntry
│       ├── atmInterfaceMaxVpcs
│       ├── atmInterfaceMaxVccs
│       ├── atmInterfaceConfVpcs
│       ├── atmInterfaceConfVccs
│       ├── atmInterfaceMaxActiveVpiBits
│       ├── atmInterfaceMaxActiveVciBits
│       ├── atmInterfaceIlmiVpi
│       └── atmInterfaceIlmiVci
└──

F1=Help      F2=Split      F3=Exit      F4=Collapse      F5=Find      F6=Walk
F7=Backward  F8=Forward    F9=Swap     F11=Right      F12=ByAttr

```

### Explore

Displays a fully-indented SNMP tree structure leading to an OID.

### Example

```

PROD1531----- MIBinsight : Browser -----Line 1 of 122
Command ==> _                               Scroll ==> PAGE

IP Address ..... 172.16.0.0
Host Name ..... ca3
GetNext Amount ... 100
S/=Browse G=Get N=GetNext U=Update E=Expand C=Collapse T=GetTable K=Skip D=Delete X=Text O=Octet B=Binary ?=List Cmds
----- MIB Layout / Object Name ----- Value
├── iso
│   ├── org
│   │   ├── dod
│   │   │   ├── internet
│   │   │   │   ├── mgmt
│   │   │   │   │   ├── mib-2
│   │   │   │   │   │   ├── system
│   │   │   │   │   │   │   ├── sysDescr
│   │   │   │   │   │   │   ├── sysObjectID
│   │   │   │   │   │   │   ├── sysUpTime
│   │   │   │   │   │   │   ├── sysContact
│   │   │   │   │   │   │   ├── sysName
│   │   │   │   │   │   │   ├── sysLocation
│   │   │   │   │   │   │   ├── sysServices
│   │   │   │   │   │   │   └── atmMIB
│   │   │   │   │   │   │       └── atmMIB.1
│   │   │   │   │   │   │           └── atmInterfaceConfTable
│   │   │   │   │   │   └──
│   │   │   │   └──
│   │   └──
│   └──
└──

F1=Help      F2=Split      F3=Exit      F4=Collapse      F5=Find      F6=Walk
F7=Backward  F8=Forward    F9=Swap     F11=Right      F12=ByAttr

```

## Display SNMP Tree in Flat Mode

To display the SNMP tree in flat mode, enter the primary command **FLATTEN** at the prompt.

## Display SNMP Tree in Explore Mode

To display the SNMP tree in explore mode, enter the primary command **EXPLORE** at the prompt.

## Expand and Collapse the Tree

Objects that have subordinate objects in the MIB, and hence are expandable, are preceded by a rectangle.

To expand the tree, enter **E** beside it.

**Note:** You can enter **EE** to perform the same action recursively through all subordinate levels.

To collapse the tree, enter **C** beside it.

**Note:** You can enter **CC** to perform the same action recursively through all subordinate levels.

You can toggle between global expand and global collapse by pressing F4, or by using the EXPAND and COLLAPSE primary commands.

## Add MIB Definition

If there are specific objects that you want to browse and these objects are embedded deep inside the MIB, you can add the MIB definition containing these objects to your MIBinsight browser.

It is more efficient to add this definition and then perform a Get action on the objects, than it would be to issue multiple GetNext actions in the original MIB display.

### To add extra MIB definitions to your MIBinsight browser

1. Enter **ADDMIB** at the prompt on the MIBinsight browser.  
The MIBinsight : Loaded MIBs panel appears.
2. Type **S** next to MIBs that you want to add to your MIBinsight browser and press F3 (OK).  
The MIBinsight browser appears with the selected MIB definitions added.

## Delete MIB Definition

### To delete MIB definitions from your MIBinsight browser

1. Enter **DELMIB** at the prompt on the MIBinsight browser.  
The MIBinsight : Browsed MIBs panel appears.
2. Type **S** next to MIBs that you want to delete from your MIBinsight browser and press F3 (OK).  
The MIBinsight browser appears with the selected MIB definitions removed.

## Sort MIB Objects

Objects in a MIB table can be sorted by index or attribute.

Sorting by Index is the default in the MIBinsight browser because it can be more useful viewing all attributes for a given resource, for example, an interface table.

### Example: MIB Sorted by Index

```

PROD----- MIBinsight : Browser -----Line 1 of 214
Command ==>                               Scroll ==> PAGE

IP Address ..... 192.168.255.255
Host Name ..... myStack
GetNext Amount ... 10
      S/=Browse G=Get N=GetNext U=Update E=Expand C=Collapse ?=List Cmds
- MIB Layout / Object Name - Value
  └─ ifTable
    └─ ifEntry
      └─ 1
        ├── ifIndex          1
        ├── ifDescr          Loopback Device
        ├── ifType            propVirtual(53)
        ├── ifMtu             0
        ├── ifSpeed           0
        ├── ifPhysAddress
        ├── ifAdminStatus     up(1)
        ├── ifOperStatus      up(1)
        ├── ifLastChange      0 Days, 00:00:02 (2970 ms)
        ├── ifInOctets        2286977
        └── ifInUcastPkts     10490

F1=Help      F2=Split      F3=Exit      F4=Collapse  F5=Find      F6=Walk
F7=Backward  F8=Forward   F9=Swap      F11=Right   F12=ByAttr

```



## Display the Values of the Next $n$ MIB Objects

### To display the value of one or more objects after a selected object in a MIB

1. Enter **N** (GetNext) next to the object.

This command gets the values of the next  $n$  objects (in attribute order) after the selected object and displays them in the Value column.

The value of  $n$  is as follows:

- The value (between 1 and 100) displayed in the GetNext Amount field (the default)
- A value (between 1 and 20) included in the command (for example, the command N5 returns values for the next five objects)

## Skip a Table or Group

This facility performs an SNMP GetNext request for the next set of objects after the current table or group. This lets you browse through a MIB without populating large tables.

### To skip a table or group

1. Enter **K** (Skip) next to a table or group.

This command gets the values of objects after the selected table or group and displays them in the Value column.

## Walk the MIB

The *walk* facility performs a GetNext request against the last OID browsed and returns the next set of objects, as determined by the size specified in the GetNext Amount field.

To walk the MIB, specify the amount by which you want to walk the MIB in the GetNext Amount field on the MIBinsight browser, and then press F6 (Walk).

## Browse the Value of MIB Objects

### To browse a MIB object

1. Enter **S** next to an object on the MIBinsight browser.

The MIBinsight : Object Details panel appears.

**Note:** Ensure that you have performed a G (Get) action on the MIB object first; otherwise, the value of the MIB object is not displayed on this panel.

## View the Full Definition of a MIB Object

The Object Details panel shows the first four lines of the object's description. If the full description is longer than four lines (indicated by ...), then press F5 (Browse) to view the full definition of the object.

## View an Enumerated MIB Object

If the object that you are browsing on the Object Details panel has an enumerated value, press F6 (ViewEnum) to display the full list of possible values for the object.

## View an Indexed MIB Object

If the object that you are browsing on the Object Details panel is indexed (that is, it is a table entry), press F6 (ViewIdx) to display the indexing for the object.

# Display the Object Values of a Selected MIB Table

This option lets you populate a table without issuing consecutive N (GetNext) actions throughout the table.

### To display the object values of a selected MIB table

1. Enter **T** (GetTable) next to the selected table.

The values of the objects in the selected table are displayed in the Value column.

**Important!** Many MIB tables (for example, the ipRouteTable) contain thousands of entries. Therefore this command can take quite a long time to return data.

## Update the Value of MIB Objects

**Note:** Only MIB objects with read-write access can be updated.

### To update the value of a read-write MIB object

1. Enter **U** next to an object on the MIBinsight browser.  
The MIBinsight : Object Details panel appears in update mode.
2. Update the Value field and press F3 (File).  
The values are saved and appear as white in the list.

**Note:** If the object being updated is an enumerated value, this is the integer enumerator for the required value. To view a list of all possible enumerated values, press F6 (View Enum).

**Note:** If message IPSNPK09 appears, your user security details are incorrect. To correct this problem, press F4 (ChgSec) from the Object Details panel, update your [user security details](#) (see page 274), and then redo the object update.

## Reformat Octet String Object Values

MIB objects with octet string syntax can contain a value that could represent anything, such as a network address, a string of bit flags, or some text. The MIBinsight browser tries to determine if the octet string value is text and, if so, to display it as text. However, you can choose to override the formatting of an octet string as follows:

- To display the value as an octet (the default), in the format xx:xx:xx:xx, enter **O** beside the object.
- To display the value as binary (for example, 100111000110), enter **B** beside the object.
- To display the value as readable text, enter **X** beside the object.



## Delete Objects from the MIBinsight Browser

You can delete objects from the MIBinsight browser to simplify your browser's display and remove objects that you are no longer interested in viewing; for example, unrequired values returned by the N (GetNext) action.

**Note:** Deleting objects from your MIBinsight browser does *not* delete these objects from the MIB itself.

### To delete an object from the MIBinsight browser

1. Enter **D** next to an object on your MIBinsight browser.  
A confirmation message appears.
2. Press Enter to confirm your request.  
The selected object is deleted.

## Add an OID

You can easily add a particular OID to the MIBinsight browser without first selecting its corresponding MIB definition or walking through the MIB to get to it.

To add an OID, enter the following command at the prompt:

```
OID oid
```

***oid***

Specifies the OID that you want to add.

### Example

OID 1.3.6.1.2.1.1.3.0 adds the OID sysUpTime to the browser.

## Get First OID

The FIRST primary command lets you add the first OID in the device's MIB to the MIBinsight browser. The value is also added, so you do not need to issue a GetValue request.

To add the first OID, enter the primary command **FIRST** at the prompt.

## Print MIB

### To print the current MIBinsight browser layout

1. Enter **PRINT** at the prompt.  
The PSM : Confirm Printer panel appears.
2. Complete the print details, as required, and press F6 (Confirm).  
**Note:** For more information about the fields, press F1 (Help).  
The details are printed.

## Maintain Your User Security Details for MIBinsight

### To maintain your user security details for browsing MIBs

1. Enter **/IPDIAG** at the prompt.  
The TCP/IP : Network Diagnosis Functions menu appears.
2. Type **MS** at the prompt and enter the following fields:  
**Host Name/Addr field.**  
Specifies the name or address of the host you want to access.  
Press Enter.  
The MIBinsight : User Security Details panel appears.
3. Complete the following fields:  
**SNMP Version to Use**  
Specifies which version of SNMP to use for your MIBinsight browser.  
**Community Names**  
Specifies the value required for read privileges/change values on the MIBinsight browser. Valid only if you entered V1 or V2C in the SNMP Version to Use field.  
**SNMP V3 Security Details**  
Specifies the security details. Valid only if you entered V3 in the SNMP Version to Use field.  
Press F3 (File).  
Your security details are saved.

**Note:** To access the MIBinsight : User Security Details panel at any time, you can enter **CHGSEC** at the prompt on a MIBinsight panel.

# Chapter 24: Performance History

---

This section contains the following topics:

[Performance Data](#) (see page 275)

[Performance Displays](#) (see page 276)

[Performance Graphs](#) (see page 278)

[Baselines](#) (see page 279)

[How to Access Performance Displays](#) (see page 280)

[How to Access Performance Graphs](#) (see page 283)

[How to Access Baselines](#) (see page 286)

## Performance Data

Your region stores performance history data for resources that are being monitored. Hourly and daily summaries are stored for up to the last 70 days.

**Note:** You can view data older than 70 days in a variety of web-based reports if you implement the optional ReportCenter component.

You can view this data from the IP Resource Monitor, IP Node Monitor, and the Performance Overviews Menu.

## Performance Displays

Performance data is presented in the following performance displays:

### Overviews

Lists all resources of this type that the region is monitoring. Use this list to compare the most recent hourly summary values of key attributes, between resources of one type. The list provides a quick comparison of the activity in the last hour.

### History

Lists every attribute being monitored for this resource and sampling application. Use this list to see the most recent sample value for each attribute. These lists are linked to the IP Resource Monitor or IP Node Monitor, and can be set up to update as these monitors sample the data. From these lists, you can update the alerting conditions for an attribute.

### Baseline Values List

Displays a single attribute. Use this list to see all daily, day-of-week, and hour-of-day baseline value. You can also see the individual values that were averaged to calculate each baseline value.

### Baseline Lists

Lists every attribute being monitored for this resource. Use this list to compare, for each attribute, information including latest sample and summary times and values, baselines and percentage differences, sample rates, and alert counts.

### Sample Lists

Displays a single attribute. Use this list to see the values, minimum, maximum, equivalent rates per hour and rates per second of the 12 most-recent sample values.

### Hourly Summary Lists

Displays a single attribute. Use this list to see the hourly summaries, minimum, maximum, baselines, and baseline percentage differences for all available hours.

### Daily Summary Lists

Displays a single attribute. Use this list to see the daily total or average for all available days.

### Weekly Interval Lists

Displays a single attribute. Use this list to see the following values for all available weeks:

- Hourly summary value for the same hour of the week
- Daily summary value for the same day of the week

## Attribute List Format on History Panels

The format of an attribute list varies as follows:

### **Attribute/Qualifier**

If the column heading is Attribute/Qualifier, the records are grouped by attribute. Each attribute can be expanded to show its component qualifier records.

### **Qualifier/Attribute**

If the column heading is Qualifier/Attribute, the records are grouped by qualifier. Each qualifier can be expanded to show its component attribute records.

Some displays are expanded when initially presented to show all items (attributes or qualifiers) in each group. Some displays are collapsed, so that only ungrouped items and groups containing a single item are expanded. The expanded group line displays totals for all items in the group.

When a sampled value is in a predefined threshold, the value appears in green. Any detail sample that causes an alert appears in one of the following colors:

- Red if the value is beyond the threshold
- Yellow for the following conditions:
  - The value is between the high-alert value and the reset value for the high alert.
  - The value is between the low-alert value and the reset value for the low alert.

A value of N/A indicates that the sample could not be taken.

## Performance Graphs

The following performance graphs are available:

### Sample Values Graph

Displays a single attribute.

Use this graph to see the raw values of the 12 most recent samples. Where applicable, that is for gauge attributes, this graph also displays the baseline values.

### Sample Hourly Rates Graph

Displays a single attribute.

Use this graph to see the equivalent rates per hour of the 12 most recent sample values. Baselines are also displayed.

### Hourly Summary Graph

Displays a single attribute.

Use this graph to see the hourly summary values for the last 24 hours. Hourly summaries are aggregated from all of the samples taken during that hour. Baselines are also displayed.

## Attribute Types

The following types of attributes are available:

### Gauge

Displays a non-negative numeric value that may increase or decrease in a range. For example, processor memory usage varies between zero and the physical limit of the hardware.

### Counter

Displays the rate of increase in units per hour in a sample period. The rate is derived from sample data, which is an accumulated count that increases in value over time (for example, bytes received). This type is also referred to as COUNT.

### Enumerated

Displays the value from a defined set of discrete values. For example, the state of a device can be ACTIVE or INACTIVE. Multiple values are aggregated so that a percentage of a particular value over time is available. This type is also referred to as ENUM.

### Total

Displays the rate of increase in units per hour in a sample period. The rate is derived from sample data, which is the total increase in value in a sample period.

## Baselines

A *baseline* is a moving average value of a monitored attribute. Baseline values are unique to your environment and reflect the performance characteristics of your system.

Using the collected data, the *baselines are calculated for numeric type attributes such as counters and gauges*. You can use these baselines as references for identifying problems.

Baselines are sliding averages of hourly values. A *sliding average* means that there is a fixed size window in which to store values. When a new value is added to the window, the oldest value is deleted; therefore, your average is always calculated on the last  $n$  values, where  $n$  is the fixed window size.

All baselines are averages of hourly summary values. The hourly summary values that are averaged depend on the baseline type.

The baseline types are as follows:

### Hour of Day Baseline

Averages the hourly summary value for one specific hour of one specific day of the week. The maximum window size is 10 (for example, Friday 17:00 for the last 10 weeks).

This is the most granular baseline because you are comparing only the same specific time of the week.

There are 168 hour of day baselines, one for each hour of each day name (24 x 7).

### Day of Week Baseline

Averages the hourly summary value for all hours in a specific day. The maximum window size is 10 (for example, every Tuesday for the last 10 weeks).

Day of week is not as precise as the hour of day baseline. Every hour on every Tuesday is averaged together, not taking into account the fact that some hours, for example, working hours, frequently have different workloads than others, for example, late shift or off-peak hours.

There are seven day of week baselines, one for each day of the week.

### Daily Baseline

Averages the hourly summary value for all hours in the day for each of the past 30 days. The window size is 30.

Daily is the least precise baseline. Like day of week, it does not account for the workloads of different hours. Also, it disregards the different daily workload patterns, for example, week days are often busier than weekend days, and so on.

There is one daily baseline.

## How to Access Performance Displays

You can display performance history from the following locations:

- IP Resource Monitor
- IP Node Monitor
- Resource Management menus
- Performance Overviews Menu

### Display Performance History from the IP Resource Monitor

The IP Resource Monitor displays the status of the IP resources that are monitored at your site. From the monitor, you can display the performance history of a resource in which you are interested.

**Follow these steps:**

1. Enter **/IPMON** at the prompt.  
The IP Resource Monitor appears.
2. Enter **H** next to the resource for which you want to display performance history.  
The History panel appears.
3. Use the actions and function keys to display various performance aspects.

**Note:** For information about the actions and function keys, press F1 (Help).

**Note:** [For a STACK resource, you have available other commands for displaying performance history](#) (see page 113).



## Display Performance History from the IP Node Monitor

The IP Node Monitor displays the status of the IP nodes that are monitored at your site. From the monitor, you can display the performance history of a node in which you are interested.

**Follow these steps:**

1. Enter **/IPNODE** at the prompt.  
The IP Node Monitor appears.
2. Enter **H** next to the IP node for which you want to display performance history.  
The History panel appears.
3. Use the actions and function keys to display various performance aspects.

**Note:** For information about the actions and function keys, press F1 (Help).

## Display Performance History from Resource Management Menus

A Management menu for a resource class (for example, stack) provides options that let you display the performance history of a resource.

**Follow these steps:**

1. Enter **/DIAG** at the prompt.  
The Network Diagnosis primary menu appears.
2. Select the option for the class of the resource in which you are interested (for example, ST for stacks).  
The Management menu for that class of resources appears.
3. Identify the resource for which you want to display performance history, and select Option **H**.  
Depending on the class of resource, either the History panel (which lists the attributes) appears or there are intervening panels before the list appears.
4. Use the actions and function keys to display various performance aspects.

**Note:** For information about the actions and function keys, press F1 (Help).

## Display Performance History from the Performance Overviews Menu

The Performance Overviews Menu lets you review the performance of various IP components.

### To display performance history

1. Enter **/PERF** at the prompt.

The Performance Overviews Menu appears.

```

PROD----- Performance Overviews Menu -----C011
Command ==>                                     Scroll ==> CSR

                                     S=Show Performance Overview from C011

Business Views          Business Applications
Applications            Telnet Applications
                        Address Spaces
                        CSM
Sessions and Connections Stack IP Connections
                        Home Addresses
                        Network IP Connections
                        Stack Telnet Connections
                        Network Telnet Connections
                        Stack FTP Connections
                        FTP Users
                        Network FTP Connections
Protocols and Ports     Stack IP, TCP, and UDP
                        Ports
IP Networking            Stack IP, TCP, and UDP
                        IP Nodes
Logical Devices          Enterprise Extender          (not monitored)
                        Enterprise Extender Connections
                        APPN/HPR
                        VIPA                          (not monitored)
Devices and Links        Stack Network Interfaces
                        OSA Cards
                        Cisco Channel Cards          (not monitored)

**END**

```

- Enter **S** beside the performance overview you want to display.

The overview appears. You can sort the displayed list by a column. Press F4 (Sort) repeatedly to cycle through the columns.

The following example shows an overview of connection workload by business applications:

|  |            |            |                |          |             |
|--|------------|------------|----------------|----------|-------------|
| PROD----- TCP/IP Performance : Overview -----C011                |            |            |                |          |             |
| Command ==>  |            |            | Scroll ==> CSR |          |             |
| Performance Data ... Connection Workload, by Application         |            |            |                |          |             |
| Note ..... Latest hourly summaries, totalled for all C011 stacks |            |            |                |          |             |
| S=Show Baseline List   |            |            |                |          |             |
| Business   | Start      |            |                |          |             |
| Application  | System     | Hour       | Bytes          | Connects | Active      |
| CCISSLGW   | C011       | 18:00      | 19.0K          | 0.0      | 1.0         |
| CCITCPG2   | C011       | 16:00      | 17.9K          | 0.0      | 1.0         |
| PROD17   | C011       | 18:00      | 1.2M           | 0.0      | 8.0         |
| PRODX4JV   | C011       | pending    | -              | -        | -           |
| PROD   | C011       | 18:00      | 21.6K          | 0.0      | 1.0         |
| PROD44   | C011       | pending    | -              | -        | -           |
| FTP  | C011       | 18:00      | 1.9M           | 15.0     | -           |
| MVSNFSC  | C011       | 18:00      | 19.6K          | 1.0      | 1.0         |
| OTHER  | C011       | pending    | -              | -        | -           |
| SMTP   | C011       | 17:00      | 3.2K           | 2.0      | -           |
| PROD1  | C011       | 18:00      | 1.2M           | 10.0     | 13.0        |
| TCPIP01  | TCPIP01    | C011 18:00 | 500.3K         | 24.0     | 4.0         |
| VANQAV62   | C011       | 18:00      | 2.2M           | 44.0     | 4.0         |
| F1=Help  | F2=Split   | F3=Exit    | F4=Sort        | F5=Find  | F6=Refresh  |
| F7=Backward  | F8=Forward | F9=Swap    |                |          | F12=Related |

## Display Related Overview

From some performance overviews, you can display related overviews. For example, if you are viewing FTP workload by stack, you can switch to FTP workload by user.

To display a related overview, press F12 (Related).

## How to Access Performance Graphs

You can display performance graphs from the following locations through the attribute lists on performance history panels:

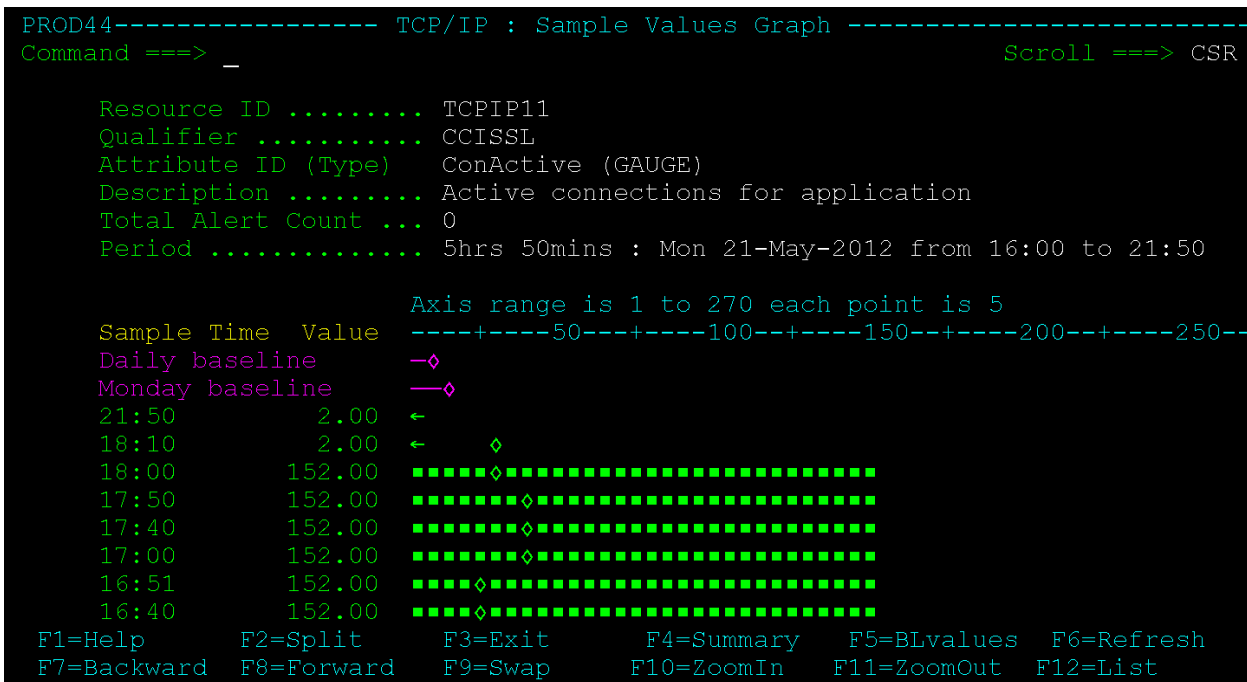
- IP Resource Monitor
- IP Node Monitor
- Resource Management menus

## Display Sample Values Graph

To display the sample values graph, enter **D** (Samples) next to an attribute of the Gauge or Enumerated type on a History panel.

### Example: Values Graph for a ConActive Attribute

This example displays the values graph for the CCISL/ConActive attribute of the TCP/IP11 stack.



### Example: Hourly Rates Graph for a ConBytes Attribute

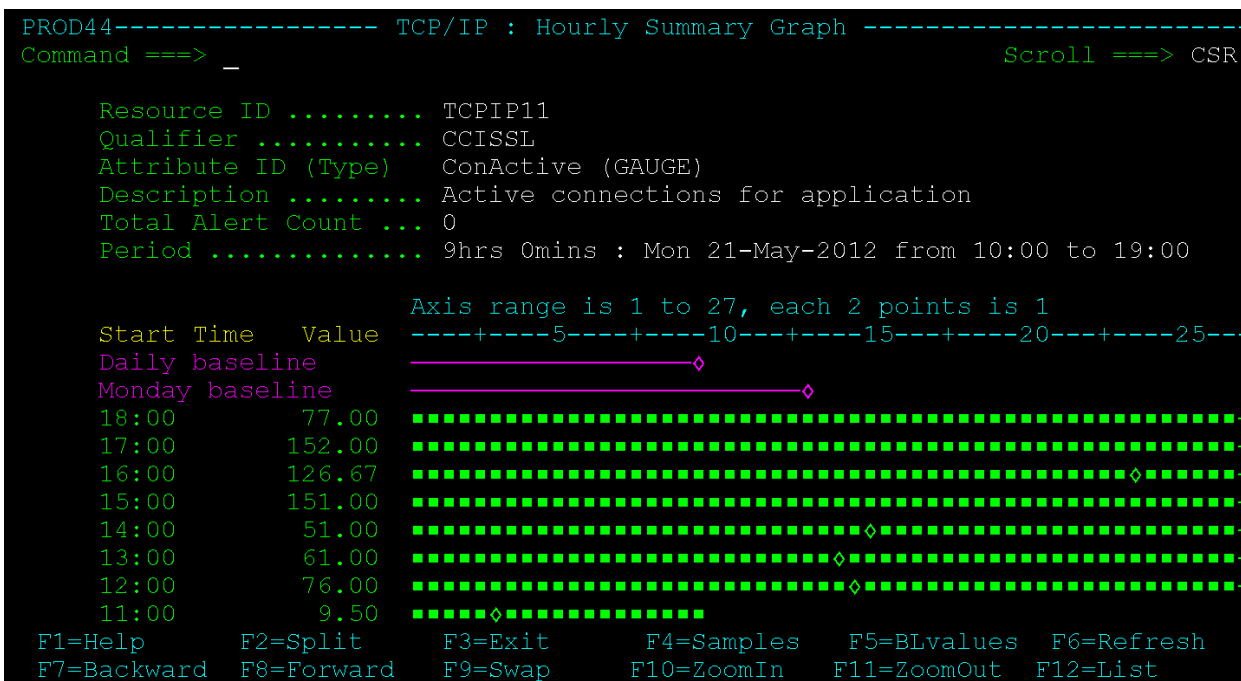
[illegible]

## Display Hourly Summary Graph

To display the hourly summary graph, enter **S** (Summary) next to an attribute on a History panel.

### Example: Hourly Summary Graph for a ConActive Attribute

This example displays the hourly summary graph for the CCISSL/ConActive attribute of the TCPIP11 stack.



## How to Access Baselines

You can display baselines from the following locations:

- IP Resource Monitor through attribute lists on performance history panels
- IP Node Monitor through attribute lists on performance history panels
- Resource Management menus through attribute lists on performance history panels
- Performance Overviews Menu through the overviews

## Display Current Baselines and Differences for Monitored Attributes

To display the current baselines for monitored attributes, enter **S** (Show Baseline List) next to a resource on the TCP/IP : Performance Overview panel. You can see how much the latest hourly summary varies from the baselines.

### Example

The following example shows the baselines for resource TCPIP3:

```

PROD----- TCP/IP Performance : Baseline List -----0001
Command ==>                                         Scroll ==> PAGE

Performance Data .... Connection Workload, by Stack
Resource ..... TCPIP3

                                S=Samples H=Hours D=Days W=Weeks B=BLvalues
                                Last Start HourOfDay HourOfDay DayOfWeek
Attribute      Summary Hour   Baseline   % Diff   Baseline
ConTotalBytes   52.9M 23:00    53.1M    -0%     90.1M
ConTotalConnects 4.0K 23:00    3.8K     +6%     3.4K
**END**

```

## Display Stored Baseline Values for an Attribute

To display stored baseline values for an attribute, enter **B** (BLvalues) beside it on the Baseline List.

You can also display the baseline values from other panels (for example, the Sample Values Graph panel).

## Display Samples List

To display the samples for a single attribute, enter **S** (Samples) next to an attribute on the Baseline List.

The format of the display varies depending on the [attribute type](#) (see page 278).

### Example

The following example shows the last 14 samples for the attribute ConTotalConnects:

```

PROD----- TCP/IP : Samples List -----
Command ==>                               Scroll ==> PAGE

Performance Data .... Connection Workload, by Stack
Resource ..... Stack TCP/IP3
Attribute ID (Type)  ConTotalConnects (total)
Description ..... Connections for stack
Period ..... Last 14 samples, since Wed 18-Jul-2012 22:17

Sample      Sample      Sample      Sample      Sample      HourOfDay  HourOfDay
Date        Time        Value Rate/Hour  Rate/Sec  Baseline   % Diff
Thu 19-Jul-2012 00:27  634.0      3.8K      1.1      2.9K      +32%
Thu 19-Jul-2012 00:17  682.0      4.1K      1.1      2.9K      +42%
Thu 19-Jul-2012 00:07  639.0      3.8K      1.1      2.9K      +33%
Wed 18-Jul-2012 23:57  665.0      4.0K      1.1      3.8K      +6%
Wed 18-Jul-2012 23:47  666.0      4.0K      1.1      3.8K      +6%
Wed 18-Jul-2012 23:37  683.0      4.1K      1.1      3.8K      +9%
Wed 18-Jul-2012 23:27  698.0      4.2K      1.2      3.8K      +11%
Wed 18-Jul-2012 23:17  633.0      3.8K      1.1      3.8K      +1%
Wed 18-Jul-2012 23:07  665.0      4.0K      1.1      3.8K      +6%
Wed 18-Jul-2012 22:57  663.0      4.0K      1.1      3.4K      +18%
Wed 18-Jul-2012 22:47  645.0      3.9K      1.1      3.4K      +14%

F1=Help      F2=Split      F3=Exit      F4=Return      F5=BLvalues  F6=Refresh
F7=Backward  F8=Forward    F9=Swap      F11=Right     F12=Hours

```



## Display Hourly Summary List

To display the hourly summary values for an attribute, enter **H** (Hours) next to an attribute on the Baseline List.

You can also display the Hourly Summary List from the Samples List by pressing F12 (Hours).

### Example

The following example shows the hourly summary values for the attribute ConTotalConnects:

```

PROD----- TCP/IP : Hourly Summary List -----
Command ==>                                     Scroll ==> PAGE

Performance Data .... Connection Workload, by Stack
Resource ..... Stack TCPIP3
Attribute ID (Type)  ConTotalConnects (total)
Description ..... Connections for stack
Period ..... Last 382 hours, since Tue 03-Jul-2012

Summary      Start    Hourly HourOfDay HourOfDay DayOfWeek DayOfWeek
Date         Hour      Total  Baseline  % Diff  Baseline  % Diff
Wed 18-Jul-2012 23:00    4.0K    3.8K    +6%     3.4K    +17%
Wed 18-Jul-2012 22:00    4.0K    3.4K    +18%     3.4K    +16%
Wed 18-Jul-2012 21:00    4.2K    3.6K    +16%     3.4K    +22%
Wed 18-Jul-2012 20:00    4.9K    3.2K    +52%     3.4K    +42%
Wed 18-Jul-2012 19:00      -     2.7K      -     3.4K      -
Wed 18-Jul-2012 18:00      -     2.6K      -     3.4K      -
Wed 18-Jul-2012 17:00      -     2.7K      -     3.4K      -
Wed 18-Jul-2012 16:00      -     2.9K      -     3.4K      -
Wed 18-Jul-2012 15:00      -     2.8K      -     3.4K      -
Wed 18-Jul-2012 14:00      -     2.7K      -     3.4K      -
Wed 18-Jul-2012 13:00      -     2.7K      -     3.4K      -
F1=Help      F2=Split    F3=Exit     F4=Return   F5=BLvalues F6=Samples
F7=Backward  F8=Forward  F9=Swap     F11=Right   F12=Days
  
```

## Display Daily Summary List

To display the daily summary values for an attribute, enter **D** (Days) next to an attribute on the Baseline List.

You can also display the Daily Summary List from the Hourly Summary List by pressing F12 (Days).

### Example

The following example shows the daily summary values for the attribute ConTotalConnects:

```

PROD----- TCP/IP : Daily Summary List -----
Command ==>                                     Scroll ==> PAGE

Performance Data .... Connection Workload, by Stack
Resource ..... Stack TCPIP3
Attribute ID (Type)  ConTotalConnects (total)
Description ..... Connections for stack
Period ..... Last 16 days, since Tue 03-Jul-2012

                                                    H=Show hours of this day

Date          Daily Total    # Hourly
                Summaries
Wed 18-Jul-2012    17.1K      4
Tue 17-Jul-2012     9.0K      3
Mon 16-Jul-2012    24.7K      8
Sun 15-Jul-2012     0.0       0
Sat 14-Jul-2012     0.0       0
Fri 13-Jul-2012    13.0K      5
Thu 12-Jul-2012    31.5K     13
Wed 11-Jul-2012    20.9K      7
Tue 10-Jul-2012    27.5K      7
Mon 09-Jul-2012    32.2K     14
F1=Help      F2=Split  F3=Exit  F4=Return  F5=Find  F6=Refresh
F7=Backward  F8=Forward  F9=Swap  F12=Weeks

```

## Display Weekly Interval List

To display the hourly and daily summary values for an attribute over a week, enter **W** (Weeks) next to an attribute on the Baseline List.

You can also display the Weekly Interval List from the Daily Summary List by pressing F12 (Weeks).

### Example

The following example shows the weekly interval list for the attribute ConTotalConnects:

```

PROD----- TCP/IP : Weekly Interval List -----
Command ==>                                     Scroll ==> PAGE

Performance Data .... Connection Workload, by Stack
Resource ..... Stack TCPIP3
Attribute ID (Type)  ConTotalConnects (total)
Description ..... Connections for stack
Period ..... Last 3 weeks

                                D=Show days of this week  H=Show hours
Week      Date and Time      Hourly Total Daily Total
This week  Wed 18-Jul-2012 23:00    4.0K    17.1K
1 week ago Wed 11-Jul-2012 23:00    2.1K    20.9K
3 weeks ago Wed 04-Jul-2012 23:00    5.1K    49.3K
**END**

F1=Help      F2=Split      F3=Exit      F4=Return      F5=Find      F6=Refresh
F7=Backward  F8=Forward      F9=Swap

```



# Chapter 25: IP Event History

---

This section contains the following topics:

[History Reports](#) (see page 293)

[View Reports](#) (see page 294)

[Search the TCP/IP Events Database](#) (see page 295)

[Extract Data to a File](#) (see page 298)

[Print Reports](#) (see page 298)

[Reporting Over Extended Periods Using the System Management Facility \(SMF\)](#) (see page 301)

[History of IP Activities](#) (see page 302)

## History Reports

CA NetMaster NM for TCP/IP records FTP, Telnet, connection, and Cisco channel card events in the event history database (IPLOG).

The TCP/IP reporting function produces online and printed reports from the database. These reports contain a list of events with details. This function also enables you to extract the data for analysis by exporting it to other data analysis and reporting tools such as Microsoft Excel.

The reporting function produces online reports by performing a search with specified criteria. It lets you do the following tasks:

- List and view predefined reports about FTP, Telnet, connection, and Cisco channel card events
- Use predefined search criteria to produce event reports
- Define your own searches to produce event reports

Performance monitoring aggregates data from individual events into event rates, such as connections per time interval and FTP transfers per time interval. The optional ReportCenter component produces web-based reports on their trends.

To enable your region to collect events, use the IPEVENT parameter group in Customizer (/PARMS). For more information, see the *Implementation Guide*.

**Note:** Depending on your site-specific implementation, the same information about Telnet, FTP, and connection activities is also available in the activity log.

## View Reports

The following predefined reports are available:

- All connections
- All FTP events
- All Telnet connections
- Failed file transfers
- Secured events

### To view reports

1. Enter **/IPHIST.B** at the prompt.

The History Report List appears.

2. Enter **S** next to the report you want to view.

The selected report appears.

From the panel, you can perform the following functions:

- Enter **B** next to an event to view more details. You can also press **F4 (Prints)** to print a copy of the details.
- Press **F4 (Extract)** to extract the report in comma-separated value (CSV) format to a data set or z/OS UNIX file.

### More information:

[Extract Data to a File](#) (see page 298)

## Search the TCP/IP Events Database

The search facility lets you use predefined search criteria or define your own search criteria (custom search) using the fields from the TCP/IP events database to obtain specific information.

### To perform a search

1. Enter **/IPHIST.B** at the prompt.  
The History Report List appears.
2. Enter **S** next to the type of search you want to perform.  
A panel for you to enter your search criteria appears.
3. Enter your search criteria, and press F6.

**Note:** Fields prefixed by a plus (+) sign provide a list of values. You can access the list by entering ? in the field. For more information about the fields, press F1 (Help).

The search results appear.

## Examples of Custom Searches

Use the following examples to help you customize your own searches of the events database.

### Custom Search: Example 1

This is an example of search criteria that produces a list of all Telnet terminal sessions that lasted for less than 10 minutes from an IP address with the 202 prefix.

```

PROD----- Network Database : Search Criteria -----
Command ==>                                         Function=Search

                                D=Delete I=Insert R=Repeat
                                Gen ")" Bool
"(" Field      Opr  Value
+ $IPRECTYPE   + =   TS
+ $IPDURATION  + <   600
+ $IPRMTADDR   + =   202
+
+
+
+

```

## Custom Search: Example 2

This is an example of search criteria that produced a list of all FTP events that failed.

|  |                |     |       |  |                 |          |          |       |  |
|--|----------------|-----|-------|--|-----------------|----------|----------|-------|--|
| PROD----- Network Database : Search Criteria ----- |                |     |       |  |                 |          |          |       |  |
| Command ==>  |                |     |       |  | Function=Search |          |          |       |  |
|  |                |     |       |  | D=Delete        | I=Insert | R=Repeat |       |  |
| "("  | Field          | Opr | Value |  |                 | Gen      | )"       | Bool  |  |
| (  | + \$IPRECTYPE  | + = | FS    |  |                 | +        |          | + OR  |  |
|  | + \$IPRECTYPE  | + = | FC    |  |                 | +        | )        | + AND |  |
|  | + \$IPLASTREPL | + = | 2     |  |                 | +        | YES      | +     |  |
|  | +              |     |       |  |                 | +        |          | +     |  |
|  | +              |     |       |  |                 | +        |          | +     |  |
|  | +              |     |       |  |                 | +        |          | +     |  |
|  | +              |     |       |  |                 | +        |          | +     |  |

## Custom Search: Example 3

This is an example of search criteria that produced a list of all file transfers for data sets with the SYS2 prefix.

|  |               |     |       |  |                 |          |          |       |  |
|--|---------------|-----|-------|--|-----------------|----------|----------|-------|--|
| PROD----- Network Database : Search Criteria ----- |               |     |       |  |                 |          |          |       |  |
| Command ==>  |               |     |       |  | Function=Search |          |          |       |  |
|  |               |     |       |  | D=Delete        | I=Insert | R=Repeat |       |  |
| "("  | Field         | Opr | Value |  |                 | Gen      | )"       | Bool  |  |
| (  | + \$IPRECTYPE | + = | FS    |  |                 | +        |          | + OR  |  |
|  | + \$IPRECTYPE | + = | FC    |  |                 | +        | )        | + AND |  |
|  | + \$IPCOMMAND | + = | RETR  |  |                 | +        |          | + AND |  |
|  | + \$IPDSNAME1 | + = | SYS2  |  |                 | +        | YES      | +     |  |
|  | +             |     |       |  |                 | +        |          | +     |  |
|  | +             |     |       |  |                 | +        |          | +     |  |



### Custom Search: Example 4

This is an example of search criteria that, performed at the time of 4:00 pm produced a list of file transfers for the last hour.

```
PROD----- Network Database : Search Criteria -----
Command ==>                                         Function=Search

          D=Delete I=Insert R=Repeat
          Gen ")" Bool
"("  Field      Opr  Value
(  + $IPRECTYPE + =   FS
  + $IPRECTYPE + =   FC
  + $IPDATE    + =   24-NOV-2006
  + $IPTIME    + >=  150000
  +
  +
  +
  +
```

## Extract Data to a File

To perform further analysis, you can extract event data to a comma-delimited file for processing by external analysis or reporting tools. You can extract the data to a data set or z/OS UNIX file.

### To extract data

1. (Optional) Define a sequential data set with the following attributes to extract the network data into this data set:  
  
RECFM: VB  
  
Record length: 502
2. Enter **/IPHIST** at the prompt.  
  
The TCP/IP : History Data panel appears.
3. Enter **EX** - Extract All TCP/IP Events to Dataset at the prompt.  
  
The Extract Events panel appears.
4. Enter the name of the data set for file to which to extract the data in the Dataset or HFS File field.  
  
The TCP/IP management region extracts all records from IPLOG in the events database (NDB) to the specified data set or file. On completion, a notification is sent using Broadcast Services.
5. Transfer the data set or file to your PC or LAN, and save it with a .CSV extension.
6. Use this .CSV file as input to your preferred PC application, and import this file as a comma-delimited format file.
7. Analyze your data by applying facilities such as graphs and charts, tables, and macros.

**Note:** From WebCenter, you can download the data in CSV or PCAP format directly to your PC.

### More information:

[View Reports](#) (see page 294)

## Print Reports

You can print reports currently defined to your TCP/IP management region using Report Writer. Alternatively, you can also use Report Writer to define your own reports.

## Print a Predefined Report

### To print a predefined report

1. Enter **/IPHIST.P** at a prompt.  
The Report Writer : Report List appears.
2. Enter **S** next to the listed report you want to print.  
The Confirm Printer panel appears.
3. Press F6.  
The report is printed.

## Check the Print Queue

After you print a report, you can access the print queue to view any reports that have not been released to the printer.

### To check the print queue, at the prompt on the Report Writer : Report List panel

1. Enter **PQ**.  
The PSM : Output Queue appears.

## Define Reports

To set up your own reports to print, you must define them to your region.

### To define printed reports by copying an existing report

1. At the prompt, enter **/RWDEFN**.  
The Report Writer : Report Definition Menu appears.
2. Enter **L** at the prompt and enter **\$IP** in the Report Appl field.  
The Report Writer : Report Definition List for the specified application appears.
3. Enter **C** next to the listed report you want to copy.  
The Report Writer : Report Description panel appears.

4. Complete the following fields:

**Report Name**

Specifies the new report name.

**Description**

Describes the report.

**Report Exit**

Specifies whether a report exit procedure is executed while the report is generated.

**Note:** To ensure that the report you are setting up is listed in the same report group as other printed reports for your region, enter **\$IPLORWX**.

**Group**

Specifies the group to which the report belongs.

**Note:** To ensure that the report you are setting up is listed in the same report group as other printed reports for your region, enter **\$IPREPORTING**.

**Criteria Name**

Specifies your own search criteria by accessing the CAS : Criteria Definition Menu. To do this, enter **/CAS.C** at the prompt. The CAS : Criteria Definition Menu appears.

Press F3 (File).

Your report is saved.

5. At the Report Writer : Report Definition List, type **LC** next to your report.

The Report Writer : Report Definition Component List appears.

6. Select **RH** - Report Header, enter your own report title, and press F3.

The Report Writer : Report Definition Component List appears.

7. Press F3 until the Report Writer : Report Definition Menu appears.

8. Select **R** - Reset Report Cache.

The new report definition is activated.

## Reporting Over Extended Periods Using the System Management Facility (SMF)

The records written to the IPLOG Events database can be written to SMF.

Records written to SMF can be analyzed by IBM and third-party products such as SLR and SAS.

The SMF can store detail data on individual events in active SMF records and offline SMF archives. Depending on your organization's requirements, this data can be kept for extended periods, and used for audit and capacity planning.

**Note:** For information about how to enable SMF logging, see the *Installation Guide*. For information about the SMF record format produced by your region, see the *Administration Guide*.

To access these records, you can customize and use your preferred SMF reporting facilities such as:

- Batch jobs created and run in TSO
- REXX procedures
- CLISTs
- SLR
- SAS

## History of IP Activities

The region sources the following activity lists from the Packet Analyzer:

- Address spaces
- Applications
- Applications by interface
- Local TCP ports
- Protocol
- Protocol by stack home address
- Protocol by stack interface
- Remote addresses
- Remote networks
- Stack home addresses
- Stack interfaces
- TCP server ports

You can access these lists from the IP History menu. Use the /IPHIST panel shortcut to access the menu, then select the TRS option. You can also use the /IPTRS panel shortcut to get there directly.

By default, the displayed list is sorted by the byte throughput for the last minute, busiest first. You can use the SORT command to resort the list.

In addition to these lists, you can download the raw [Packet Analyzer records](#) (see page 359) of these and other activities in CSV format from WebCenter. The CSV format enables you to analyze the data using a spreadsheet application. To access the download page, click History, IP Activity Lists.

# Chapter 26: Using Operator Console Services

---

This section contains the following topics:

- [Operator Console Services](#) (see page 303)
- [Access OCS](#) (see page 304)
- [OCS Panel](#) (see page 304)
- [Run Multiple OCS Panels](#) (see page 306)
- [Function Keys](#) (see page 307)
- [Assign Your Own Values to Function Keys](#) (see page 308)
- [Use Commands in OCS](#) (see page 311)
- [Monitor and Control in OCS](#) (see page 314)
- [Receive Non-roll Delete Messages](#) (see page 316)
- [Use the Activity Log to Help Monitor Your Regions](#) (see page 318)
- [Interpret Messages and Codes to Help Monitor Your Region](#) (see page 318)
- [Issue Commands](#) (see page 318)
- [Execute or Start NCL Processes from OCS](#) (see page 324)
- [Start REXX Programs from OCS](#) (see page 326)
- [Issue System Commands from Your Console](#) (see page 327)

## Operator Console Services

Operator Console Services (OCS) lets you enter commands to control and monitor your resources.

OCS uses a formatted display panel called an OCS window to provide an environment for executing commands or NCL procedures. Your command results are returned to the window, with other system information, to provide a console function.

The level of authority granted in your user ID definition limits the actions you can perform in OCS. You control the way your OCS window looks and the way you use it. This set of attributes, privileges, and options is called your *operator profile*.

Certain attributes of your operator profile are controlled by UAMS. Other attributes can be changed using the PROFILE command.

## Access OCS

### To access OCS

1. Enter **O** at the prompt at the main Primary Menu.  
The OCS window appears.

## OCS Panel

The OCS panel has two distinct activity areas: a one-line command input area at the bottom of the window, and an output message display area called the roll delete area, which occupies the remaining space above the command line.

## Command Line

The command line is the bottom line of the OCS window. The command line is the only display field where input is permitted. The cursor is automatically positioned to the right of the command line prompt when the panel is first displayed. To enter a command, position the cursor in the command line and press Enter.

## Operating Mode Indicators

A mode indicator may appear to the left of your command entry area to indicate how the OCS window is currently operating. Values of the operating mode indicators and their meanings are as follows:

### **M (Monitor)**

Terminal has monitor status and receives monitor messages.

### **P (Paused)**

An NCL procedure has paused awaiting the entry of a GO, END, or FLUSH command. The SHOW NCL command gives you further details.

### **W (Waiting)**

An NCL procedure is waiting for specific text to arrive. The SHOW NCL command gives you further details.



## Roll Delete Area

When you receive messages as the result of commands entered on the command line, they are reported in the roll delete area with any unsolicited information you are profiled to receive.

Output to the roll delete area is written line-by-line from top to bottom of the screen. When the display area is full, new output messages wrap back to the top of the screen, overwriting the oldest displayed messages first.

## Non-roll Delete Area

Any messages requiring a reply are delivered as non-roll delete messages. This means that the messages stay on your screen until you respond. These messages are displayed at the top of an OCS window above the roll delete area. The non-roll delete area is created only when a non-roll delete message is delivered to your OCS window.

## Roll-delimiter Line

Messages are written from top to bottom of the screen. The next line for use is filled by a line of underscore ( `_` ) characters. This line is called the roll-delimiter line. It separates the oldest and newest output displayed. Output below this line is the oldest display information; output above the line is the most recent.

**Note:** The underscore characters used for this line can be changed using the PROFILE DELCHAR command.

## Title Line

The top of the roll delete display area is reserved for a title that can be set or reset by using the TITLE command.

## Time Display

The top left of the title line includes the present system time in *hh.mm* format and is automatically updated each time anything is written to the OCS window.

## Run Multiple OCS Panels

You can use the [screen-splitting function](#) (see page 49) to run two OCS windows in parallel on the same screen.

You can have one screen window operating in OCS with the other part-screen or window in full-screen mode (for example, as a menu).

## Set Window IDs

When two OCS windows are running simultaneously, it helps if you can distinguish each window while executing NCL procedures.

To set a name for each OCS window, enter the OCSID command followed by a 1- to 8-character name at the command prompt on an OCS window and press Enter. The name for each window appears to the right of the line, immediately above the command line.

### Example: Set Window ID

To set a window ID of NET01, enter the following command:

```
OCSID NET01
```

After pressing Enter, NET01 appears to the right of the line immediately above the command line.

**Note:** You can set profile attributes for each OCS window, so that two OCS windows on the same terminal can have different profiles and appearances.

## Function Keys

OCS windows have full support for 24 function keys. You can set function keys for each OCS window to suit your requirements. If you are running two OCS windows, each window can have a separate set of function key definitions.

A variety of function keys are available:

- Default (system-wide) function keys
- Immediate function keys
- Conversational function keys
- Prefix function keys
- Suffix function keys
- NCL controlled function keys

The OCS function keys are set to system default values when you enter OCS.

When you redefine a function key, its defined value applies only to the function key settings for your current window, and remains in effect only while your current window is active.

When you press an immediate function key, its assigned value is immediately entered into the system, without the need for further action by you.

**Note:** To discover the assignment of each function key, use the PF LIST command.

## Conversational Function Keys

A conversational function key lets you modify its action before you release it for processing. When you press a conversational function key, its assigned value is displayed in the command line, so you can add to or modify the text. Press Enter to run the command after you modify it.

## Prefix and Suffix Function Keys

A prefix function key assigns a set value as a prefix to the line of text where the cursor is located when that function key is pressed (that is, the command line or any other line in the OCS window display area).

### Example: Prefix and Suffix Function Keys

The F6 function key is defined using the following command:

```
PF6 PREF,MSG USER1+
```

When you enter a message in the command line saying: SYSTEM DOWN AT 17.00, and press F6, the following command is generated and entered:

```
MSG USER1 SYSTEM DOWN AT 17.00
```

**Note:** The plus sign (+) leaves a blank after the text before concatenating it with the entered string.

A suffix function key acts like a prefix key, but adds its value to the end of the line of text where your cursor is positioned (that is, the command line or any other line in the OCS window display area).

## Assign Your Own Values to Function Keys

You can assign your own values to function keys so that they invoke an NCL procedure or act as the Enter key. If a function key is being used as the Enter key, you can redefine the Enter key to perform an OCS function.

## Specify Commands to Function Keys

To redefine function keys, use the PF command. You can specify the new function key value as *one* of the following:

### **Conversational**

The value of the function key appears in the command line so that it can be edited before being issued.

### **Immediate**

The function key performs an immediate function such as Enter.

### **Suffix**

The function key value is placed at the end of an entry in the command line.

### **Prefix**

The function key value is placed at the beginning of an entry in the command line.

### **Example: Assign a Conversational Function Key**

To assign the SHOW NCL command as a conversational function key to the F4 key, enter the following command:

```
PF4 CONV,SHOW NCL=
```

When you press F4 from now on, SHOW NCL= is displayed at the command prompt so that you can add to it before executing it.

### **Example: Define Multiple Commands**

You can use a semicolon as a command separator in the function key value to define multiple commands. When entering the PF command, specify two semicolons.

To define F20 to clear the screen and display users, enter the following:

```
PF20 CLEAR;;SHOW USERS
```

## Set Function Keys as Enter Keys

The PF command can set a function key to act as the Enter key. The Enter key is defined as an immediate function key with no associated value.

### Example: Define Enter Key

To define PF12 as the Enter key, enter the following:

```
PF12 IMM
```

PF12 acts as the Enter key because there is no entry after IMM. When you press F12, text is executed from the command line as if the Enter key is pressed.

## Redefine the Enter Key

You can use the ENTER command to redefine the action of the Enter key.

**Important!** You must define at least one function key to act as Enter *before* you redefine the Enter key.

### Example: Redefine Enter Key to Act as CLEAR Command

To redefine the value of the Enter key to act as the CLEAR command, type the following:

```
ENTER CLEAR
```

The Enter key no longer acts in its standard manner.

### Example: Reset Enter Key

To reset the Enter key, type the following text and then press the function key that is defined as Enter:

```
ENTER IMM
```

## Specify Function Keys Using NCL Procedures

You can also assign values to a function key from an NCL procedure. By setting the appropriate function keys in an NCL procedure and setting your initial command to execute the NCL procedure on entry to OCS, you can set the function keys for your OCS window.

## Use Commands in OCS

OCS windows can be used to enter product commands and monitor the results. Commands are entered on the command line and take effect when you press the Enter key.

You can access a list of all product commands from online help.

### To access the list of commands from any OCS window

1. Press F1 (Help).

The OCS Overview panel appears.

2. Enter **S** beside the List of Commands topic.

The commands are listed. You can select any of the commands displayed to get more information about its use and syntax.

## Command Authority Levels

All commands are assigned an authority level within the range 0 to 255, zero being the lowest and 255 the highest authority level. The operands on some commands might require a higher authority than the base command itself.

You are allocated a command authority level in your user ID definition, corresponding to the scope of system control you require. Whenever you enter a command, your user ID authority level must be equal to or higher than the authority level of the command entered, otherwise the command is rejected.

This authority level checking also applies to commands executed from NCL processes invoked under your user ID.

## Abbreviate Commands

All commands consist of a single command, which can be followed by one or more operands. Most commands can be abbreviated to the smallest number of characters consistent with their being distinguishable from any other product command. For example, the SHOW command can be abbreviated to SH.

## Concatenate Commands

Several commands can be entered simultaneously by concatenating them into the same OCS command line and separating each command with a semicolon (;). The concatenated commands are processed from left to right in the order they are entered.

### Example: Concatenate Commands

The command string `D LU10;D LU11` is treated by the system as two independent commands:

```
D LU10
D LU11
```

You can use the `CLEAR` command in this manner to clear the display area before the results of the next command are displayed. For example:

```
CLEAR;D BFRUSE
```

If you need to enter a semicolon as part of a command (that is, to use it as part of the command text), you must enter two semicolons instead of one.

To enter the command `a;b`, you must enter `a;;b`. The second semicolon is stripped from the text and the `a;b` string passed to the system as a single command. The remaining semicolon is not regarded as a command separator character.

Command separators are specified by using the `PROFILE CMDSEP` command.

## Prevent Command Concatenation

You can prevent command concatenation by using the `CMDSEP` operand of the `PROFILE` command. When `CMDSEP` is set to `NO`, semicolons are not regarded as command separators and are always treated as part of the command string.

You can assign concatenated commands to function keys because the value of the `CMDSEP` operand is overridden by the value that the operand contained when the function key was defined.

## Reuse Commands

If you enter a command regularly, you do not need to retype it every time you want to issue the command. There are facilities provided with OCS that let you reuse commands you have previously entered.



**More information:**

[Use the Command Stack](#) (see page 313)

[Retain Commands on the Command Line](#) (see page 313)

[Copy Display Lines into the Command Line](#) (see page 313)

## Use the Command Stack

Each OCS window keeps a stack of the commands most recently entered from its command line. The stack does not include immediate function key entries. The number of entries kept in this stack can be changed by using the PROFILE CMDSTACK command.

You can use the command stack to retrieve previous commands entered and redisplay them on the command line so that they can be modified for re-entry.

Commands are retrieved from the stack using the CS+ or CS- commands. The default system function key series includes settings for the CS+ and CS- commands. These are F10 and F11 respectively. We recommend that you retain these.

## Retain Commands on the Command Line

When you execute a command, the command can be retained on the command line so that you can execute it again, or edit the command before executing it again. This facility lets you increment and enter command sequences with minimal effort.

This feature can be turned on or off using the PROFILE CMDKEEP command. When turned off, the command line is cleared as soon as the Enter key is pressed and a command must be retrieved from the command stack if it is required again. When turned on, the command you enter is retained on the command line so that you can enter it again.

## Copy Display Lines into the Command Line

To copy a command (or some other message) from an OCS window display area to the command line, put the cursor on the line you want to copy, and enter CS+ or CS- (or press F10 or F11).

The command or message appears in the command line.

## Rename Commands

EQUATE commands can be included in initialization procedures to do the following:

- Override or rename standard commands
- Define a series of 1- to 8-character strings for use in place of lengthy command strings

## Monitor and Control in OCS

OCS allows you to monitor and control your regions by receiving messages and allowing you to issue commands. Events from your network are sent to your OCS window. You can issue commands to take control of any problems that might occur.

As you receive messages and output from commands, you can control, reorder, or clear output on the screen so that it can be read more easily.

### Control Message Presentation Speed

When the bottom line of the display area is filled, the system pauses before wrapping back to the top of the display area to write the next message.

Sometimes, a large number of messages might be sent to the screen within a very short period of time. This causes the display to roll messages faster than you can read them. There are two options you can use to temporarily suspend message delivery or change the way the messages display:

- The HOLD option
- The AUTOHOLD option

### Stop Message Flow Manually

To stop the flow of output to the screen at any time, press the Enter key while nothing is in the command line. This freezes the display and no further messages appear until you enter data.

While the screen is frozen, the word HOLDING appears immediately above the command line.

### Stop Message Flow Automatically

The default value for automatic hold supplied with your system automatically freezes an OCS window when a message fills the last line and there are messages queued to wrap back to the top of the screen. This is specified by the AUTOHOLD command.

When AUTOHOLD freezes your screen, the caption AUTOHOLD is displayed above the command line. No further messages appear until you input something.

The AUTOHOLD command option is part of your operator profile.

**Note:** If more unsolicited messages arrive while the screen is in HOLDING or AUTOHOLD mode, the caption above the command line changes to MSG QUED, and the terminal alarm sounds.

## Message Queue Holding Limit

Your system queues a limited number of messages for an OCS window while in the HOLDING or AUTOHOLD mode. The queue limit default before any OCS window messages are discarded is 200 messages.

The HOLDING or AUTOHOLD caption above the command line changes to 75% LIMIT, HOLD LIMIT, and then MSGS LOST, as this limit is approached, reached, and then exceeded. Each caption change also sounds the terminal alarm. These conditions vary and update while you actively monitor and release system messages in the OCS window.

You can define the queue limit for each OCS user window by using the PROFILE command.

## Contention Delay Interval

One of the characteristics of an OCS window is that your system can send messages to your window at the same time as you are entering a command. These messages are displayed differently depending on the type of terminal you are using:

### A Non-SNA Terminal

Any data you have just entered is immediately frozen and any new data entered is ignored while the message writes to the screen. You can then continue to type in your command text when message delivery has finished.

### An SNA 3270 Terminal

A contention condition arises. The terminal is seen as being in a send state (because you have started typing on the keyboard), and refuses to accept any output from your system until your input has been sent. However, rather than defer your system, the system interrupts you after a set period and forces the output of a message.

The default contention delay interval is 15 seconds. This is usually long enough to let you complete a standard command input operation.

## Unwrap Messages

To resequence or unwrap messages displayed in your OCS window, enter the **ORDER** command.

The OCS messages are redisplayed in the window in chronological order, with the oldest messages at the top of the window.

The ORDER command is assigned to F12 by default.

**Note:** This command does not affect the HOLDING or AUTOHOLD condition.

## Clear the OCS Window

After many messages have appeared in your OCS window, you may want to clear the window before any new messages arrive.

To clear your OCS window, enter the **CLEAR** or **K** command.

## Receive Non-roll Delete Messages

Most messages displayed on an OCS window are classified as roll delete messages. This means they are displayed once and eventually roll off the top of the screen as subsequent messages arrive and overwrite them.

When a non-roll delete (NRD) message is delivered to an OCS window, it remains in your OCS window until deleted. The NRD messages are in two categories:

- Those that are remembered by the system and are retained until explicitly deleted by the issuing process
- Those that are only displayed at individual OCS windows until deleted and are not remembered by the system

The non-roll delete area is separated from the roll delete area by a delimiter line. This line is usually a series of dash (-) characters. To change the character, use the PROFILE NRDELCH command.

NRD messages are managed centrally and held in a queue. Your system administrator determines the size of this queue. If there are more NRD messages than this limit, the oldest outstanding NRD message is deleted to remove copies of the message from all affected OCS windows.

However, NRD messages from &WRITE NCL statements are never deleted automatically. It is therefore only possible to exceed the NRDLIM queue depth if large numbers of &WRITE-generated NRD messages exist at the same time.

A warning message is sent to all OCS users with monitor status to notify them when the NRD message queue reaches 75 percent full.

You can hide these messages to allow other message flows to continue in your OCS window, and then reveal them again when you are able to deal with them.

## Hide NRD Messages

To remove an NRD message from the OCS display, move your cursor to the line on the screen with the NRD message you want to remove and then press Enter.

The NRD message disappears and the screen is reformatted. Removing NRD messages in this way provides more room for pending NRD messages or a larger roll delete area.

**Note:** System NRD messages are not deleted from the NRD message queue, only from your OCS window. NRD messages specific to your OCS window are deleted, and cannot be recalled.

## Restore Hidden NRD Messages

Hidden NRD messages can be restored by entering the NRDRET command. The oldest hidden NRD messages are returned to the non-roll delete area first, until the area has expanded to its maximum size.

The NRDRET command displays all hidden NRD messages that you are entitled to view, including those that occurred before you entered OCS and any that are still outstanding.

NRDRET can be issued from any environment capable of receiving NRD messages, including NCL &INTCMD environments.

## Delete NRD Messages

An NRD message is automatically deleted when *one* of the following conditions is satisfied:

- The condition to which an NRD message refers is satisfied
- An NCL process issues an &NRDDEL NCL statement to delete a specific NRD message
- The NCL process that generated the NRD is terminated

You can only delete NRD messages that are remembered by the system by using the PURGE command.

## Use NRD Messages with ROF Sessions

Messages that originate from a remote system carry the NRD message attribute and appear as NRD messages, in the same way as locally-produced messages.

When an INMC link fails and breaks any ROF sessions traveling across it, all NRD messages from that remote system are automatically deleted.

When you close a ROF session to a particular remote system by using the SIGNOFF command, any NRD messages you have received across the ROF session are deleted from your window. Other users displaying the same NRD messages are not affected.

## Use the Activity Log to Help Monitor Your Regions

The activity log records all commands, responses to commands, and messages that occur in your regions. By accessing the activity log when you are in OCS you can browse through recent activity on the system to assist you in locating information and analyzing problems.

To access the activity log browse function from OCS, enter **/LOG** at the prompt.

On initial entry to the activity log, you are positioned at the end of the log for the current day. You can use the F8 (Forward) and F7 (Backward) function keys to scroll through the log for the current day as well as for previous days.

**Note:** For more information about locating information in the activity log, press F1 (Help) from the activity log panel.

## Interpret Messages and Codes to Help Monitor Your Region

The information database provides categories of information about commonly used codes and errors. By accessing the information database from OCS, you can get information about error messages that appear in your OCS window.

To access the information database from OCS, enter **/CODES** at the prompt.

## Issue Commands

Being able to issue commands from OCS is an important part of controlling your regions. From OCS you can issue commands to the background processes of your product, and you can set commands to issue automatically, based on a specified time.

## Issue Commands in Background Environments

Background environments are internal to your system and services. They process commands submitted to them by users and support system level procedures such as LOGPROC. Each background process has a user ID, but is not associated with any physical terminal.

The following background environments are available:

### **BSYS**

Background system environment

### **BMON**

Background monitor environment

### **BSVR**

Background server environment

### **BLOG**

Background logger environment

You can send commands to these environments for them to execute, as if they were real OCS users by using the SUBMIT command. You can submit commands or NCL procedures. For example, if you want the background system environment to start the procedure MONPROC, enter the following command:

```
SUBMIT BSYS START MONPROC
```

After a command is submitted, its processing is managed by that environment. It is not affected if you log off or leave OCS, and its command authority remains the same as the user ID of the submitter.

Background environment processing is ideal for monitoring an NCL procedure that regularly checks the status of network components. Commands directed to the Background Monitor route the command and its results to all monitor status terminals logged on to the system, and to the activity log. Commands directed to the Background Logger for execution log the command and its results only.

[Timer commands](#) (see page 320) can also be routed to background environments by the SUBMIT command or by the ROUTE operand for the timer command being issued.

## Issue Commands at Specified Times

You can issue commands at specified times and at specified intervals. These commands are known as timer-initiated commands. The following timer-initiated commands are available:

### **AT**

Executes commands at a specified time of day. Timer commands use a 24-hour clock with the format *hh.mm.ss*.

**Limits:** 24.00.00 (midnight)

### **EVERY**

Repeats commands at a given time frequency.

**Default:** 10 seconds

Timer commands can be entered in OCS, or included in NCL procedures.

A maximum of 9999 concurrent timer commands is supported, and this maximum is the default.

If you log off after issuing a timer command, that command is not executed. However, you can use the ROUTE or KEEP operand when you enter an AT command to specify another user to issue the command in your place. This feature allows you to sign off and have the results of the command returned to you when you sign on again.

The ROUTE and KEEP options are ideal if you are including timer commands for specific operators in the system initialization procedures that are executed automatically during startup.

Timer commands can also be specified with a limit to the number of times they can execute before being automatically purged.



### Example: Monitor Users at a Specified Interval

To monitor the users that are logged on to the system every half hour, enter the following command:

```
EVERY .30 CMD=SHOW USERS
```

Also, if you want to remind users of a three o'clock meeting one hour before it starts, enter the following command:

```
AT 14.00 MSG ALL DON'T FORGET MEETING AT 15.00
```

When a timer command executes, the command text is echoed on all applicable terminals as if the command had been entered from those terminals. A unique timer ID prefixes the command text echo and has the following format:

```
#nnnn command_text
```

## Display Active Timer Commands

You can display pending timer commands by using the SHOW TIMER command. By default, this command lets you display any timer commands initiated by your user ID. However, by specifying the ALL operand you can display all outstanding timer commands on your system.

### Example: Display Active Timer Commands

To find out what timer commands you have initiated, enter the following command:

```
SHOW TIMER
```

Using the example given above, the following is displayed:

```
ID BY INTERVAL -USERID-R LIM CNT K/P ENV P/M TID  NEXT
 4 EV 00:30:00 USER01      0  0 NO PRI YES -   12:29:48
    CMD=SHOW USERS
 5 AT 14:00:00 USER01      0  0 NO PRI YES -   14:00:00
    CMD=MSG ALL DON'T FORGET MEETING AT 15.00
NUMBER OF TIMER COMMANDS DISPLAYED WAS 2.
```

## Delete Timer Commands Manually

When you initiate a timer command, the system allocates a unique four-digit number known as the timer ID, or purge ID. This number prefixes all displays resulting from that command, and must be used when manually deleting a timer command.

To delete a timer command manually, use the **PURGE** command.

To delete a timer command created by another user, you require a command authority level of 2 or higher.

### Example: Delete Command

To delete an AT timer command, enter the following command:

```
PURGE TIMER=5
```

The value 5 is the purge ID assigned to the AT command.

## Delete Timer Commands Automatically

By default, your timer commands remain active only while you are logged onto the system. Before each attempt to execute the command, the system checks that you are still logged on.

If you are no longer logged on to your system, the timer command is automatically deleted, without further execution.

## Redirect Timer Commands

If you want your timer-initiated commands to continue to execute after you log off, you can redirect the command results to the background logger, background monitor, or the system background environment.

To redirect the timer command, specify an AT or EVERY command with the KEEP operand.

By default, the KEEP operand requires a command authority level of 2 or higher.

### Example: Redirect Timer Commands

To redirect the SHOW USERS command for execution by the background system environment, enter the following command:

```
EVERY .30 KEEP=SYS CMD=SHOW USERS
```

If the KEEP operand is in use, the execution of timer commands continues irrespective of whether you are logged on to the region.

## Limit Timer Command Executions

When defining a timer command, you can use the LIMIT operand to specify a limit on the number of times the command is executed. When this limit is reached, the command is automatically purged.

The limit you assign and the number of times a command has already executed are displayed by the SHOW TIMER command.

### Example: Limit Timer Command Execution

To limit the number of times the SHOW USERS command is executed to 5, enter the following command:

```
EVERY .30 LIMIT=5 CMD=SHOW USERS
```

When the SHOW USERS command has been executed five times, the timer command is deleted.

### Execute a Timer Command Under Another User ID

The ROUTE operand lets you direct a command for execution under another user ID—the target user ID. The operand requires a command authority level of at least 2.

With this option, the timer command is retained even if the target user ID is not logged on. Command execution is bypassed and the time interval reset. The command is attempted again only after the time interval has again elapsed.

### Example: Execute Timer Command Under Another User ID

If you want USER02 to execute the SHOW USERS command, enter the following command:

```
EVERY .30 ROUTE=USER02 CMD=SHOW USERS
```

### Specify Concatenated Commands in Timer Commands

Concatenated commands can be specified in the command text for a timer command. Separate each command in the concatenation with a colon (:). These are internally translated into normal concatenation characters, that is, semicolons (;), before execution.

## Network Commands

The OCS provides various commands for retrieving information about your network.

### Example: Display Information About a VTAM Resource Using the D Command

You can use the D command to display information about a VTAM resource, for example:

```
D major_node_name
```

### Example: Display Connections in TCP/IP Resources Using the NETSTAT Command

You can use the NETSTAT command to display the connections in IBM TCP/IP or CA TCPAccess CS resources.

**Note:** For information about the NETSTAT (IBM) command, type NETSTAT on the OCS panel (option O on the primary menu) and press F1 (Help). For information about the NETSTAT (CA TCPAccess CS) command, see the *System Management Guide* for CA TCPAccess CS.

**Note:** You can also display the NETSTAT commands in a list and issue a command from the list. The panel shortcut to the list is /STACK.NS.

### Example: Look Up a Name or Address Using the NSLOOKUP Command

You can use the NSLOOKUP command to look up the name or address of a host, for example:

```
NSLOOKUP ip_address
```

## Execute or Start NCL Processes from OCS

There is an NCL processing environment for each window of your terminal that allows commands and NCL processes to execute on behalf of that window.

When you use an EXEC or START command to invoke an NCL process, the NCL process executes in the NCL processing environment for the OCS window.

**Note:** If you enter the EXEC or START command incorrectly, the system attempts to execute the command as if it were an NCL process.

Any NCL process can have a dependent processing environment that lets it issue commands or execute other NCL processes independently using the &INTCMD statement. NCL procedures can also use ROF sessions to collect information from other systems.

## Execute NCL Processes Serially

An OCS window can execute a serial stream of NCL processes so that they are invoked one after the other. Serial execution is suitable for processes with a short duration.

To execute NCL processes serially, use the **EXEC** command.

Processes invoked by the EXEC command can issue the &PAUSE statement to wait for further input from the OCS window. The GO, END, FLUSH, and INTQ commands, together with the process's unique identifier, let you communicate with the process.

### Example: Execute Processes in Sequence

To execute PROC1 and PROC2 in sequence, enter the following commands:

```
EXEC PROC1  
EXEC PROC2
```

Your OCS window places the two processes in an EXEC queue, which are executed on a first-come, first-served basis. Process PROC1 is scheduled for immediate execution and process PROC2 is queued to execute after PROC1 ends.

## Execute NCL Processes Concurrently

An OCS window can execute NCL processes in parallel at the same time.

To execute NCL processes concurrently, use the **START** command. If you enter the name of an NCL procedure by itself, the START command is implied.

Any started procedure can issue an &PAUSE statement to wait for further input from GO, END, and FLUSH commands from the OCS window. These commands, together with the unique identifier for the process, let you communicate with the process explicitly.

### Example: Execute NCL Processes Concurrently

To execute PROC1 and PROC2 at the same time, enter the following commands:

```
START PROC1  
START PROC2
```

## NCL Identifiers

Each NCL process is allocated a unique identifier that links it to the issuing OCS window. This ensures any &WRITE or &PANEL statements issued by the NCL process (or any other processes it starts or executes), are returned to that window only. If the window is terminated, any queued process is deleted.

## Execute an NCL Process from a Serial or Concurrent Process

An NCL process executed from an OCS window (or any process it invokes) can itself issue EXEC or START commands.

If an EXEC command is used to execute an NCL process, the process issuing the command is suspended when the new process starts executing. Only when the new process ends does the issuing process resume processing.

Invoking a process from another process in this way is called nesting. Nesting is an easy way to structure a series of processes.

**Note:** The &CALL PROC NCL statement is the recommended method for nesting procedure calls.

If a START command is used to execute an NCL process, the new process starts executing immediately. The new process runs concurrently with the invoking process and independently of it. Each process is unaffected by the termination of the other process.

## Advantages of Started Procedures

Using the START command to invoke NCL processes has the following advantages:

- You can perform relatively complex, long-term tasks from your OCS window. This does not prevent other operations from performing concurrently.
- You can perform periodic checking of the network status without operator involvement.
- You can operate a large number of independent, slave procedures on behalf of one OCS window. This lets you monitor many different aspects of the same operation, and various procedures need only communicate with you if errors are detected.

## Start REXX Programs from OCS

Your region supports the REXX language. A processing environment for each OCS window lets REXX processes execute on behalf of that window.

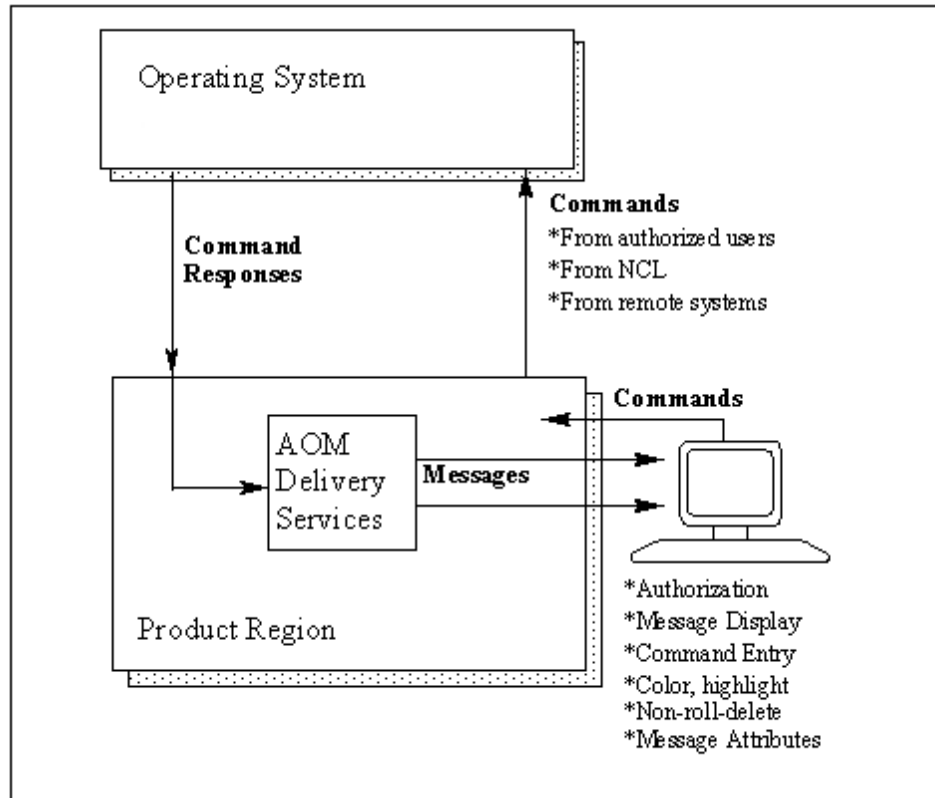
To start a REXX program from OCS, enter the following command:

REXX *program\_name*

**Note:** For information about how your product supports REXX, see the *NetMaster REXX Guide*.

## Issue System Commands from Your Console

The SYSCMD facility gives you the ability to issue operating system commands and receive responses without having to use a *real* operating system console; for example, to display the channel path or unit status of a local non-SNA terminal.



### Use the SYSCMD Facility

The SYSCMD command has several operands that you can use to enter master console commands, lock a console, or issue a command as if it came from a specific console.

In its most basic form, the SYSCMD command is:

`SYSCMD command-text`

***command-text***

The command to be entered.

**Note:** You are restricted in your use of the SYSCMD facility by both your command authority and your user security profile. These are set by your systems administrator.

## Enter Master Console Commands

If the command to be entered is usually restricted to the master console, the CON=MASTER operand must be used with the SYSCMD command.

### Example

```
SYSCMD CON=MASTER DATA=VARY CPU(0) OFFLINE
```

You must have MASTER authority for this.

**Note:** This is not necessary if you are using Extended Multiple Console Support (EXTMCS) consoles.

## Lock a Console

To ensure that you can issue commands when you need to, you can lock a console to a specific environment using the following operand:

```
OPT=LOCK
```

When you no longer require the console, you should release it, using the following operand, so that it is made available to other SYSCMD users:

```
OPT=REL
```

## Simulate Command Issue from a Specific Console

If you want to simulate issuing a command from a specific console that you are not using, enter the following form of the SYSCMD command (where *n* is the console number):

```
SYSCMD CON=n DATA=command-text
```

This can be done from anywhere in the system.

As no console authority checks are made by the SYSCMD facility, the existing authority for the specified console is used.

**Note:** The form of the SYSCMD command described in the example above is not supported if you are using EXTMCS consoles.



# Chapter 27: Using Logs

---

You can access various logs to assist in solving problems.

This section contains the following topics:

[Log Types](#) (see page 329)

[Display a Transient Log](#) (see page 329)

[Display the Activity Log](#) (see page 333)

## Log Types

Typically, a region keeps two types of logs: transient logs and activity logs.

Each resource has its own transient log. The transient log provides a real-time view of the activity associated with a particular resource. Transient logs are not kept between region restarts. However, depending on the log details defined for a resource, the transient log information may be written to the permanent activity log.

The activity log provides a historical view of the system activities associated with all resources monitored by the region. A region can have more than one activity log, of which only one is open for logging. The activity log is stored on DASD, so that you can access the activity log if necessary. You can also [access the activity log from the transient log](#) (see page 329).

The information that is logged is determined by the log parameters specified in the resource definition. The region logs the information to the transient log, as well as to any other destinations specified in the definition.

## Display a Transient Log

The transient log provides a real-time view of the activity associated with a particular resource. You can display the transient log from your monitor. This log and the activity log contain messages and other information associated with a resource. The logs help you diagnose problems (for example, resource failure).

### To display the transient log

1. Enter **L** beside a resource on the monitor.

The Transient Log Browse panel appears for the selected resource. The panel displays messages in chronological order.

2. (Optional) Enter **L** beside a message in the transient log to access the activity log to see what was happening in the system at that time.

## Set Criteria to Display Logged Messages Selectively

When you access the transient log of a resource, you are profiled to view all messages logged for that resource. You can limit the number of messages you see in the current session by profiling for certain criteria.

### To set profile values

1. Enter the **PROFILE** command at the prompt.  
A panel appears displaying the current profile setting.
2. Change the settings, as required.

**Note:** For information about the settings, see the online help.

You can also supply the profile values directly by using the command operands. The syntax of the PROFILE command is:

```
PROFILE [[SEV={1|2|3|4|5|6}]  
        [NCLID=ncl-process-identifier]  
        [PROC=ncl-procedure-name]] |  
        [RESET=YES]
```

You can profile messages according to the following:

### SEV

Determines how critical the messages are. For example, specify **SEV=1** to see only the most critical messages or **SEV=4** to see the messages of severity levels 1 through 4.

### NCLID

Specifies the ID of the NCL process that issued the messages you want to see. The NCL processes are created when NCL procedures are executed. The region creates NCL processes when performing automation tasks.

Each NCL process has a unique ID, so you can use the NCLID operand to differentiate between executing copies of the same NCL procedure if, for example, the same NCL procedure was run more than once in a given period.

The region processes resources asynchronously, and a number of NCL processes for the resource may be active at the same time. Messages raised by these NCL processes intermingle in the transient log. You can use the NCLID operand to view the messages raised by a particular NCL process (that is, to view the messages for a particular task).

**PROC**

Specifies the name of the executing NCL procedure that issued the messages you want to see.

You can use the asterisk (\*) wildcard character to include more than one NCL procedure. The wild card represents any single character except at the end of a string when the wild card represents one or more characters.

**RESET**

Specify **RESET=YES** to reset the profile to view all available messages.

## Display User-defined Log Messages

A user-defined log message can be specified for a resource on the Define Event Related Actions panel when the resource is defined.

If you want to see only these messages in the transient logs, enter **UL** beside the resource.

## Obtain Help on a Logged Message

You can obtain more information about product messages in a transient log through help.

**To display the detailed help text associated with a message in the transient log**

1. Enter **H** beside the message.

The help text appears.

## Print a Transient Log

### To print a transient log

1. Enter **P** beside a resource to print its transient log.

The Generate a Report panel appears, which lets you print a default report or an extended report of the resource's transient log.

2. Specify your printing requirements.

- To print the default report (TRANSIENTLOG), ensure that the displayed information is satisfactory.
- The extended report contains additional fields that display the S (severity), Nclid (NCL ID), and Proc (procedure) for each item in the transient log. To print the extended report, enter ? in the Report Name field, and then select TRANSX.

Press F6 (Action).

The log report is printed.

## Reset a Transient Log

When you do not need the messages in the transient log anymore, you can clear the messages by resetting the log.

### To reset the transient log of a resource

1. Enter **LR** beside the resource.

Its transient log is cleared of all messages.

## Display the Activity Log

Your region logs all significant activity and events to the activity log. Connection activity such as the starting and stopping of Telnet connections and FTP activity can be logged to the activity log as well as, or instead of, to the events database. The activity log also records operator commands issued and the output of executed obeyfiles.

**Note:** You can collect messages issued by CA TCPaccess CS and display each message in the activity log.

To access the activity log, do *one* of the following:

- Enter **/LOG** or **\$LOG** at the prompt on a panel to display the activity log for the local region.
- Enter **\$LOG linkname** at the prompt on a panel to display the activity log for the specified linked region.
- Press F7 in OCS.
- Use the L (Activity Log) option on the Historical Data primary menu.
- Enter **L** (Display Activity Log) next to an entry on any connection list.

## Browse the Activity Log Online

The following aids are available to help you use the activity log:

- Forward and backward scroll
- Various display formats
- Highlighting log records
- Log filter to restrict the records displayed
- Positioning by date or time, either absolute or relative
- Positioning by labels set in the log
- Searching forward or backward for text
- Selective printing of log records

**Note:** For detailed information about these aids, see the online help.

## Record Additional Information in the Activity Log

You can use the LOG command to record additional information in the log that is outside the scope of that recorded by default. For example, enter the following at the prompt:

```
LOG PRODUCTION LINK TO LOS ANGELES DOWN FOR MAINTENANCE
```

This produces the following entry in the log for the time the command was issued:

```
LOG ENTRY : PRODUCTION LINK TO LOS ANGELES DOWN FOR MAINTENANCE
```

You can record a message up to 256 characters long.

## Telnet Activity in the Log

Telnet connections can be logged as they are started and ended.

**Note:** Logging of Telnet activity is specified in the IPEVENT parameter group. For more information, see the *Implementation Guide*.

### Example

Examples of Telnet connection start and end messages are:

```
IPCM2002 TELNET CONNECTION STARTED FROM 192.168.2.66..4925 AS TSTCP007 TO TEST1  
LOGICAL DEVICE 0006
```

```
IPCM2003 TELNET CONNECTION ENDED FROM 192.168.6.127 AS TSTCP006 TO TEST4, BYTES IN  
550 OUT 32665 DURATION 0 DAYS 00.06.35
```

From the log, you can obtain the following information:

- The time that the connection started, plus the port number, LU, and device number used
- The time that the connection ended, the IP address and LU name of the device where the connection ended, the application to which the session was connected, the number of bytes in and out, and the duration of the connection

## FTP Activity in the Log

From the log, you can obtain information about the following FTP activities associated with FTP server and client processing:

### File Transfers

Provides information including user's IP address, the data set name and size, and how long the file transfer took.

### Deletion and Renaming of Files

Provides the name of the file being deleted or renamed, and the new name for a file being renamed.

### Failures

Provides a record of failed logons and failed transfers.

**Note:** Logging of FTP activity is specified in the IPEVENT parameter group. For more information, see the *Implementation Guide*.

### Example

Examples of FTP messages are:

```
IPFM2103 FTP RETR BY USER01 AT 192.168.9.57 DSN AUDE0.TEST01.BIGFILE 1872317 BYTES  
IN 43.56 SECONDS 42982 BYTES/SEC SERVER FTPTEST1
```

```
IPFM2102 FTP LOGON FAILED FOR USR02 AT 192.168.7.23 SERVER FTPTEST1
```





# Chapter 28: Using Monitors

---

Various monitors let you keep track of defined resources. General usage of these monitors is described here.

This section contains the following topics:

[Resource Monitors](#) (see page 337)

[Graphical Monitor](#) (see page 338)

[Monitor Display](#) (see page 341)

[Organize the Information on the Monitor](#) (see page 342)

[Change to a Different Monitor Filter](#) (see page 343)

[Change Your Default Monitor Profile](#) (see page 344)

[Use Commands in the Status and Graphical Monitors](#) (see page 344)

[Acknowledge a Link Failure](#) (see page 347)

[Respond to the Initialization Status Panel](#) (see page 347)

[Respond to the Database Synchronization Panel](#) (see page 348)

## Resource Monitors

The IP Resource Monitor, IP Node Monitor, and Graphical Monitor enable you to monitor at the resource level in your environment.

The monitors enable you to monitor the resource activities from two different viewpoints. Use the IP Resource Monitor and IP Node Monitor to view the status of *individual* resources, and the Graphical Monitor to view the status of *groups* of resources.

In a multisystem environment, you can monitor the resources on multiple systems from any of the connected focal point regions. From subordinate regions, you can monitor locally-managed resources only. You can use logs to display the messages associated with a resource and therefore with system activity. Authorized users can define filters and profiles that enable the viewing of information about specific resources.

## Graphical Monitor

The graphical monitor displays groups of resources as graphical images called *icons*. This monitor uses display attributes to alert you to changes in the status of the represented groups. Changes in an icon are caused by changes in the members in the group. Thus, if an icon changes color, you can look at its members to see what is causing the change.

The display attributes of an icon reflect the status of the represented member that is in the worst state. The attributes are controlled by the display attribute tables, except that icons do not use the highlighting attribute, as all icons appear in reverse video. The display attributes can be customized by a user with the appropriate authority.

**Note:** For information about the default display attributes and how to change them, see the *Administration Guide*.

An icon is associated with a group of resources, or a panel, as follows:

### Group of Resources

A group, when represented by an icon, enables items managed by the region to be presented with a service-driven operations perspective.

When you issue the Z (Zoom) command against an icon associated with a group, the members in the group are listed. You can then monitor the individual resources.

When you issue an operations command against an icon associated with a group, the command acts on all the members.

**Important!** Issuing commands that return responses against a group with many resources results in many panels that you have to scroll through.

### Panel

When you issue the Z (Zoom) command against an icon associated with a panel, a panel of component icons is displayed. For example, an icon may represent all the resources in the system EASTTEST. When you select the icon, a panel of icons is displayed. The component icons may contain specific types of resources. Each of these icons may be associated with another panel or with a group of resources. You can follow a very specific path leading directly to any resource that is causing the problem.

You cannot issue operations commands against an icon associated with a panel.

## Access the Graphical Monitor


### To access the graphical monitor

1. Enter **/GMON** at the prompt.  
The Graphical Monitor appears.

## Interpret the Graphical Monitor Display

Icons on the graphical monitor group resources together. Icons can group different types of resources, and can group resources from different systems.

Typically, each icon is identified by a name. You can enter commands in the command entry window. The following shows an icon and the information it contains.

| RESOURCES   | Icon Name                |
|---|--------------------------|
| Tot:22  |                          |
| Ok:9  |                          |
|  | Command Entry Window     |
| All   |                          |
| TAPE  |                          |
| 9999  | User-defined Information |

An icon may display other information (for example, the resource states).

## Operations From the Graphical Monitor

From the graphical monitor, you can do the following:

- Use the Z (Zoom) command to view the status of the resources attached to an icon
- Issue commands to solicit information about, or to modify the behavior of, all the resources attached to an icon

## Use the Z (Zoom) Command

Use the graphical monitor to get a high level view of the monitored resources. If an icon indicates a failure, issue the **Z** command from the icon command entry window to access the icon components and find the problem.

### Zooming to the Status Monitor

If the icon is associated directly with a list of resources, the Monitor panel is displayed. This panel contains only those resources defined to the selected icon.

Use the Monitor panel to check the status of resources to see which resources are causing the problem. You can then perform status monitor actions, access the logs, or issue line commands to locate the source of the problem.

### Zooming to an Icon Panel

If the icon is associated with a panel, the panel is displayed. This panel contains icons that are subsets of the main icon. For example, the icon containing all resources in EASTTEST may change to red, indicating a problem. You can zoom to the next panel of icons to see which icon has caused the main icon to change color. Select any icons that have changed state to see which resources are causing the problem. When you display the monitor, the status of the individual resources appears.

## Use Other Commands

You can enter line commands in the command entry field of an icon that directly represents a group of resources (that is, an icon that is *not* pointing to another icon panel). To list commonly used commands, enter **?**; to list all available commands, enter **??**.

A command acts on all the members of the group.

When you use a command on a group, a Confirm Command panel may appear (depending on a setting in the DISPLAYS region parameter group).

The panel advises you of the number of members in the group. You can:

- Press F6 (Action) to confirm the command.
- Press F5 (Zoom) to list the members if you decide that you do not want to issue the command against all the members. The list enables you to issue the command against individual members.
- Press F12 (Cancel) if you change your mind and do not want to issue the command.

## Change to a Different Default Icon Panel

When you access the graphical monitor, the type of information available is determined by your default icon panel.

### To change the panel

1. Enter **PROFILE** at the prompt.  
A Profile panel appears. This panel contains a field that enables you to change your default icon panel for the monitor.
2. To select a new default, enter **?** in the Panel Name field.  
A list of available panels appears.
3. Select the required panel by entering **S** beside the panel name.
4. Do one of the following:
  - Press F3 (File) to save the new default and return to the graphical monitor.
  - Press F4 (Save) to save the new default and remain on the panel.
  - If you change your mind and do *not* want to change the default, press F12 (Cancel) to return to the graphical monitor without saving the changes.

**Note:** If you want to view a different icon panel temporarily, use the F5 (Panel) function key or the PANEL command.

## Monitor Display

Depending on the monitor, the default display format includes some of the following information:

- The name of the system image that contains the resource
- The name of the resource and its class  
**Note:** Resources of the INTNL class with names in the form xx(\*) are dynamic resources that provide communications between regions.
- The status of the resource
- The alert statistics
- The ping statistics
- The override flag that indicates whether normal operation is overridden  
**Note:** For information about override flags, see the online help.

You are notified of changes in the status of monitored items that are not in view.

## Organize the Information on the Monitor

You can enter the following commands at the prompt to organize the information on the monitor.

### **FORMAT** {*?*|*format-name*}

Use this command to change the way information is displayed for a particular columns setting. If you do not know the name of a format, enter **FORMAT** and select it from the displayed list of format definitions.

#### **Notes:**

- Your product supplies a number of predefined formats. If authorized, you can define your own formats from the List Definition List panel. To access the list, enter **/ASADMIN.L** at the prompt. For information about how to define monitor formats, see the *Reference Guide*.
- If you updated the current format, you need to enter the REFORMAT command to make the updates effective in the current session.

### **SORT** *operand*

Use this command to sort the resources displayed on your screen in a particular order.

To list the column fields that can be sorted, enter **SORT**.

**Note:** Resources that rank the same by *operand* are further sorted by the object IDs.

## Change to a Different Monitor Filter

Authorized users can create filters to define which resources are displayed. Filters are sets of rules stored in the knowledge base that enable you to display a subset of the monitored resources.

The resources you see the first time you access the monitor depends on the filter specified in your user profile. If no filter is specified, you see all of the resources for the selected monitor.

You can change your view of displayed resources by using a temporary filter. The filter that you select remains valid for the current monitor session only.

### To select a filter and change the view of displayed resources

1. Enter *one* of the following commands at the command prompt of the monitor:

#### **FILTER**

Enter this command to display a list of the available filters. Enter the number that identifies the filter you want to use. Only the resources that match the filter are displayed.

#### **FILTER *filter-name***

Enter the name of the filter that you want to use. Only the resources that match the filter are displayed.

#### **FILTER NONE**

This command removes any filtering. You now see every resource for the systems to which you are connected.

The resources, as specified in the filter, appear.

#### **Notes:**

- If authorized, you can enter **F** on the Automation Services Administration Menu to select the Status Monitor Filters option to create and maintain monitor filters. You can also use the **/ASADMIN.F** path to select the Status Monitor Filters option.
- If you updated the current filter, you need to enter the **REFILTER** command to make the updates effective in the current session.

## Change Your Default Monitor Profile

When you access the monitor, the type of information available is determined by your default monitor profile. The profile specifies the following:

- Filter to use when you first enter the IP Resource Monitor and IP Node Monitor
- Number of monitored entities to display across the screen and the corresponding display format, if applicable
- Criteria that determine how the monitored entities are sorted for display

### To change the defaults

1. Enter **PROFILE** at the prompt.

A Profile panel appears.

This panel contains fields that enable you to change your default profile for this type of monitor.

2. To select a new default, enter **?** in the appropriate field.

A list of available values appears.

3. Select a value, and press Enter.

4. Do *one* of the following:

- Press F3 (File) to save the new defaults and return to the monitor.
- Press F4 (Save) to save the new defaults and remain on the panel.
- If you do *not* want to change the defaults, press F12 (Cancel) to return to the monitor without saving the changes.

## Use Commands in the Status and Graphical Monitors

You can issue commands to perform various actions from the monitors, depending on your authority level.

Use the **?** command to find a short list of commands (ShortLst) available for the selected resource. For descriptions of the commands, press F1 (Help).

Use the **??** command to find a full list of commands (FullList) available for the selected resource. For descriptions of the commands, press F1 (Help).

**Note:** While displaying a list of commands, you can press F4 to toggle between the full list and the short list.



## Find Out More About Monitored Resources

Use the **S** command to display summary information about the selected resources.

## Reply to a WTOR Message

When the status indicates that there are outstanding write-to-operator with reply (WTOR) messages waiting to be replied to, enter **W** beside the resource. A Command Entry panel appears listing the WTOR messages.

### To reply to a WTOR message

1. Issue the following command at the SYSCMD prompt:

```
REPLY wtor-id,reply-text
```

## Override Monitoring Mode

You can override the default setting for monitoring through the IP Resource Monitor and IP Node Monitor.

### To override monitoring

1. Do *one* of the following:
  - Enter **/IPMON** at the prompt.
  - Enter **/IPNODE** at the promptThe selected monitor appears.
2. Enter **UMA** beside the resource for which you want to override monitoring. The Monitoring Activity panel appears.
3. Complete the following field:

#### Monitoring Activity

Specifies whether an override is in place for monitoring. Valid values are:

**Active** - Monitoring active.

**Inactive** - Monitoring inactive.

**None** - Resets the monitoring activity override.

Press F4 (Save).

The override is set. The Ovr column on the monitor displays M.

**Note:** You can also use the AM, IM, and RM commands to control monitoring.

## Override Alerting Mode

You can override the default setting for alerting through the IP Resource Monitor and IP Node Monitor.

### To override monitoring

1. Do *one* of the following:
  - Enter **/IPMON** at the prompt.
  - Enter **/IPNODE** at the promptThe selected monitor appears.
2. Enter **UMA** beside the resource for which you want to override alerting.  
The Monitoring Activity panel appears.
3. Complete the following field:

#### Alerting Status

Specifies whether an override is in place for alerting. Valid values are:

**No** - Alerting inactive.

**Yes** - Alerting active.

**None** - Resets the alerting status override.

Press F4 (Save).

The override is set. The Ovr column on the monitor displays A.

**Note:** You can also use the AA, IA, and RA commands to control alerting.

## Acknowledge a Link Failure

When a link between connected regions fails, the resources being monitored through the failed link appear in the UNKNOWN state. A failed link can affect a large number of resources and fill your monitor with link failure error states. Use the **ACKLNKFAIL** command to acknowledge that you note the failure and to clear your monitor of the affected resources so that you can better monitor the other resources. The affected resources reappear when the link recovers.

### To acknowledge a link failure

1. On your Monitor panel, type **ACKLNKFAIL** at the prompt and press Enter.

The Execute ACKLNKFAIL Command panel appears.

The panel displays the list of regions connected to your region. The panel identifies the access method control block (ACB) name of each region and the system image that is active in that region.

2. Type **S** beside the regions affected by the failed link, and press Enter.

A confirmation panel appears.

3. Enter **CONFIRM** in the Response field to execute the command.

The Monitor panel appears with the resources under the control of the selected regions removed from the list of monitored resources.

## Respond to the Initialization Status Panel

If the loading of a system image starts in your region while you are using the monitor, your monitor session ends and the Initialization Status panel is displayed. Similarly, if you attempt to access the monitor while the system image is being loaded, the Initialization Status panel is displayed. You can take *one* of the following actions:

- Press F6 (Action) to monitor the loading process.
- Press Enter to refresh the information in the status window.
- Press F3 (Exit) to exit the panel.

You can return to the monitor when the loading process completes.

## Respond to the Database Synchronization Panel

If knowledge base synchronization is started for your region while you are using the monitor, your monitor session ends and the Database Synchronization panel is displayed. Similarly, if you attempt to access the monitor while the knowledge base is being synchronized, the Database Synchronization panel is displayed. You can take *one* of the following actions:

- Press F6 (Action) to monitor the synchronization process.
- Press Enter to refresh the information in the status window.
- Press F3 (Exit) to exit the panel.

You can return to the monitor when the synchronization process completes.

# Chapter 29: Using WebCenter

---

This section contains the following topics:

[WebCenter Features](#) (see page 349)

[Set Up Your Web Browser](#) (see page 350)

[Log On to WebCenter](#) (see page 353)

[CA SYSVIEW Integration](#) (see page 354)

## WebCenter Features

WebCenter is a web browser interface that lets you access some or all of the following functions:

- Diagnostics
- Monitoring
- Performance
- History
- ReportCenter
- CA SYSVIEW
- Utilities

If your region has WebCenter enabled, the URL is displayed on the primary menu.

WebCenter is z/OS-hosted. The WebCenter web server runs in the region address space and requires no third-party components.

Problem resolution time is decreased and ease-of-use is increased. Users who are not familiar with accessing mainframe products using a 3270 interface can diagnose problems with their standard web browser.

Each WebCenter page has a Help link in the upper-right corner that you can click for context-sensitive online help.

## Set Up Your Web Browser

You can access WebCenter by using Internet Explorer or Firefox.

The WebCenter interface requires the Java Runtime Environment (JRE).

If your organization prevents you from downloading software through the Internet, arrange to have the JRE installed. The JRE is available from <http://www.java.com>.

The JRE is required to be downloaded once only, not once per WebCenter release.

**Note:** For software requirements on your PC to support WebCenter, see the *Installation Guide*.

## Set Up Internet Explorer

If your PC does not have JRE installed, a download dialog prompt appears when you enter web pages containing Java applets.

For IPv6 support, WebCenter requires at least JRE Version 1.5.0\_12. If your site has implemented IPv6 and you do not have the required version of JRE, you receive an error dialog instead. The dialog tells you to download Version 1.5.0\_12 or later directly from the website.

**Important!** WebCenter does not work with JRE Version 1.6.0\_13 through Version 1.6.0\_20.

If your organization permits you to download software from the Internet, you can download and install the Java runtime library. However, this download requires your security settings to permit you to access the website for a once only ActiveX control download.

You can configure the settings through Internet Options from the Tools menu of your browser. On the Security tab, for the web content zone associated with access to the website (usually the Internet), click Custom Level. On the Security Setting dialog that appears, the Download signed ActiveX controls option must not be disabled.

For you to access WebCenter correctly, specify the correct options in Internet Explorer.

### To set up Internet Explorer

1. Click Tools, Internet Options.

The Internet Options dialog appears.

2. Click the Security tab.
3. Click the web content zone to which your WebCenter belongs, and then click Custom Level.

The Security Settings dialog appears.

4. Enable the following options:

**ActiveX controls and plug-ins**

Initialize and script ActiveX controls not marked as safe

Run ActiveX controls and plug-ins

**Microsoft VM**

Java permissions: High safety

**Scripting**

Scripting of Java applets

5. Disable the following option:

**Miscellaneous**

Use Pop-up Blocker

Click OK

6. Click the Privacy Tab, and then click the Sites button.

The Per Site Privacy Actions dialog appears.

7. Complete the following field:

**Address Of Web Site**

Enter the WebCenter URL.

Click Allow, and then click OK.

8. Click the Advanced Tab.

9. Enable the following option:

**Multimedia**

Show pictures

If you do not require Sun JRE as your default virtual machine, clear the following option:

**Java (Sun)**

Use Java 2 *version\_number* for <applet>

Click OK.

The options are saved.

## Set Up Firefox

If your PC does not have JRE installed, the following alert appears when you access WebCenter:

Java is not enabled in this browser. The Web Interface requires a Java-enabled browser.

Go to the website to download and install the JRE.

For IPv6 support, WebCenter requires JRE Version 1.5.0\_12. If your site has implemented IPv6, download Version 1.5.0\_12 or later.

**Important!** WebCenter does not work with JRE Version 1.6.0\_13 through Version 1.6.0\_20.

For you to access WebCenter correctly, enable the correct options in Firefox.

### To set up Firefox

1. Click Tools, Options.

The Options dialog appears.

2. Click Content, and review the following options:

#### **Block pop-up windows**

Clear the check box, or click Exceptions to add the WebCenter URL to the allowed sites.

#### **Load images automatically**

Select the check box.

#### **Enable JavaScript**

Select the check box; click Advanced, and select all the check boxes.

#### **Enable Java**

Select the check box.

3. Click Privacy, and review the following option:

#### **Cookies**

Accept third-party cookies

4. Click OK.

The options are saved.



# Log On to WebCenter

A standard user ID and password are used to access WebCenter.

## To log on to WebCenter:

1. Start your web browser and enter the access URL for WebCenter in the Address text box.

The WebCenter login page appears.

### Notes:

- The access URL is defined when your product is installed. You can find the value on the primary menu of the mainframe region.

**Note:** For more information, see the *Installation Guide*.

- To access WebCenter easily and quickly in the future, create a bookmark for WebCenter web access URL in your web browser.

2. Enter your User ID and Password, and click the Log In button.

The initial WebCenter page appears, showing a menu on the left pane.

**Note:** If your Security Administrator has installed a digital certificate, a dialog appears. Click OK to accept the certificate and continue.

The screenshot displays the NetMaster WebCenter interface. At the top, the title bar reads "NetMaster® - COMP1". The top navigation bar includes links for "Home", "Log Out", "Full Window", and "Help". Below this, a welcome message says "Welcome: John Doe".

The left sidebar contains a "WebCenter Menu" with expand/collapse options. The menu items include:
 

- Diagnostics
  - IP Diagnostics
    - IP Summary (selected)
    - IP Nodes
    - SNA Nodes
    - Telnet Connection
    - IP Connections
    - IP Stacks
    - VIPAs
    - CSM
    - Cisco Channel Card
    - OSA Cards
    - Enterprise Extended
    - Address Spaces
    - Line Printers (LPD)
    - SmartTrace
- File Transfer Diagnostics
- Monitoring
- Performance
- History
- SYSVIEW
- Utilities
- User Functions

The main content area is titled "IP Summary". It features a "System Name" dropdown set to "CO11" and a "Go" button. The date and time are displayed as "On Date: 19-DEC-2007" and "At Time: 18:10".

The "System Summary for CA11" table shows the following data:

|                             | Packets/Second | Bytes/Second | Connections |
|-----------------------------|----------------|--------------|-------------|
| Stack                       | 59.69          | 13.7K        | 179         |
| Most Active Application     | 3.310          | 3.880        | 2%          |
| Most Active TCP Server Port | 2.747          | 3.257        | 1%          |
| Most Active Home Address    | 27.93          | 31.68        | 99%         |
| Most Active Remote Network  | 13.44          | 11.33        | 25%         |

Below the summary table, there are sections for "TCP/IP11 Protocol Usage" and "Alert Summary".

The "TCP/IP11 Protocol Usage" table shows:

| Protocol | Usage |
|----------|-------|
| TCP      | 70%   |
| UDP      | 24%   |
| ICMP     | 6%    |
| OSPF     | 0%    |
| Other    | 0%    |

The "Alert Summary" section shows a bar chart with four alerts: "2 Sev1" (red), "4 Sev2" (orange), "1 Sev3" (purple), and "2 Sev4" (blue). A "Monitor" button is located to the left of the chart.

At the bottom of the main content area, there is a list of expandable sections:
 

- IP Throughput
- Application Summary
- TCP Server Port Summary
- Home Address Summary
- Remote Network Summary
- Protocol Details

The footer of the interface includes the copyright notice "Copyright © 2007 CA. All rights reserved." and a link to "About".

## CA SYSVIEW Integration

When the CA SYSVIEW interface is enabled (through the WEBCENTER parameter group), it appears in the WebCenter interface, providing a persistent command interface to CA SYSVIEW.

Any command entered into the Command Text field can be executed, or more specifically, passed to CA SYSVIEW to be executed. CA SYSVIEW in turn passes results back in the form of output that is restricted to the Maximum Lines Returned specified in the Execute a SYSVIEW Command Criteria field.

To improve performance and to cut down on network traffic, the CA SYSVIEW interface restricts the maximum number of lines returned to WebCenter for each command to 2000 lines.

For security reasons, CA SYSVIEW limits execution of certain commands to administrators or users with superuser authority. Because of the nature of the web interface to CA SYSVIEW, it is not possible to identify who is issuing the commands.

This is particularly apparent in the UNIX System Services displays, therefore:

- The output of certain commands such as UDIRTREE or UPROCESS, which rely on a particular user's profile, will vary a little.
- The output of other commands, such as USUPER, which toggles the current user authority to superuser mode, will not work at all.

One additional limitation in the CA SYSVIEW interface is that line commands, or commands that are entered against a particular line of CA SYSVIEW output, are not implemented in WebCenter. However, in many cases, there is a direct CA SYSVIEW command that will produce the desired output. Use the MENU command to navigate through the CA SYSVIEW menus and the HELP command to request help for specific CA SYSVIEW commands.

# Chapter 30: Using Print Services

---

This section contains the following topics:

[Print Services Manager](#) (see page 355)

[Access PSM](#) (see page 355)

[List Entries in the Print Queue](#) (see page 356)

[Confirm Printing](#) (see page 357)

## Print Services Manager

Print Services Manager (PSM) lets you control the physical printing of the reports your organization generates on JES or network printers. Output can be viewed online before or after printing and can be redirected to another destination.

PSM provides the following facilities:

### Print Spooling

Writes output to a print spool providing more control over output. This facility lets you redirect output to another printer if one is not available.

### Centralized Printer Definition Facilities

Supports VTAM (LU1) and JES (SYSOUT) devices and lets you assign printer aliases. This facility also allows the output destination to be a printer exit.

### Print Request Control

Lets you hold, release, browse and delete print requests, redirect print requests to another printer, change priorities and numbers of copies, and display the status of requests.

### Notes:

- For information about defining and maintaining printers, see the *Administration Guide*.
- References to JES also apply to VOS3's JES3 and JES4 subsystems.

## Access PSM

### To access PSM

1. Enter **/PSM** at the prompt.

The PSM : Primary Menu appears.

## List Entries in the Print Queue

You can list all of the entries that are queued to print, and on which printer they are to print.

### To display the entries in the print queue

1. Enter **Q** at the prompt on the PSM : Primary Menu.

The PSM : Output Queue appears.

**Note:** You can limit the display to the print queue for a specific printer by specifying a printer in the Printer field on the PSM : Primary Menu before entering the Q option.

## Display the Output of a Print Request

You can preview the output to see exactly how the print request looks when printed.

**Note:** Only data lines, not heading lines, are displayed.

To browse the output of a print request, enter **B**, **/**, or **S** next to the required print request on the Output Queue panel.

The details appear.

### Example: Browse Output

```

PROD----- PSM : Browse Output -----REQ# 0265
Command ==>                               Scroll ==> PAGE

S A B U Data
  --+---10--+---20--+---30--+---40--+---50--+---60--+---70
N N =====
1 N  COMMAND ENTRY CAPTURE PRINT
1 N =====
2 N  USERID : USER01             NAME : USER NUMBER 1      LO
2 N  DATE   : MON 26-APR-2010
2 N  TIME   : 11.16.39
2 N =====
2 N  pr
1 N  N10601 USERID: USER01 TERMINAL-ID: TERM02
1 N  N10602 NCL PROCEDURE LIBRARY ID: COMMANDS
1 N  N13450 PANEL SERVICES PATH NAME: PANELS
1 N  N10603 AUTHORITY LEVEL IS 82
1 N  N13451 NO EDS PROFILES ACTIVE IN ENVIRONMENT.
1 N  N13433 USER SERVICES PROCEDURE: $USERSER
1 N  N10624 NO NPF COMMAND RESTRICTIONS.
1 N  N10627 PPO MESSAGE DELIVERY DETAILS:
1 N  N10628 ..NO NPF MESSAGE RESTRICTIONS.
F1=Help   F2=Split   F3=Exit   F4=Return   F5=Find   F6=Refresh
F7=Backward F8=Forward F9=Swap   F11=Right

```

## Modify a Printer Entry

You can modify a print request to change where and how it is to be printed.

### To modify a print request

1. Enter **M** next to the required print request in the PSM: Output Queue.

The PSM : Print Request panel appears.

The PSM : Print Request Panel provides all details about the print request. You can alter some of the fields on the panel.

## Confirm Printing

When you send a print request to a printer, the PSM : Confirm Printer panel appears. This panel is used to confirm the printer name, the number of copies, and the hold and keep settings that you require for your print request. The fields displayed on the panel are set to the values you used last.

To change any of these fields, overwrite them with the required information, and press F6 (Confirm).

The new information is used to print your request.

**Note:** For more information about the fields displayed on this panel, press F1 (Help).

## Select the Printer

If you do not know what printers are available to send your print request to, you can display a list of active printers.

### To select the printer

1. Enter a question mark (?) in the Printer Name field on the PSM: Print Request panel.

The list of active printers appears.

**Note:** If the list is longer than a full page, use F8 (Forward) and F7 (Backward) to scroll through the list.

2. Enter the selection code at the prompt.

The printer is selected.



# Appendix A: Packet Analyzer Records

---

The following descriptions help you interpret the raw Packet Analyzer records that you download from the History, IP Activity Lists page of WebCenter.

**Note:** Several of the record types contain arrays of data that is time-related. These arrays are typically grouped with partial field names of `‘.STATS.ONEMINXn.’` or `‘.STATS.FIVEMINXn.’`. X0 means the current 1- or 5-minute interval (‘current’ means the time that the record was produced). X1 means the previous 1- or 5-minute interval, and so on.

## **ACTIVE**

I/F ACTIVE INDICATOR

## **ACTIVETIME**

CONNECTION ACTIVE TIME

## **ACTUALSENDERATE**

ACTUAL SEND RATE

## **ADFKEY**

CREATING ADF KEY

## **ALLOWEDSENDERATE**

ALLOWED SEND RATE

## **APPNAME**

GENERATED APPLICATION NAME (For a list of the names, enter the **/IPAPPLS** panel shortcut to display the Application Name Definition List panel.)

## **ARBMODE**

ARB PACING MODE

## **COLLECTSTATS**

COLLECT STATISTICS?

## **CONNECT**

CONNECTION ACTIVE INDICATOR

## **CONNID**

CONNECTION ID FOR NETSTAT (HEX)

## **CONNMODE**

UDP CONNECTION MODE (CLIENT/SERVER/PEER/UNKNOWN)

**CONNNAME**

CONNECTION NAME FROM UDP PORT ASSIGNMENTS

**CONNTYPE**

CONNECTION TYPE

**COS**

RTP Class Of Service

**CURR1MINOFFSET**

CURRENT 1MINUTE OFFSET (100THS, 0 TO 5999)

**CURR5MINOFFSET**

CURRENT 5MINUTE OFFSET (100THS, 0 TO 29999)

**CURROWNERNAME**

CURRENT PORT OWNER TASK NAME

**DATABYTESRCVD**

RTP DATA BYTES RECEIVED

**DATABYTESENT**

RTP DATA BYTES SENT

**DC**

YES IF CONNECTION CAME FROM SYSPLEX DISTRIBUTOR

**DEVTYPE**

I/F DEVICE TYPE

**DISTCONNCURR**

CURR NUM OF DISTTO CONNECTIONS

**DISTCONNMAX**

MAX NUM OF DISTTO CONNECTIONS

**DISTCONNTOTAL**

TOTAL NUM OF DISTTO CONNECTIONS

**DISTFROMADDR**

IF DISTTO, IP@ OF DISTRIBUTOR

**DVIPA**

DVIPA INTERFACE INDICATOR

**DYNAMIC**

DYNAMICALLY INSERTED I/F INDICATOR



**EECONNINFO.LCLIPADDR**

LOCAL IP ADDRESS

**EECONNINFO.RMTIPADDR**

REMOTE IP ADDRESS

**EECONNINFO.STACKNAME**

STACK NAME

**EEREL**

YES IF EE-RELATED CONNECTION

**EESTATSFIELDS.S01BI**

BYTES IN TOTAL PKTS/BYTES

**EESTATSFIELDS.S01BO**

BYTES OUT TOTAL PKTS/BYTES

**EESTATSFIELDS.S01PI**

PKTS IN TOTAL PKTS/BYTES

**EESTATSFIELDS.S01PO**

PKTS OUT TOTAL PKTS/BYTES

**EESTATSFIELDS.S02BI**

BYTES IN IP HDR

**EESTATSFIELDS.S02BO**

BYTES OUT IP HDR

**EESTATSFIELDS.S02PI**

PKTS IN IP HDR

**EESTATSFIELDS.S02PO**

PKTS OUT IP HDR

**EESTATSFIELDS.S03BI**

BYTES IN UDP HDR

**EESTATSFIELDS.S03BO**

BYTES OUT UDP HDR

**EESTATSFIELDS.S03PI**

PKTS IN UDP HDR

**EESTATSFIELDS.S03PO**

PKTS OUT UDP HDR

**EESTATSFIELDS.S04BI**

BYTES IN LLC HDR

**EESTATSFIELDS.S04BO**

BYTES OUT LLC HDR

**EESTATSFIELDS.S04PI**

PKTS IN LLC HDR

**EESTATSFIELDS.S04PO**

PKTS OUT LLC HDR

**EESTATSFIELDS.S05BI**

BYTES IN LLC XID QRY/XCH

**EESTATSFIELDS.S05BO**

BYTES OUT LLC XID QRY/XCH

**EESTATSFIELDS.S05PI**

PKTS IN LLC XID QRY/XCH

**EESTATSFIELDS.S05PO**

PKTS OUT LLC XID QRY/XCH

**EESTATSFIELDS.S06BI**

BYTES IN LLC HEARTBEAT

**EESTATSFIELDS.S06BO**

BYTES OUT LLC HEARTBEAT

**EESTATSFIELDS.S06PI**

PKTS IN LLC HEARTBEAT

**EESTATSFIELDS.S06PO**

PKTS OUT LLC HEARTBEAT

**EESTATSFIELDS.S07BI**

BYTES IN LLC DISC

**EESTATSFIELDS.S07BO**

BYTES OUT LLC DISC

**EESTATSFIELDS.S07PI**

PKTS IN LLC DISC

**EESTATSFIELDS.S07PO**

PKTS OUT LLC DISC

**EESTATSFIELDS.S08BI**

BYTES IN FUNCTION ROUTING

**EESTATSFIELDS.S08BO**

BYTES OUT FUNCTION ROUTING

**EESTATSFIELDS.S08PI**

PKTS IN FUNCTION ROUTING

**EESTATSFIELDS.S08PO**

PKTS OUT FUNCTION ROUTING

**EESTATSFIELDS.S08BI**

BYTES IN FUNCTION ROUTING

**EESTATSFIELDS.S08BO**

BYTES OUT FUNCTION ROUTING

**EESTATSFIELDS.S08PI**

PKTS IN FUNCTION ROUTING

**EESTATSFIELDS.S08PO**

PKTS OUT FUNCTION ROUTING

**EESTATSFIELDS.S010BI**

BYTES IN NHDR WITH SLOWDOWN 1 OR 2 SET

**EESTATSFIELDS.S010BO**

BYTES OUT NHDR WITH SLOWDOWN 1 OR 2 SET

**EESTATSFIELDS.S010PI**

PKTS IN NHDR WITH SLOWDOWN 1 OR 2 SET

**EESTATSFIELDS.S010PO**

PKTS OUT NHDR WITH SLOWDOWN 1 OR 2 SET

**EESTATSFIELDS.S011BI**

BYTES IN THDR

**EESTATSFIELDS.S011BO**

BYTES OUT THDR

**EESTATSFIELDS.S011PI**

PKTS IN THDR

**EESTATSFIELDS.S011PO**

PKTS OUT THDR

**EESTATSFIELDS.S012BI**

BYTES IN THDR ONLY (HPRCTL)

**EESTATSFIELDS.S012BO**

BYTES OUT THDR ONLY (HPRCTL)

**EESTATSFIELDS.S012PI**

PKTS IN THDR ONLY (HPRCTL)

**EESTATSFIELDS.S012PO**

PKTS OUT THDR ONLY (HPRCTL)

**EESTATSFIELDS.S013BI**

BYTES IN THDR WITH GAP INDICATOR SET

**EESTATSFIELDS.S013BO**

BYTES OUT THDR WITH GAP INDICATOR SET

**EESTATSFIELDS.S013PI**

PKTS IN THDR WITH GAP INDICATOR SET

**EESTATSFIELDS.S013PO**

PKTS OUT THDR WITH GAP INDICATOR SET

**EESTATSFIELDS.S014BI**

BYTES IN THDR WITH IDLE INDICATOR SET

**EESTATSFIELDS.S014BO**

BYTES OUT THDR WITH IDLE INDICATOR SET

**EESTATSFIELDS.S014PI**

PKTS IN THDR WITH IDLE INDICATOR SET

**EESTATSFIELDS.S014PO**

PKTS OUT THDR WITH IDLE INDICATOR SET

**EESTATSFIELDS.S015BI**

BYTES IN RTP SEGMENT (THDR NOT SOM+EOM)

**EESTATSFIELDS.S015BO**

BYTES OUT RTP SEGMENT (THDR NOT SOM+EOM)

**EESTATSFIELDS.S015PI**

PKTS IN RTP SEGMENT (THDR NOT SOM+EOM)

**EESTATSFIELDS.S015PO**

PKTS OUT RTP SEGMENT (THDR NOT SOM+EOM)

**EESTATSFIELDS.S016BI**

BYTES IN THDR + RU ONLY

**EESTATSFIELDS.S016BO**

BYTES OUT THDR + RU ONLY

**EESTATSFIELDS.S016PI**

PKTS IN THDR + RU ONLY

**EESTATSFIELDS.S016PO**

PKTS OUT THDR + RU ONLY

**EESTATSFIELDS.S017BI**

BYTES IN SLOWDOWN 1 (NHDR OR THDR)

**EESTATSFIELDS.S017BO**

BYTES OUT SLOWDOWN 1 (NHDR OR THDR)

**EESTATSFIELDS.S017PI**

PKTS IN SLOWDOWN 1 (NHDR OR THDR)

**EESTATSFIELDS.S017PO**

PKTS OUT SLOWDOWN 1 (NHDR OR THDR)

**EESTATSFIELDS.S018BI**

BYTES IN SLOWDOWN 2 (NHDR OR THDR)

**EESTATSFIELDS.S018BO**

BYTES OUT SLOWDOWN 2 (NHDR OR THDR)

**EESTATSFIELDS.S018PI**

PKTS IN SLOWDOWN 2 (NHDR OR THDR)

**EESTATSFIELDS.S018PO**

PKTS OUT SLOWDOWN 2 (NHDR OR THDR)

**EESTATSFIELDS.S019BI**

BYTES IN ARB CRITICAL (CRITICAL, THDR)

**EESTATSFIELDS.S019BO**

BYTES OUT ARB CRITICAL (CRITICAL, THDR)

**EESTATSFIELDS.S019PI**

PKTS IN ARB CRITICAL (CRITICAL, THDR)

**EESTATSFIELDS.S019PO**

PKTS OUT ARB CRITICAL (CRITICAL, THDR)

**EESTATSFIELDS.S020BI**

BYTES IN TH (ALL)

**EESTATSFIELDS.S020BO**

BYTES OUT TH (ALL)

**EESTATSFIELDS.S020PI**

PKTS IN TH (ALL)

**EESTATSFIELDS.S020PO**

PKTS OUT TH (ALL)

**EESTATSFIELDS.S021BI**

BYTES IN TH (NOT OIC)

**EESTATSFIELDS.S021BO**

BYTES OUT TH (NOT OIC)

**EESTATSFIELDS.S021PI**

PKTS IN TH (NOT OIC)

**EESTATSFIELDS.S021PO**

PKTS OUT TH (NOT OIC)

**EESTATSFIELDS.S022BI**

BYTES IN RH

**EESTATSFIELDS.S022BO**

BYTES OUT RH

**EESTATSFIELDS.S022PI**

PKTS IN RH

**EESTATSFIELDS.S022PO**

PKTS OUT RH

**EESTATSFIELDS.S023BI**

BYTES IN RU (INCL RTP/SNA SEG RU ONLY)

**EESTATSFIELDS.S023BO**

BYTES OUT RU (INCL RTP/SNA SEG RU ONLY)

**EESTATSFIELDS.S023PI**

PKTS IN RU (INCL RTP/SNA SEG RU ONLY)

**EESTATSFIELDS.S023PO**

PKTS OUT RU (INCL RTP/SNA SEG RU ONLY)

**EESTATSFIELDS.S024BI**

BYTES IN LLC CONNECTION TEST

**EESTATSFIELDS.S024BO**

BYTES OUT LLC CONNECTION TEST

**EESTATSFIELDS.S024PI**

PKTS IN LLC CONNECTION TEST

**EESTATSFIELDS.S024PO**

PKTS OUT LLC CONNECTION TEST

**EESTATSFIELDS.S025BI**

BYTES IN SPARE 25

**EESTATSFIELDS.S025BO**

BYTES OUT SPARE 25

**EESTATSFIELDS.S025PI**

PKTS IN SPARE 25

**EESTATSFIELDS.S025PO**

PKTS OUT SPARE 25

**EESTATSFIELDS.S026BI**

BYTES IN SPARE 26

**EESTATSFIELDS.S026BO**

BYTES OUT SPARE 26

**EESTATSFIELDS.S026PI**

PKTS IN SPARE 26

**EESTATSFIELDS.S026PO**

PKTS OUT SPARE 26

**EESTATSFIELDS.S027BI**

BYTES IN SPARE 26

**EESTATSFIELDS.S027BO**

BYTES OUT SPARE 26

**EESTATSFIELDS.S027PI**

PKTS IN SPARE 26

**EESTATSFIELDS.S027PO**

PKTS OUT SPARE 26

**EESTATSFIELDS.S027BI**

BYTES IN SPARE 27

**EESTATSFIELDS.S027BO**

BYTES OUT SPARE 27

**EESTATSFIELDS.S027PI**

PKTS IN SPARE 27

**EESTATSFIELDS.S027PO**

PKTS OUT SPARE 27

**EESTATSFIELDS.S028BI**

BYTES IN SPARE 28

**EESTATSFIELDS.S028BO**

BYTES OUT SPARE 28

**EESTATSFIELDS.S028PI**

PKTS IN SPARE 28

**EESTATSFIELDS.S028PO**

PKTS OUT SPARE 28

**EESTATSFIELDS.S029BI**

BYTES IN SPARE 29

**EESTATSFIELDS.S029BO**

BYTES OUT SPARE 29

**EESTATSFIELDS.S029PI**

PKTS IN SPARE 29

**EESTATSFIELDS.S029PO**

PKTS OUT SPARE 29

**EESTATSFIELDS.S030BI**

BYTES IN SPARE 30

**EESTATSFIELDS.S030BO**

BYTES OUT SPARE 30

**EESTATSFIELDS.S030PI**

PKTS IN SPARE 30

**EESTATSFIELDS.S030PO**

PKTS OUT SPARE 30



**EESTATSFIELDS.S031BI**

INDETERMINATE (TRUNCATED)

**EESTATSFIELDS.S031BO**

INDETERMINATE (TRUNCATED)

**EESTATSFIELDS.S031PI**

INDETERMINATE (TRUNCATED)

**EESTATSFIELDS.S031PO**

INDETERMINATE (TRUNCATED)

**EESTATSFIELDS.S032BI**

UNKNOWN FORMAT

**EESTATSFIELDS.S032BO**

UNKNOWN FORMAT

**EESTATSFIELDS.S032PI**

UNKNOWN FORMAT

**EESTATSFIELDS.S032PO**

UNKNOWN FORMAT

**ELIGIBLEFORDIST**

ELIGIBLE FOR DISTRIBUTION (IE UNSURE)

**ENDDATETIME**

CONNECTION END DATE/TIME (LCL YYYYMMDDHHMMSSSTH)

**EXCEPTION**

EXCEPTION INDICATOR

**FRAGMENTATION**

FRAGMENTATION INDICATOR

**HISTCOUNT**

# TIMES THIS CONNECTION MADE "HISTORY"

**HISTORY**

YES/NO HISTORY INDICATOR – YES INDICATES CONNECTION HAS ENDED

**HISTORYSECS**

HISTORY KEEP TIME USED (SECONDS)

**HOMEIPADDRESS**

HOME IP ADDRESS

**IBFRAG**

I/B FRAGMENTATION INDICATOR

**IBFRAGCOUNT**

# INBOUND FRAGMENTED PACKETS SEEN

**ICID**

INTERNAL UCN CONNECTION ID KEY FOR TRACE

**IDLETIME**

CONNECTION IDLE TIME (100THS)

**IFCMISMATCHCOUNT**

# TIMES NO IFC MATCHED

**INITIALSENDRATE**

INITIAL SEND RATE

**INTF1.I1NAME**

INTERFACE 1 NAME

**INTF1.I1NUMBYTESIN**

INTERFACE 1 # BYTES IN

**INTF1.I1NUMBYTESOUT**

INTERFACE 1 # BYTES OUT

**INTF1.I1NUMPKTSIN**

INTERFACE 1 # PACKETS IN

**INTF1.I1NUMPKTSOUT**

INTERFACE 1 # PACKETS OUT

**INTF2.I2NAME**

INTERFACE 2 NAME

**INTF2.I22NUMBYTESIN**

INTERFACE 2 # BYTES IN

**INTF2.I2NUMBYTESOUT**

INTERFACE 2 # BYTES OUT

**INTF2.I2NUMPKTSIN**

INTERFACE 2 # PACKETS IN

**INTF2.I2NUMPKTSOUT**

INTERFACE 2 # PACKETS OUT

**INTF3.I3NAME**

INTERFACE 3 NAME

**INTF3.I3NUMBYTESIN**

INTERFACE 3 # BYTES IN

**INTF3.I3NUMBYTESOUT**

INTERFACE 3 # BYTES OUT

**INTF3.I3NUMPKTSIN**

INTERFACE 3 # PACKETS IN

**INTF3.I3NUMPKTSOUT**

INTERFACE 3 # PACKETS OUT

**INTF4.I4NAME**

INTERFACE 4 NAME

**INTF4.I4NUMBYTESIN**

INTERFACE 4 # BYTES IN

**INTF4.I4NUMBYTESOUT**

INTERFACE 4 # BYTES OUT

**INTF4.I4NUMPKTSIN**

INTERFACE 4 # PACKETS IN

**INTF4.I4NUMPKTSOUT**

INTERFACE 4 # PACKETS OUT

**IPV4**

YES IF BOTH ADDRS ARE IPV4

**IPV6**

IPV6 INTERFACE INDICATOR

**JOBNAME**

CONNECTION OWNER NAME

**KEY.APPLICATIONNAME**

APPLICATION NAME

**KEY.INTERFACENAME**

INTERFACE NAME

**KEY.JOBNAME**

CONNECTION OWNER NAME

**KEY.LCLIPADDR**

LOCAL IP ADDRESSPORT

**KEY.LCLIPPORT**

LOCAL IP PORT

**KEY.NAME**

RTP PU NAME

**KEY.RMTIPADDR**

REMOTE IP ADDRESS

**KEY.RMTIPPORT**

REMOTE IP PORT

**KEY.RMTNWADDR**

REMOTE NETWORK IP ADDRESS

**KEY.STACKNAME**

STACK NAME

**KNOWNTYPE**

KNOWN TYPE

**LASTOWNERNAME**

LAST PORT OWNER NAME

**LASTPATHSWITCHREASON**

LAST PATH SWITCH REASON

**LCLCPNAME**

LOCAL VTAM CP NAME

**LCLNWID**

LOCAL VTAM N/W ID

**LCLTCID**

LOCAL VTAM TCID

**LEVEL1BYTESIN**

LEVEL 1 BYTES IN

**LEVEL1BYTESOUT**

LEVEL 1 BYTES OUT

**LEVEL2BYTESIN**

LEVEL 2 BYTES IN

**LEVEL2BYTESOUT**

LEVEL 2 BYTES OUT

**LEVEL3BYTESIN**

LEVEL 3 BYTES IN

**LEVEL3BYTESOUT**

LEVEL 3 BYTES OUT

**LEVEL1COUNTER1**

LEVEL 1 EXTRA COUNTER 1

**LEVEL1COUNTER2**

LEVEL 1 EXTRA COUNTER 2

**LEVEL2COUNTER1**

LEVEL 2 EXTRA COUNTER 1

**LEVEL2COUNTER2**

LEVEL 2 EXTRA COUNTER 2

**LEVEL3COUNTER1**

LEVEL 3 EXTRA COUNTER 1

**LEVEL3COUNTER2**

LEVEL 3 EXTRA COUNTER 2

**LOOPBACK**

LOOPBACK INTERFACE INDICATOR

**NLPSONACKWAITQ**

NLPS ON WAIT FOR ACK QUEUE

**NLPSONINSEQQ**

NLPS ON IN SEGMENT QUEUE

**NLPSONOOSQ**

NLPS ON OUT OF SEQUEUCE MESSAGE QUEUE

**NLPSONPENDSENDQ**

NLPS ON PENDING SEND QUEUE

**NLPSRCVD**

NLPS RECEIVED

**NLPSRXMT**

NLPS RXMT

**NLPSENT**

NLPS SENT

**NOAPPL**

IND: THIS IS THE "NOAPPL" IFA

**NOKEYS**

SET TO YES TO PREVENT SCAN KEY USE

**NUMLULUCESS**

NUMBER OF LU-LU SESSIONS USING HPR CONNECTION

**NUMSVRRSTS**

NUMBER OF SERVER-ISSUED RESETS

**NUMTCPCONN.CURRENT**

CURRENT # TCP CONNECTIONS

**NUMTCPCONN.ENDED**

ENDED # TCP CONNECTIONS

**NUMTCPCONN.NUMDUR $n$**

NUM ENDED TCP CONNS DURATION BUCKET #  $n$

$n$  is 1 through 10.

**NUMTCPCONN.SMFBYTESIN**

TOTAL BYTES IN FROM SMF ETC CLOSE EVENT

**NUMTCPCONN.SMFBYTESOUT**

TOTAL BYTES OUT FROM SMF ETC CLOSE EVENT

**NUMTCPCONN.STARTED**

STARTED # TCP CONNECTIONS

**NUMTCPCONN.TCPBYTESRCVD**

TOTAL TCP APPL BYTES RECEIVED FROM PKTS

**NUMTCPCONN.TCPBYTESENT**

TOTAL TCP APPL BYTES SENT FROM PKTS

**NUMTCPCONN.TOTAL**

TOTAL # TCP CONNECTIONS

**NWI.AVAILV4MTU**

IND: IPV4 MTU AVAIL

**NWI.AVAILV4MTULF**

IND: IPV4 LAST FAIL MTU AVAIL

**NWI.AVAILV4TTL**

IND: IPV4 TTL AVAIL

**NWI.AVAILV4TTLLF**

IND: IPV4 LAST FAIL TTL AVAIL

**NWI.AVAILV6HOP**

IND: IPV6 HOP AVAIL

**NWI.AVAILV6HOPLF**

IND: IPV6 LAST FAIL HOP AVAIL

**NWI.AVAILV6MTU**

IND: IPV6 MTU AVAIL

**NWI.AVAILV6MTULF**

IND: IPV4 LAST FAIL MTU AVAIL

**NWI.BEINGMONITORED**

IND: REMOTE ADDRESS BEING MONITORED

**NWI.HLF6A**

IPV6 HOP LAST FAIL RPT IP ADDRESS

**NWI.HOP6**

IPV6 HOP VALUE

**NWI.HOP6MIN**

IPV6 HOP VALUE SET MINUTE

**NWI.LASTREFUPD1MIN**

LAST REFERENCED/UPDATED 1-MINUTE TIME

**NWI.LASTUPDATED1MIN**

LAST UPDATED 1 MINUTE TIME

**NWI.LFHOP6**

LAST-FAIL IPV6 HOP VALUE

**NWI.LFMTU4**

LAST-FAIL IPV4 MTU VALUE

**NWI.LFMTU6**

LAST-FAIL IPV6 MTU VALUE

**NWI.LFTTL4**

LAST-FAIL IPV4 TTL VALUE

**NWI.MLF4A**

IPV4 MTU LAST FAIL RPT IP ADDRESS

**NWI.MLF6A**

IPV6 MTU LAST FAIL RPT IP ADDRESS

**NWI.MONMTU**

IND: MONITING MTU

**NWI.MONRTT**

IND: MONITING RTT

**NWI.MONTTL**

IND: MONITING TTL (V6: HOP)

**NWI.MTU4**

IPV4 MTU VALUE

**NWI.MTU4MIN**

IPV4 MTU VALUE SET MINUTE

**NWI.MTU6**

IPV6 MTU VALUE

**NWI.MTU6MIN**

IPV6 MTU VALUE SET MINUTE

**NWI.NUM1MINSLOTS**

# 1 MIN SLOTS IN RECORD

**NWI.ONEMA.Xn.AVGSAMP**

AVERAGE RTT SAMPLES TIME S#  $n$  (1/100THS)

$n$  is 0 through 10.

**NWI.ONEMA.Xn.ICMPNUMSAMP**

NUMBER OF ICMP-DERIVED RTT SAMPLES S#  $n$

$n$  is 0 through 10.

**NWI.ONEMA.Xn.INTNUMRTTREQS**

# INTERNAL RTT REQUESTS S#  $n$

$n$  is 0 through 10.

**NWI.ONEMA.Xn.MAXRTTSAMPVAL**

MAX RTT SAMPLE VALUE SEEN S#  $n$

$n$  is 0 through 10.



**NWI.ONEMA.Xn.MINRTTSAMPVAL**MIN RTT SAMPLE VALUE SEEN S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.NUMFRAGPKTSRCVD**# OF FRAG"D PACKETS RECEIVED (FRONT ONLY) S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.NUMFRAGPKTSSENT**# OF FRAG"D PACKETS SENT (FRONT ONLY) S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.NUMTCPRETRANS**# TCP RETRANSMITS S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.SDSAMP**STD. DEV RTT SAMPLES TIME S# *n* (1/100THS)*n* is 0 through 10.**NWI.ONEMA.Xn.SUMRTTSAMP**SUM OF RTT SAMPLE TIMES S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.SUMSQRTTSAMP**SUM OF SQUARES OF RTT SAMPLE TIMES S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.TOTNUMSAMP**TOTAL NUMBER OF RTT SAMPLES S# *n**n* is 0 through 10.**NWI.ONEMA.Xn.VASAMP**VARIANCE RTT SAMPLES TIME S# *n* (1/100THS)*n* is 0 through 10.**NWI.TLF4A**

IPV4 TTL LAST FAIL RPT IP ADDRESS

**NWI.TTL4**

IPV4 TTL VALUE

**NWI.TTL4MIN**

IPV4 TTL VALUE SET MINUTE

**NWI.VIA4**

IPV4 VIA IP ADDRESS

**NWI.VIA6**

IPV6 VIA IP ADDRESS

**OBFRAG**

O/B FRAGMENTATION INDICATOR

**OBFRAGCOUNT**

# O/BOUND FRAGMENTED PACKETS SEEN

**PARTCPNAME**

PARTNER CP NAME

**PARTNWID**

PARTNER N/W ID

**PATHSWITCHLOCAL**

NUMBER OF PATH SWITCHES INITIATED BY LOCAL CP

**PATHSWITCHREMOTE**

NUMBER OF PATH SWITCHES INITIATED BY REMOTE CP

**PKTINFO.AVGRTT**

APPARENT AVG ROUND-TRIP TIME (RTT) (100THS)

**PKTINFO.CLOSEREASONAVAILABLE**

INDICATES IF THE CLOSE REASON IS AVAILABLE

**PKTINFO.CLOSEREASONSMT**

CLOSE REASON FROM SMT

**PKTINFO.CONNDURSLOTNUM**

CONNECTION DURATION SLOT NUMBER (WHEN CLOSED)

**PKTINFO.HIGHPRTYFIELDS.FRAG**

FRAGMENTATION INDICATOR

**PKTINFO.HIGHPRTYFIELDS.IBFRAG**

I/B FRAGMENTATION INDICATOR

**PKTINFO.HIGHPRTYFIELDS.ICID1**

HIGH CONN 1 UCN.ICID

**PKTINFO.HIGHPRTYFIELDS.ICID2**

HIGH CONN 2 UCN.ICID

**PKTINFO.HIGHPRTYFIELDS.ICID3**

HIGH CONN 3 UCN.ICID

**PKTINFO.HIGHPRTYFIELDS.NUMBYTESIN**

HIGH CONN # BYTES IN

**PKTINFO.HIGHPRTYFIELDS.NUMBYTESOUT**

HIGH CONN # BYTES OUT

**PKTINFO.HIGHPRTYFIELDS.NUMPKTSIN**

HIGH CONN # PACKETS IN

**PKTINFO.HIGHPRTYFIELDS.NUMPKTSOUT**

HIGH CONN # PACKETS OUT

**PKTINFO.HIGHPRTYFIELDS.OBFRAG**

O/B FRAGMENTATION INDICATOR

**PKTINFO.LCL.L1START**

LCL APPARENT 1ST APP RSP TIME (100THS)

**PKTINFO.LCL.L1STARTSET**

YES IF LCL 1ST APP RSP TIME SET

**PKTINFO.LCL.LAVGART**

LCL APPARENT AVG APP RSP TIME (100THS)

**PKTINFO.LCL.LCURWIND**

LCL CURRENT RCV WINDOW SIZE (AS SCALED)

**PKTINFO.LCL.LFRAG**

YES IF O/B FRAGMENTED PACKETS

**PKTINFO.LCL.LMAXART**

LCL APPARENT MAX APP RSP TIME (100THS)

**PKTINFO.LCL.LMAXWIND**

LCL MAXIMUM RCV WINDOW SIZE (AS SCALED)

**PKTINFO.LCL.LMINART**

LCL APPARENT MIN APP RSP TIME (100THS)

**PKTINFO.LCL.LMINWIND**

LCL MINIMUM RCV WINDOW SIZE (AS SCALED)

**PKTINFO.LCL.LMSS**

LCL (OUTBOUND) MAXIMUM SEGMENT SIZE DFLT OR SET

**PKTINFO.LCL.LOERROR**

YES IF LCL OPTION SYNTAX ERROR SEEN

**PKTINFO.LCL.LOMSS**

YES IF LCL OPTION: MAXIMUM SEGMENT SIZE

**PKTINFO.LCL.LOOTHER**

YES IF LCL OPTION: <OTHERS>

**PKTINFO.LCL.LOSACK**

YES IF LCL OPTION: SACK

**PKTINFO.LCL.LOSACKP**

YES IF LCL OPTION: SACK PERMITTED SENT

**PKTINFO.LCL.LOTSOPT**

YES IF LCL OPTION: TSOPT

**PKTINFO.LCL.LOWSC**

YES IF LCL OPTION: WINDOW SCALE

**PKTINFO.LCL.LREXMITS**

LCL APPARENT # RETRANSMITS

**PKTINFO.LCL.LWINDCLOSECOUNT**

LCL COUNT OF TIMES RCV WINDOW CLOSED

**PKTINFO.LCL.LWINDCLOSETIME**

LCL TOTAL TIME RCV WINDOW CLOSED (100THS)

**PKTINFO.LCL.LWINDPROBECOUNT**

LCL # TIMES A WINDOW PROBE SENT TO REMOTE

**PKTINFO.LCL.LWS**

LCL (OUTBOUND) WINDOW SCALE VALUE (OR 0)

**PKTINFO.LOWPRTYFIELDS.FRAG**

FRAGMENTATION INDICATOR

**PKTINFO.LOWPRTYFIELDS.IBFRAG**

I/B FRAGMENTATION INDICATOR

**PKTINFO.LOWPRTYFIELDS.ICID1**

LOW CONN 1 UCN.ICID

**PKTINFO.LOWPRTYFIELDS.ICID2**

LOW CONN 2 UCN.ICID

**PKTINFO.LOWPRTYFIELDS.ICID3**

LOW CONN 3 UCN.ICID

**PKTINFO.LOWPRTYFIELDS.NUMBYTESIN**

LOW CONN # BYTES IN

**PKTINFO.LOWPRTYFIELDS.NUMBYTESOUT**

LOW CONN # BYTES OUT

**PKTINFO.LOWPRTYFIELDS.NUMPKTSIN**

LOW CONN # PACKETS IN

**PKTINFO.LOWPRTYFIELDS.NUMPKTSOUT**

LOW CONN # PACKETS OUT

**PKTINFO.LOWPRTYFIELDS.OBFRAG**

O/B FRAGMENTATION INDICATOR

**PKTINFO.MAXRTT**

APPARENT MAX ROUND-TRIP TIME (RTT) (100THS)

**PKTINFO.MEDPRTYFIELDS.FRAG**

FRAGMENTATION INDICATOR

**PKTINFO.MEDPRTYFIELDS.IBFRAG**

I/B FRAGMENTATION INDICATOR

**PKTINFO.MEDPRTYFIELDS.ICID1**

MED CONN 1 UCN.ICID

**PKTINFO.MEDPRTYFIELDS.ICID2**

MED CONN 2 UCN.ICID

**PKTINFO.MEDPRTYFIELDS.ICID3**

MED CONN 3 UCN.ICID

**PKTINFO.MEDPRTYFIELDS.NUMBYTESIN**

MED CONN # BYTES IN

**PKTINFO.MEDPRTYFIELDS.NUMBYTESOUT**

MED CONN # BYTES OUT

**PKTINFO.MEDPRTYFIELDS.NUMPKTSIN**

MED CONN # PACKETS IN

**PKTINFO.MEDPRTYFIELDS.NUMPKTSOUT**

MED CONN # PACKETS OUT

**PKTINFO.MEDPRTYFIELDS.OBFRAG**

O/B FRAGMENTATION INDICATOR

**PKTINFO.MINRTT**

APPARENT MIN ROUND-TRIP TIME (RTT) (100THS)

**PKTINFO.NETWORKFIELDS.FRAG**

FRAGMENTATION INDICATOR

**PKTINFO.NETWORKFIELDS.IBFRAG**

I/B FRAGMENTATION INDICATOR

**PKTINFO.NETWORKFIELDS.ICID1**

NTW CONN 1 UCN.ICID

**PKTINFO.NETWORKFIELDS.ICID2**

NTW CONN 2 UCN.ICID

**PKTINFO.NETWORKFIELDS.ICID3**

NTW CONN 3 UCN.ICID

**PKTINFO.NETWORKFIELDS.NUMBYTESIN**

NTW CONN # BYTES IN

**PKTINFO.NETWORKFIELDS.NUMBYTESOUT**

NTW CONN # BYTES OUT

**PKTINFO.NETWORKFIELDS.NUMPKTSIN**

NTW CONN # PACKETS IN

**PKTINFO.NETWORKFIELDS.NUMPKTSOUT**

NTW CONN # PACKETS OUT

**PKTINFO.NETWORKFIELDS.OBFRAG**

O/B FRAGMENTATION INDICATOR

**PKTINFO.NUMRTT**

NUMBER RTT SAMPLES USED TO CALC AVG

**PKTINFO.PKTINFOSET**

PACKET INFO AVAILABLE INDICATOR (SET ON 1ST PKT)

**PKTINFO.PKTSTATSFIELDS.S01BI**

BYTES IN TOTAL PKTS/BYTES

**PKTINFO.PKTSTATSFIELDS.S01BO**

BYTES OUT TOTAL PKTS/BYTES

**PKTINFO.PKTSTATSFIELDS.S01PI**

PKTS IN TOTAL PKTS/BYTES

**PKTINFO.PKTSTATSFIELDS.S01PO**

PKTS OUT TOTAL PKTS/BYTES

**PKTINFO.PKTSTATSFIELDS.S02BI**

BYTES IN IP HDR

**PKTINFO.PKTSTATSFIELDS.S02BO**

BYTES OUT IP HDR

**PKTINFO.PKTSTATSFIELDS.S02PI**

PKTS IN IP HDR

**PKTINFO.PKTSTATSFIELDS.S02PO**

PKTS OUT IP HDR

**PKTINFO.PKTSTATSFIELDS.S03BI**

BYTES IN -UDP HDR

**PKTINFO.PKTSTATSFIELDS.S03BO**

BYTES OUT UDP HDR

**PKTINFO.PKTSTATSFIELDS.S03PI**

PKTS IN UDP HDR

**PKTINFO.PKTSTATSFIELDS.S03PO**

PKTS OUT UDP HDR

**PKTINFO.PKTSTATSFIELDS.S04BI**

BYTES IN -LLC HDR

**PKTINFO.PKTSTATSFIELDS.S04BO**

BYTES OUT LLC HDR

**PKTINFO.PKTSTATSFIELDS.S04PI**

PKTS IN LLC HDR

**PKTINFO.PKTSTATSFIELDS.S04PO**

PKTS OUT LLC HDR

**PKTINFO.PKTSTATSFIELDS.S05BI**

BYTES IN LLC XID QRY/XCH

**PKTINFO.PKTSTATSFIELDS.S05BO**

BYTES OUT LLC XID QRY/XCH

**PKTINFO.PKTSTATSFIELDS.S05PI**

PKTS IN LLC XID QRY/XCH

**PKTINFO.PKTSTATSFIELDS.S05PO**

PKTS OUT LLC XID QRY/XCH

**PKTINFO.PKTSTATSFIELDS.S06BI**

BYTES IN LLC HEARTBEAT

**PKTINFO.PKTSTATSFIELDS.S06BO**

BYTES OUT LLC HEARTBEAT

**PKTINFO.PKTSTATSFIELDS.S06PI**

PKTS IN LLC HEARTBEAT

**PKTINFO.PKTSTATSFIELDS.S06PO**

PKTS OUT LLC HEARTBEAT

**PKTINFO.PKTSTATSFIELDS.S07BI**

BYTES IN LLC DISC

**PKTINFO.PKTSTATSFIELDS.S07BO**

BYTES OUT LLC DISC

**PKTINFO.PKTSTATSFIELDS.S07PI**

PKTS IN LLC DISC

**PKTINFO.PKTSTATSFIELDS.S07PO**

PKTS OUT LLC DISC

**PKTINFO.PKTSTATSFIELDS.S08BI**

BYTES IN FUNCTION ROUTING

**PKTINFO.PKTSTATSFIELDS.S08BO**

BYTES OUT FUNCTION ROUTING

**PKTINFO.PKTSTATSFIELDS.S08PI**

PKTS IN FUNCTION ROUTING

**PKTINFO.PKTSTATSFIELDS.S08PO**

PKTS OUT FUNCTION ROUTING

**PKTINFO.PKTSTATSFIELDS.S09BI**

BYTES IN NHDR

**PKTINFO.PKTSTATSFIELDS.S09BO**

BYTES OUT NHDR



**PKTINFO.PKTSTATSFIELDS.S09PI**

PKTS IN NHDR

**PKTINFO.PKTSTATSFIELDS.S09PO**

PKTS OUT NHDR

**PKTINFO.PKTSTATSFIELDS.S010BI**

BYTES IN NHDR WITH SLOWDOWN 1 OR 2 SET

**PKTINFO.PKTSTATSFIELDS.S010BO**

BYTES OUT NHDR WITH SLOWDOWN 1 OR 2 SET

**PKTINFO.PKTSTATSFIELDS.S010PI**

PKTS IN NHDR WITH SLOWDOWN 1 OR 2 SET

**PKTINFO.PKTSTATSFIELDS.S010PO**

PKTS OUT NHDR WITH SLOWDOWN 1 OR 2 SET

**PKTINFO.PKTSTATSFIELDS.S011BI**

BYTES IN THDR

**PKTINFO.PKTSTATSFIELDS.S011BO**

BYTES OUT THDR

**PKTINFO.PKTSTATSFIELDS.S011PI**

PKTS IN THDR

**PKTINFO.PKTSTATSFIELDS.S011PO**

PKTS OUT THDR

**PKTINFO.PKTSTATSFIELDS.S012BI**

BYTES IN THDR ONLY (HPRCTL)

**PKTINFO.PKTSTATSFIELDS.S012BO**

BYTES OUT THDR ONLY (HPRCTL)

**PKTINFO.PKTSTATSFIELDS.S012PI**

PKTS IN THDR ONLY (HPRCTL)

**PKTINFO.PKTSTATSFIELDS.S012PO**

PKTS OUT THDR ONLY (HPRCTL)

**PKTINFO.PKTSTATSFIELDS.S013BI**

BYTES IN THDR WITH GAP INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S013BO**

BYTES OUT THDR WITH GAP INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S013PI**

PKTS IN THDR WITH GAP INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S013PO**

PKTS OUT THDR WITH GAP INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S014BI**

BYTES IN THDR WITH IDLE INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S014BO**

BYTES OUT THDR WITH IDLE INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S014PI**

PKTS IN THDR WITH IDLE INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S014PO**

PKTS OUT THDR WITH IDLE INDICATOR SET

**PKTINFO.PKTSTATSFIELDS.S015BI**

BYTES IN RTP SEGMENT (THDR NOT SOM+EOM)

**PKTINFO.PKTSTATSFIELDS.S015BO**

BYTES OUT RTP SEGMENT (THDR NOT SOM+EOM)

**PKTINFO.PKTSTATSFIELDS.S015PI**

PKTS IN RTP SEGMENT (THDR NOT SOM+EOM)

**PKTINFO.PKTSTATSFIELDS.S015PO**

PKTS OUT RTP SEGMENT (THDR NOT SOM+EOM)

**PKTINFO.PKTSTATSFIELDS.S016BI**

BYTES IN THDR + RU ONLY

**PKTINFO.PKTSTATSFIELDS.S016BO**

BYTES OUT THDR + RU ONLY

**PKTINFO.PKTSTATSFIELDS.S016PI**

PKTS IN THDR + RU ONLY

**PKTINFO.PKTSTATSFIELDS.S016PO**

PKTS OUT THDR + RU ONLY

**PKTINFO.PKTSTATSFIELDS.S017BI**

BYTES IN SLOWDOWN 1 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S017BO**

BYTES OUT SLOWDOWN 1 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S017PI**

PKTS IN SLOWDOWN 1 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S017PO**

PKTS OUT SLOWDOWN 1 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S018BI**

BYTES IN SLOWDOWN 2 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S018BO**

BYTES OUT SLOWDOWN 2 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S018PI**

PKTS IN SLOWDOWN 2 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S018PO**

PKTS OUT SLOWDOWN 2 (NHDR OR THDR)

**PKTINFO.PKTSTATSFIELDS.S019BI**

BYTES IN ARB CRITICAL (CRITICAL, THDR)

**PKTINFO.PKTSTATSFIELDS.S019BO**

BYTES OUT ARB CRITICAL (CRITICAL, THDR)

**PKTINFO.PKTSTATSFIELDS.S019PI**

PKTS IN ARB CRITICAL (CRITICAL, THDR)

**PKTINFO.PKTSTATSFIELDS.S019PO**

PKTS OUT ARB CRITICAL (CRITICAL, THDR)

**PKTINFO.PKTSTATSFIELDS.S020BI**

BYTES IN TH (ALL)

**PKTINFO.PKTSTATSFIELDS.S020BO**

BYTES OUT TH (ALL)

**PKTINFO.PKTSTATSFIELDS.S020PI**

PKTS IN TH (ALL)

**PKTINFO.PKTSTATSFIELDS.S020PO**

PKTS OUT TH (ALL)

**PKTINFO.PKTSTATSFIELDS.S021BI**

BYTES IN TH (NOT OIC)

**PKTINFO.PKTSTATSFIELDS.S021BO**

BYTES OUT TH (NOT OIC)

**PKTINFO.PKTSTATSFIELDS.S021PI**

PKTS IN TH (NOT OIC)

**PKTINFO.PKTSTATSFIELDS.S021PO**

PKTS OUT TH (NOT OIC)

**PKTINFO.PKTSTATSFIELDS.S022BI**

BYTES IN RH

**PKTINFO.PKTSTATSFIELDS.S022BO**

BYTES OUT RH

**PKTINFO.PKTSTATSFIELDS.S022PI**

PKTS IN RH

**PKTINFO.PKTSTATSFIELDS.S022PO**

PKTS OUT RH

**PKTINFO.PKTSTATSFIELDS.S023BI**

BYTES IN RU (INCL RTP/SNA SEG RU ONLY)

**PKTINFO.PKTSTATSFIELDS.S023BO**

BYTES OUT RU (INCL RTP/SNA SEG RU ONLY)

**PKTINFO.PKTSTATSFIELDS.S023PI**

PKTS IN RU (INCL RTP/SNA SEG RU ONLY)

**PKTINFO.PKTSTATSFIELDS.S023PO**

PKTS OUT RU (INCL RTP/SNA SEG RU ONLY)

**PKTINFO.PKTSTATSFIELDS.S024BI**

BYTES IN LLC CONN TEST

**PKTINFO.PKTSTATSFIELDS.S024BO**

BYTES OUT LLC CONN TEST

**PKTINFO.PKTSTATSFIELDS.S024PI**

PKTS IN LLC CONN TEST

**PKTINFO.PKTSTATSFIELDS.S024PO**

PKTS OUT LLC CONN TEST

**PKTINFO.PKTSTATSFIELDS.S025BI**

BYTES IN SPARE 25

**PKTINFO.PKTSTATSFIELDS.S025BO**

BYTES OUT SPARE 25

**PKTINFO.PKTSTATSFIELDS.S025PI**

PKTS IN SPARE 25

**PKTINFO.PKTSTATSFIELDS.S025PO**

PKTS OUT SPARE 25

**PKTINFO.PKTSTATSFIELDS.S026BI**

BYTES IN SPARE 26

**PKTINFO.PKTSTATSFIELDS.S026BO**

BYTES OUT SPARE 26

**PKTINFO.PKTSTATSFIELDS.S026PI**

PKTS IN SPARE 26

**PKTINFO.PKTSTATSFIELDS.S026PO**

PKTS OUT SPARE 26

**PKTINFO.PKTSTATSFIELDS.S027BI**

BYTES IN SPARE 27

**PKTINFO.PKTSTATSFIELDS.S027BO**

BYTES OUT SPARE 27

**PKTINFO.PKTSTATSFIELDS.S027PI**

PKTS IN SPARE 27

**PKTINFO.PKTSTATSFIELDS.S027PO**

PKTS OUT SPARE 27

**PKTINFO.PKTSTATSFIELDS.S028BI**

BYTES IN SPARE 28

**PKTINFO.PKTSTATSFIELDS.S028BO**

BYTES OUT SPARE 28

**PKTINFO.PKTSTATSFIELDS.S028PI**

PKTS IN SPARE 28

**PKTINFO.PKTSTATSFIELDS.S028PO**

PKTS OUT SPARE 28

**PKTINFO.PKTSTATSFIELDS.S029BI**

BYTES IN SPARE 29

**PKTINFO.PKTSTATSFIELDS.S029BO**

BYTES OUT SPARE 29

**PKTINFO.PKTSTATSFIELDS.S029PI**

PKTS IN SPARE 29

**PKTINFO.PKTSTATSFIELDS.S029PO**

PKTS OUT SPARE 29

**PKTINFO.PKTSTATSFIELDS.S030BI**

BYTES IN SPARE 30

**PKTINFO.PKTSTATSFIELDS.S030BO**

BYTES OUT SPARE 30

**PKTINFO.PKTSTATSFIELDS.S030PI**

PKTS IN SPARE 30

**PKTINFO.PKTSTATSFIELDS.S030PO**

PKTS OUT SPARE 30

**PKTINFO.PKTSTATSFIELDS.S031BI**

BYTES IN INDETERMINATE (TRUNCATED)

**PKTINFO.PKTSTATSFIELDS.S031BO**

BYTES OUT INDETERMINATE (TRUNCATED)

**PKTINFO.PKTSTATSFIELDS.S031PI**

PKTS IN INDETERMINATE (TRUNCATED)

**PKTINFO.PKTSTATSFIELDS.S031PO**

PKTS OUT INDETERMINATE (TRUNCATED)

**PKTINFO.PKTSTATSFIELDS.S032BI**

BYTES IN UNKNOWN FORMAT

**PKTINFO.PKTSTATSFIELDS.S032BO**

BYTES OUT UNKNOWN FORMAT

**PKTINFO.PKTSTATSFIELDS.S032PI**

PKTS IN UNKNOWN FORMAT

**PKTINFO.PKTSTATSFIELDS.S032PO**

PKTS OUT UNKNOWN FORMAT

**PKTINFO.RESET**

CONVERSATION RESET INDICATOR ANY

**PKTINFO.RESETCLT**

CONVERSATION RESET INDICATOR CLIENT

**PKTINFO.RESETLCL**

CONVERSATION RESET INDICATOR LOCAL

**PKTINFO.RESETRMT**

CONVERSATION RESET INDICATOR REMOTE

**PKTINFO.RESETSVR**

CONVERSATION RESET INDICATOR SERVER

**PKTINFO.RMT.R1START**

REMOTE APPARENT 1ST APP RSP TIME (100THS)

**PKTINFO.RMT.R1STARTSET**

YES IF REMOTE 1ST APP RSP TIME SET

**PKTINFO.RMT.RAVGART**

REMOTE APPARENT AVG APP RSP TIME (100THS)

**PKTINFO.RMT.RCURWIND**

REMOTE CURRENT RCV WINDOW SIZE (AS SCALED)

**PKTINFO.RMT.RFRAG**

YES IF I/B FRAGMENTED PACKETS

**PKTINFO.RMT.RMAXART**

REMOTE APPARENT MAX APP RSP TIME (100THS)

**PKTINFO.RMT.RMAXWIND**

REMOTE MAXIMUM RCV WINDOW SIZE (AS SCALED)

**PKTINFO.RMT.RMINART**

REMOTE APPARENT MIN APP RSP TIME (100THS)

**PKTINFO.RMT.RMINWIND**

REMOTE MINIMUM RCV WINDOW SIZE (AS SCALED)

**PKTINFO.RMT.RMSS**

REMOTE (INBOUND) MAXIMUM SEGMENT SIZE DFLT OR SET

**PKTINFO.RMT.ROERROR**

YES IF REMOTE OPTION SYNTAX ERROR SEEN

**PKTINFO.RMT.ROMSS**

YES IF REMOTE OPTION MSS

**PKTINFO.RMT.ROOTHER**

YES IF REMOTE OPTION <OTHERS>

**PKTINFO.RMT.ROSACK**

YES IF REMOTE OPTION SACK

**PKTINFO.RMT.ROSACKP**

YES IF REMOTE OPTION SACK PERMITTED RECEIVED

**PKTINFO.RMT.ROTSOPT**

YES IF REMOTE OPTION TSOPT

**PKTINFO.RMT.ROWSC**

YES IF REMOTE OPTION WINDOW SCALE

**PKTINFO.RMT.RREXMITS**

REMOTE APPARENT # RETRANSMITS

**PKTINFO.RMT.RWINDCLOSECOUNT**

REMOTE COUNT OF TIMES RCV WINDOW CLOSED

**PKTINFO.RMT.RWINDCLOSETIME**

REMOTE TOTAL TIME RCV WINDOW CLOSED (100THS)

**PKTINFO.RMT.RWINDPROBECOUNT**

REMOTE # TIMES A WINDOW PROBE SENT FM LCL

**PKTINFO.RMT.RWS**

REMOTE (INBOUND) WINDOW SCALE VALUE (OR 0)

**PKTINFO.SIGNALFIELDS.FRAG**

FRAGMENTATION INDICATOR

**PKTINFO.SIGNALFIELDS.IBFRAG**

I/B FRAGMENTATION INDICATOR

**PKTINFO.SIGNALFIELDS.ICID1**

SIG CONN 1 UCN.ICID

**PKTINFO.SIGNALFIELDS.ICID2**

SIG CONN 2 UCN.ICID

**PKTINFO.SIGNALFIELDS.ICID3**

SIG CONN 3 UCN.ICID

**PKTINFO.SIGNALFIELDS.NUMBYTESIN**

SIG CONN # BYTES IN

**PKTINFO.SIGNALFIELDS.NUMBYTESOUT**

SIG CONN # BYTES OUT



**PKTINFO.SIGNALFIELDS.NUMPKTSIN**

SIG CONN # PACKETS IN

**PKTINFO.SIGNALFIELDS.NUMPKTSOUT**

SIG CONN # PACKETS OUT

**PKTINFO.SIGNALFIELDS.OBFRAG**

O/B FRAGMENTATION INDICATOR

**PKTINFO.STATS.FIVEMINX0.BYTESIN**

BYTES IN 5 MIN CURRENT

**PKTINFO.STATS.FIVEMINX0.BYTESOUT**

BYTES OUT 5 MIN CURRENT

**PKTINFO.STATS.FIVEMINX0.PKTSIN**

PKTS IN 5 MIN CURRENT

**PKTINFO.STATS.FIVEMINX0.PKTSOUT**

PKTS OUT 5 MIN CURRENT

**PKTINFO.STATS.FIVEMINX $n$ .BYTESIN**BYTES IN 5 MIN –  $n$  $n$  is 1 through 12.**PKTINFO.STATS.FIVEMINX $n$ .BYTESOUT**BYTES OUT 5 MIN -  $n$  $n$  is 1 through 12.**PKTINFO.STATS.FIVEMINX $n$ .PKTSIN**PKTS IN 5 MIN -  $n$  $n$  is 1 through 12.**PKTINFO.STATS.FIVEMINX $n$ .PKTSOUT**PKTS OUT 5 MIN -  $n$  $n$  is 1 through 12.**PKTINFO.STATS.LASTREFUPD1MIN**

LAST REFERENCED/UPDATED 1 MINUTE TIME

**PKTINFO.STATS.LASTUPDATED1MIN**

LAST UPDATED 1-MINUTE TIME

**PKTINFO.STATS.NUM1MINSLOTS**

# 1 MIN SLOTS IN RECORD

**PKTINFO.STATS.NUM5MINSLOTS**

FIELD WITH # 5 MIN SLOTS IN RECORD

**PKTINFO.STATS.ONEMINXn.BYTESIN**

BYTES IN 1 MIN CURRENT

**PKTINFO.STATS.ONEMINXn.BYTESOUT**

BYTES OUT 1 MIN CURRENT

**PKTINFO.STATS.ONEMINXn.PKTSIN**

PKTS IN 1 MIN CURRENT

**PKTINFO.STATS.ONEMINXn.PKTSOUT**

PKTS OUT 1 MIN CURRENT

**PKTINFO.STATS.ONEMINXn.BYTESIN**

BYTES IN 1 MIN -  $n$

$n$  is 1 through 5.

**PKTINFO.STATS.ONEMINXn.BYTESOUT**

BYTES OUT 1 MIN -  $n$

$n$  is 1 through 5.

**PKTINFO.STATS.ONEMINXn.PKTSIN**

PKTS IN 1 MIN -  $n$

$n$  is 1 through 5.

**PKTINFO.STATS.ONEMINXn.PKTSOUT**

PKTS OUT 1 MIN -  $n$

$n$  is 1 through 5.

**PKTINFO.STATS.TOTAL1MBYTESIN**

TOTAL BYTES IN IN LAST 5 MINS

**PKTINFO.STATS.TOTAL1MBYTESINNC**

TOTAL BYTES IN IN LAST 5 MINS X CUR

**PKTINFO.STATS.TOTAL1MBYTESIO**

TOTAL BYTES I/O IN LAST 5 MINS

**PKTINFO.STATS.TOTAL1MBYTESIONC**

TOTAL BYTES I/O IN LAST 5 MINS X CUR

**PKTINFO.STATS.TOTAL1MBYTESOUT**

TOTAL BYTES OUT IN LAST 5 MINS

**PKTINFO.STATS.TOTAL1MBYTESOUTNC**

TOTAL BYTES OUT IN LAST 5 MINS X CUR

**PKTINFO.STATS.TOTAL1MPKTSIN**

TOTAL PKTS IN IN LAST 5 MINS

**PKTINFO.STATS.TOTAL1MPKTSINNC**

TOTAL PKTS IN IN LAST 5 MINS X CUR

**PKTINFO.STATS.TOTAL1MPKTSIO**

TOTAL PKTS I/O IN LAST 5 MINS

**PKTINFO.STATS.TOTAL1MPKTSIONC**

TOTAL PKTS I/O IN LAST 5 MINS X CUR

**PKTINFO.STATS.TOTAL1MPKTSOUT**

TOTAL PKTS OUT IN LAST 5 MINS

**PKTINFO.STATS.TOTAL1MPKTSOUTNC**

TOTAL PKTS OUT IN LAST 5 MINS X CUR

**PKTINFO.STATS.TOTAL5MBYTESIN**

TOTAL BYTES IN IN LAST 60 MINS

**PKTINFO.STATS.TOTAL5MBYTESINNC**

TOTAL BYTES IN IN LAST 60 MINS X CUR

**PKTINFO.STATS.TOTAL5MBYTESIO**

TOTAL BYTES I/O IN LAST 60 MINS

**PKTINFO.STATS.TOTAL5MBYTESIONC**

TOTAL BYTES I/O IN LAST 60 MINS X CUR

**PKTINFO.STATS.TOTAL5MBYTESOUT**

TOTAL BYTES OUT IN LAST 60 MINS

**PKTINFO.STATS.TOTAL5MBYTESOUTNC**

TOTAL BYTES OUT IN LAST 60 MINS X CUR

**PKTINFO.STATS.TOTAL5MPKTSIN**

TOTAL PKTS IN IN LAST 60 MINS

**PKTINFO.STATS.TOTAL5MPKTSINNC**

TOTAL PKTS IN IN LAST 60 MINS X CUR

**PKTINFO.STATS.TOTAL5MPKTSIO**

TOTAL PKTS I/O IN LAST 60 MINS

**PKTINFO.STATS.TOTAL5MPKTSIONC**

TOTAL PKTS I/O IN LAST 60 MINS X CUR

**PKTINFO.STATS.TOTAL5MPKTSOUT**

TOTAL PKTS OUT IN LAST 60 MINS

**PKTINFO.STATS.TOTAL5MPKTSOUTNC**

TOTAL PKTS OUT IN LAST 60 MINS X CUR

**PKTINFO.STATS.TOTALBYTESIN**

TOTAL BYTES RECEIVED

**PKTINFO.STATS.TOTALBYTESOUT**

TOTAL BYTES SENT

**PKTINFO.STATS.TOTALPKTSIN**

TOTAL PACKETS RECEIVED

**PKTINFO.STATS.TOTALPKTSOUT**

TOTAL PACKETS SENT

**PKTINFO.TCPBYTESRCVD**

TOTAL TCP APPL BYTES RECEIVED

**PKTINFO.TCPBYTESENT**

TOTAL TCP APPL BYTES SENT

**PKTINFO.TCPSTATE**

TCP CONNECTION STATE

**PKTINFO.TCPTYPE**

APPARENT TCP USAGE TYPE (CLIENT, SERVER, UNKNOWN)

**PKTINFO.TURNCOUNT**

CALCULATED TURN COUNT

**PLUNAME**

APPLICATION LU NAME

**QDIO**

QDIO INTERFACE INDICATOR

**RESCOUNT**

# TIMES THIS CONNECTION RESURRECTED FROM HISTORY

**RESTORECOUNT**

CONNECTION RESTORE COUNT

**RESTOREDATETIME**

CONNECTION RESTORE DATE/TIME (LCL YYYYMMDDHHMMSSSTH)

**RMTCPNAME**

REMOTE CP NAME

**RMTNWADDR**

REMOTE NETWORK IP ADDRESS

**RMTNWID**

REMOTE N/W ID

**RMTTCID**

REMOTE VTAM TCID

**SCHIFNAME**

SEARCH I/F NAME MATCH ANY PRESENT I/F NAME

**SECCONVSEEN**

INDICATOR FOR SSL/TLS CONVERSATIONS SEEN

**SECINFO.SECALERTAVAIL**

IND: SEC ALERT (SECALERTINFO) AVAILABLE

**SECINFO.SECALERTINFO**

CONV SECURITY ALERT INFO IF AVAIL SECINFO.SECCIPHER

**SECINFO.SECCIPHERAVAIL**

IND: SEC CIPHER (SECCIPHER) AVAILABLE

**SECINFO.SECCOMP**

CONV SECURITY COMPRESSION OPTION IF KNOWN

**SECINFO.SECCOMPAVAIL**

IND: SEC COMPRESS (SECCOMP) AVAILABLE

**SECINFO.SECHSSEEN**

IND: SEC HANDSHAKE SEEN

**SECINFO.SECINUSE**

IND: SEC IN USE

**SECINFO.SECMODE**

CONV SECURITY MODE

**SECINFO.SECSETUPFAILED**

IND: SEC (SETUP) FAILED

**SECINFO.SECVERSDIFF**

IND: SEC CLIENT/SERVER VERSIONS DIFFERENT

**SECINFO.SECVERSION**

CONV SECURITY VERSION

**SECINFO.SECVERSIONAVAIL**

IND: SEC VERSION (SECVERSION) AVAILABLE

**SECPKTSSEEN**

IND: SEC-REL PKTS SEEN FOR THIS REMOTE N/W

**SEGOFFLOADSEEN**

TCP SEG OFFLOAD REQ SEEN

**SLUNAME**

TELNET LU NAME SLU

**SMFBYTESIN**

TOTAL BYTES IN FROM SMF ETC CLOSE EVENT

**SMFBYTESOUT**

TOTAL BYTES OUT FROM SMF ETC CLOSE EVENT

**SMOOTHRTT**

SMOOTHED ROUND-TRIP TIME (MILLISECONDS)

**SNAINFO.HIGHFIELDS.BYTESRCVD**

HIGH PRTY BYTES RECEIVED

**SNAINFO.HIGHFIELDS.BYTESSENT**

HIGH PRTY BYTES SENT

**SNAINFO.HIGHFIELDS.NLP SRCVD**

HIGH PRTY NLPS RECEIVED

**SNAINFO.HIGHFIELDS.NLP SRXMT**

HIGH PRTY NLPS RXMT

**SNAINFO.HIGHFIELDS.NLP SENT**

HIGH PRTY NLPS SENT

**SNAINFO.LCLCPNAME**

LOCAL VTAM CP NAME

**SNAINFO.LCLNWID**

LOCAL VTAM N/W ID

**SNAINFO.LCLSAP**

LOCAL SAP

**SNAINFO.LINENAME**

LINE NAME

**SNAINFO.LOWFIELDS.BYTESRCVD**

LOW PRY BYTES RECEIVED

**SNAINFO.LOWFIELDS.BYTESENT**

LOW PRY BYTES SENT

**SNAINFO.LOWFIELDS.NLP SRCVD**

LOW PRY NLPS RECEIVED

**SNAINFO.LOWFIELDS.NLP SRXMT**

LOW PRY NLPS RXMT

**SNAINFO.LOWFIELDS.NLP SENT**

LOW PRY NLPS SENT

**SNAINFO.MEDFIELDS.BYTESRCVD**

MEDIUM PRY BYTES RECEIVED

**SNAINFO.MEDFIELDS.BYTESENT**

MEDIUM PRY BYTES SENT

**SNAINFO.MEDFIELDS.NLP SRCVD**

MEDIUM PRY NLPS RECEIVED

**SNAINFO.MEDFIELDS.NLP SRXMT**

MEDIUM PRY NLPS RXMT

**SNAINFO.MEDFIELDS.NLP SENT**

MEDIUM PRY NLPS SENT

**SNAINFO.NETWORKFIELDS.BYTESRCVD**

NETWORK PRY BYTES RECEIVED

**SNAINFO.NETWORKFIELDS.BYTESENT**

NETWORK PRY BYTES SENT

**SNAINFO.NETWORKFIELDS.NLP SRCVD**

NETWORK PRY NLPS RECEIVED

**SNAINFO.NETWORKFIELDS.NLP SRXMT**

NETWORK PRY NLPS RXMT

**SNAINFO.NETWORKFIELDS.NLPSENT**

NETWORK PRTY NLPS SENT

**SNAINFO.NUMLULUCESS**

NUMBER OF LU-LU SESSIONS ON EE CONNECTION

**SNAINFO.NUMRTPPIPE**

NUMBER OF RTP PIPES ON EE CONNECTION

**SNAINFO.PUNAME**

PU NAME

**SNAINFO.RMTCPNAME**

REMOTE VTAM CP NAME

**SNAINFO.RMTNWID**

REMOTE VTAM N/W ID

**SNAINFO.RMTSAP**

REMOTE SAP

**SNAINFO.SIGNALFIELDS.BYTESRCVD**

SIGNAL PRTY BYTES RECEIVED

**SNAINFO.SIGNALFIELDS.BYTESSENT**

SIGNAL PRTY BYTES SENT

**SNAINFO.SIGNALFIELDS.NLP SRCVD**

SIGNAL PRTY NLPS RECEIVED

**SNAINFO.SIGNALFIELDS.NLP SRXMT**

SIGNAL PRTY NLPS RXMT

**SNAINFO.SIGNALFIELDS.NLP SENT**

SIGNAL PRTY NLPS SENT

**SNAINFO.SNACONNECT**

SNA CONNECTION ACTIVE INDICATOR

**SNAINFO.SNADYNPU**

SNA DYNAMIC PU INDICATOR

**SNAINFO.SNAINFOAVAIL**

SNA INFORMATION AVAILABLE INDICATOR

**SNAINFO.STATS.FIVEMINX0.HIGH.BYTESRCVD**

HIGH PRTY BYTES RECEIVED 5 MIN CURR SNA



**SNAINFO.STATS.FIVEMINX0.HIGH.BYTESENT**

HIGH PRTY BYTES SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.HIGH.NLP SRCVD**

HIGH PRTY NLPS RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.HIGH.NLP SRXMT**

HIGH PRTY NLPS RXMT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.HIGH.NLP SENT**

HIGH PRTY NLPS SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX $n$ .HIGH.BYTESRCVD**

HIGH PRTY BYTES RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .HIGH.BYTESENT**

HIGH PRTY BYTES SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .HIGH.NLP SRCVD**

HIGH PRTY NLPS RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .HIGH.NLP SRXMT**

HIGH PRTY NLPS RXMT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .HIGH.NLP SENT**

HIGH PRTY NLPS SENT 5 MIN  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX0.LOW.BYTESRCVD**

LOW PRTY BYTES RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.LOW.BYTESENT**

LOW PRTY BYTES SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.LOW.NLP SRCVD**

LOW PRTY NLPS RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.LOW.NLP SRXMT**

LOW PRTY NLPS RXMT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.LOW.NLP SENT**

LOW PRTY NLPS SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX $n$ .LOW.BYTESRCVD**

LOW PRTY BYTES RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .LOW.BYTESENT**

LOW PRTY BYTES SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .LOW.NLP SRCVD**

LOW PRTY NLPS RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .LOW.NLP SRXMT**

LOW PRTY NLPS RXMT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .LOW.NLP SENT**

LOW PRTY NLPS SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX0.MED.BYTESRCVD**

MEDIUM PRTY BYTES RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.MED.BYTESENT**

MEDIUM PRTY BYTES SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.MED.NLP SRCVD**

MEDIUM PRTY NLPS RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.MED.NLP SRXMT**

MEDIUM PRTY NLPS RXMT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.MED.NLP SENT**

MEDIUM PRTY NLPS SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX $n$ .MED.BYTESRCVD**

MEDIUM PRTY BYTES RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .MED.BYTESENT**

MEDIUM PRTY BYTES SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .MED.NLP SRCVD**

MEDIUM PRTY NLPS RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12

**SNAINFO.STATS.FIVEMINX $n$ .MED NLPSRXMT**

MEDIUM PRTY NLPS RXMT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .MED.NLP SENT**

MEDIUM PRTY NLPS SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX0.NET.BYTESRCVD**

NETWORK PRTY BYTES RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.NET.BYTESENT**

NETWORK PRTY BYTES SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.NET.NLP SRCVD**

NETWORK PRTY NLPS RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.NET.NLP SRXMT**

NETWORK PRTY NLPS RXMT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.NET.NLP SENT**

NETWORK PRTY NLPS SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX $n$ .NET.BYTESRCVD**

NETWORK PRTY BYTES RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .NET.BYTESENT**

NETWORK PRTY BYTES SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .NET.NLP SRCVD**

NETWORK PRTY NLPS RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .NET NLPSRXMT**

NETWORK PRTY NLPS RXMT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .NET.NLPSENT**

NETWORK PRTY NLPS SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX0.SIG.BYTESRCVD**

SIGNAL PRTY BYTES RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.SIG.BYTESENT**

SIGNAL PRTY BYTES SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.SIG.NLPsrcVD**

SIGNAL PRTY NLPS RECEIVED 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.SIG.NLPsrXMT**

SIGNAL PRTY NLPS RXMT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX0.SIG.NLPSENT**

SIGNAL PRTY NLPS SENT 5 MIN CURR SNA

**SNAINFO.STATS.FIVEMINX $n$ .SIG.BYTESRCVD**

SIGNAL PRTY BYTES RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .SIG.BYTESENT**

SIGNAL PRTY BYTES SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .SIG.NLPsrcVD**

SIGNAL PRTY NLPS RECEIVED 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .SIG.NLPsrXMT**

SIGNAL PRTY NLPS RXMT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.FIVEMINX $n$ .SIG.NLPSENT**

SIGNAL PRTY NLPS SENT 5 MIN -  $n$  SNA

$n$  is 1 through 12.

**SNAINFO.STATS.LASTREFUPD5MIN**

LAST REF/UPDATED 5-MINUTE TIME SNA

**SNAINFO.STATS.LASTUPDATED5MIN**

LAST UPDATED 5-MINUTE TIME SNA

**SNAINFO.STATS.NUM5MINSLOTS**

# 5 MIN SLOTS IN RECORD SNA

**SOCKETVIEWFIELDS.CICSTERMID**

SOCKETVIEW CICS TERMINAL ID

**SOCKETVIEWFIELDS.ITXNNAME**

SOCKETVIEW CICS TRANSACTION NAME

**SOCKETVIEWFIELDS.ITXNUM**

SOCKETVIEW CICS TRANSACTION NUMBER

**SOCKETVIEWFIELDS.SOCKETVIEWHANDLE**

SOCKETVIEW HANDLE

**SPARECOUNTER1**

SPARE COUNTER # 1

**SPARECOUNTER2**

SPARE COUNTER # 2

**SPARECOUNTER3**

SPARE COUNTER # 3

**STACKTYPE**

STACK TYPE

**STARTDATETIME**

CONNECTION START DATE/TIME (LCL YYYYMMDDHHMMSSSTH)

**STATS.FIVEMINX0.BYTESIN**

BYTES IN 5 MIN CURRENT

**STATS.FIVEMINX0.BYTESOUT**

BYTES OUT 5 MIN CURRENT

**STATS.FIVEMINX0.DATABYTESRCVD**

DATA BYTES RECEIVED 5 MIN CURRENT

**STATS.FIVEMINX0.DATABYTESSENT**

DATA BYTES SENT 5 MIN CURRENT

**STATS.FIVEMINX0.LASTPATHSWITCHREASON**

LAST PATH SWITCH REASON 5 MIN CURRENT

**STATS.FIVEMINX0.NLPSRCVD**

NLPS RECEIVED 5 MIN CURRENT

**STATS.FIVEMINX0.NLPSRXMT**

NLPS RXMT 5 MIN CURRENT

**STATS.FIVEMINX0.NLPSENT**

NLPS SENT 5 MIN CURRENT

**STATS.FIVEMINX0.PATHSWITCHLOCAL**

PATH SWITCHES BY LOCAL CP 5 MIN CURRENT

**STATS.FIVEMINX0.PATHSWITCHREMOTE**

PATH SWITCHES BY REMOTE CP 5 MIN CURRENT

**STATS.FIVEMINX0.PKTSIN**

PKTS IN 5 MIN CURRENT

**STATS.FIVEMINX0.PKTSOUT**

PKTS OUT 5 MIN CURRENT

**STATS.FIVEMINX0.TOTALBYTESRCVD**

TOTAL BYTES RECEIVED 5 MIN CURRENT

**STATS.FIVEMINX0.TOTALBYTESENT**

TOTAL BYTES SENT 5 MIN CURRENT

**STATS.FIVEMINX $n$ .BYTESIN**

BYTES IN 5 MIN -  $n$

$n$  is 1 through 12.

**STATS.FIVEMINX $n$ .BYTESOUT**

BYTES OUT 5 MIN -  $n$

$n$  is 1 through 12.

**STATS.FIVEMINX $n$ .DATABYTESRCVD**

DATA BYTES RECEIVED 5 MIN -  $n$

$n$  is 1 through 12.

**STATS.FIVEMINX $n$ .DATABYTESENT**

DATA BYTES SENT 5 MIN -  $n$

$n$  is 1 through 12.

**STATS.FIVEMINX $n$ .LASTPATHSWITCHREASON**

LAST PATH SWITCH REASON 5 MIN -  $n$

$n$  is 1 through 12.

**STATS.FIVEMINX $n$ .NLPSRCVD**NLPS RECEIVED 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .NLPSRXMT**NLPS RXMT 5 MIN -  $n$  $n$  is 1 through 12**STATS.FIVEMINX $n$ .NLPSENT**NLPS SENT 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .PATHSWITCHLOCAL**PATH SWITCHES BY LOCAL CP 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .PATHSWITCHREMOTE**PATH SWITCHES BY REMOTE CP 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .PKTSIN**PKTS IN 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .PKTSOUT**PKTS OUT 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .TOTALBYTESRCVD**TOTAL BYTES RECEIVED 5 MIN -  $n$  $n$  is 1 through 12.**STATS.FIVEMINX $n$ .TOTALBYTESENT**TOTAL BYTES SENT 5 MIN -  $n$  $n$  is 1 through 12.**STATS.LASTREFUPD1MIN**

LAST REFERENCED/UPDATED 1-MINUTE TIME

**STATS.LASTREFUPD5MIN**

LAST REF/UPDATED 5-MINUTE TIME SNA

**STATS.LASTUPDATED1MIN**

LAST UPDATED 1 MINUTE TIME

**STATS.LASTUPDATED5MIN**

LAST UPDATED 5-MINUTE TIME SNA

**STATS.NUM1MINSLOTS**

# 1 MIN SLOTS IN RECORD

**STATS.NUM5MINSLOTS**

FIELD WITH # 5 MIN SLOTS IN RECORD

**STATS.ONEMINX0.BYTESIN**

BYTES IN 1 MIN CURRENT

**STATS.ONEMINX0.BYTESOUT**

BYTES OUT 1 MIN CURRENT

**STATS.ONEMINX0.PKTSIN**

PKTS IN 1 MIN CURRENT

**STATS.ONEMINX0.PKTSOUT**

PKTS OUT 1 MIN CURRENT

**STATS.ONEMINX $n$ .BYTESIN**

BYTES IN 1 MIN -  $n$

$n$  is 1 through 5.

**STATS.ONEMINX $n$ .BYTESOUT**

BYTES OUT 1 MIN -  $n$

$n$  is 1 through 5.

**STATS.ONEMINX $n$ .PKTSIN**

PKTS IN 1 MIN -  $n$

$n$  is 1 through 5.

**STATS.ONEMINX $n$ .PKTSOUT**

PKTS OUT 1 MIN -  $n$

$n$  is 1 through 5.

**STATS.TOTAL1MBYTESIN**

TOTAL BYTES IN IN LAST 5 MINS

**STATS.TOTAL1MBYTESINNC**

TOTAL BYTES IN IN LAST 5 MINS X CUR

**STATS.TOTAL1MBYTESIO**

TOTAL BYTES I/O IN LAST 5 MINS



**STATS.TOTAL1MBYTESIONC**

TOTAL BYTES I/O IN LAST 5 MINS X CUR

**STATS.TOTAL1MBYTESOUT**

TOTAL BYTES OUT IN LAST 5 MINS

**STATS.TOTAL1MBYTESOUTNC**

TOTAL BYTES OUT IN LAST 5 MINS X CUR

**STATS.TOTAL1MPKTSIN**

TOTAL PKTS IN IN LAST 5 MINS

**STATS.TOTAL1MPKTSINNC**

TOTAL PKTS IN IN LAST 5 MINS X CUR

**STATS.TOTAL1MPKTSIO**

TOTAL PKTS I/O IN LAST 5 MINS

**STATS.TOTAL1MPKTSIONC**

TOTAL PKTS I/O IN LAST 5 MINS X CUR

**STATS.TOTAL1MPKTSOUT**

TOTAL PKTS OUT IN LAST 5 MINS

**STATS.TOTAL1MPKTSOUTNC**

TOTAL PKTS OUT IN LAST 5 MINS X CUR

**STATS.TOTAL5MBYTESIN**

TOTAL BYTES IN IN LAST 60 MINS

**STATS.TOTAL5MBYTESINNC**

TOTAL BYTES IN IN LAST 60 MINS X CUR

**STATS.TOTAL5MBYTESIO**

TOTAL BYTES I/O IN LAST 60 MINS

**STATS.TOTAL5MBYTESIONC**

TOTAL BYTES I/O IN LAST 60 MINS X CUR

**STATS.TOTAL5MBYTESOUT**

TOTAL BYTES OUT IN LAST 60 MINS

**STATS.TOTAL5MBYTESOUTNC**

TOTAL BYTES OUT IN LAST 60 MINS X CUR

**STATS.TOTAL5MPKTSIN**

TOTAL PKTS IN IN LAST 60 MINS

**STATS.TOTAL5MPKTSINNC**

TOTAL PKTS IN IN LAST 60 MINS X CUR

**STATS.TOTAL5MPKTSIO**

TOTAL PKTS I/O IN LAST 60 MINS

**STATS.TOTAL5MPKTSIONC**

TOTAL PKTS I/O IN LAST 60 MINS X CUR

**STATS.TOTAL5MPKTSOUT**

TOTAL PKTS OUT IN LAST 60 MINS

**STATS.TOTAL5MPKTSOUTNC**

TOTAL PKTS OUT IN LAST 60 MINS X CUR

**STATS.TOTALBYTESIN**

TOTAL BYTES RECEIVED

**STATS.TOTALBYTESOUT**

TOTAL BYTES SENT

**STATS.TOTALPKTSIN**

TOTAL PACKETS RECEIVED

**STATS.TOTALPKTSOUT**

TOTAL PACKETS SENT

**STEADYRED**

STEADY ARB RED INDICATOR

**TCPARI.COLLARTSTATS**

COLLECT APPL RSP TIME STATISTICS?

**TCPARI.LASTREFUPD1MIN**

LAST REFERENCED/UPDATED 1-MINUTE TIME

**TCPARI.LASTUPDATED1MIN**

LAST UPDATED 1-MINUTE TIME

**TCPARI.NUM1MINSLOTS**

# 1 MIN SLOTS IN RECORD

**TCPARI.ONEMA.Xn.AVGSAVP**

AVERAGE SAMPLES TIME S# *n* (1/100THS)

*n* is 1 through 10.

**TCPARI.ONEMA.Xn.ENDNCONNS**# CONNS THAT ENDED S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.MAXNCONNS**MAX # OF CONNS S# *n**n* is 1 through 10**TCPARI.ONEMA.Xn.MAXSAMP**MAX ARSP SAMPLE VALUE S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.MINNCONNS**MIN # OF CONNS S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.MINSAMP**MIN ARSP SAMPLE VALUE S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.NUMSAMP**NUMBER OF SAMPLES S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.SDSAMP**STD. DEV SAMPLES TIME S# *n* (1/100THS)*n* is 1 through 10.**TCPARI.ONEMA.Xn.STANCONNS**# CONNS THAT STARTED S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.SUMSAMP**SUM OF SAMPLE TIMES S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.SUMSQSAMP**SUM OF SQUARES OF SAMPLE TIMES S# *n**n* is 1 through 10.**TCPARI.ONEMA.Xn.VASAMP**VARIANCE SAMPLES TIME S# *n* (1/100THS)*n* is 1 through 10.

**TCPSEGOFFLOAD.AVGLASTTCPSEGSIZE**

AVG LEN OF TCP DATA IN LAST SEGMENT

**TCPSEGOFFLOAD.MAXLASTTCPSEGSIZE**

MAX LEN OF TCP DATA IN LAST SEGMENT

**TCPSEGOFFLOAD.MINLASTTCPSEGSIZE**

MIN LEN OF TCP DATA IN LAST SEGMENT

**TCPSEGOFFLOAD.SEGGENPKTBYES**

TCP O/B BYTES GENERATED FROM SEQMENTATION OFFLOAD REQ

**TCPSEGOFFLOAD.SEGGENPKTCNT**

TCP O/B PKTS GENERATED FROM SEQMENTATION OFFLOAD REQ

**TCPSEGOFFLOAD.SEGREQPKTBYES**

TCP O/B BYTES WITH SEGMENTATION OFFLOAD REQ

**TCPSEGOFFLOAD.SEGREQPKTCNT**

TCP O/B PKTS WITH SEGMENTATION OFFLOAD REQ

**TCPSEGOFFLOAD.UNSEGPKTBYES**

TCP O/B BYTES WITHOUT SEGMENTATION OFFLOAD REQ

**TCPSEGOFFLOAD.UNSEGPKTCNT**

TCP O/B PKTS WITHOUT SEGMENTATION OFFLOAD REQ

**TCPTYPE**

APPARENT TCP USAGE TYPE (CLIENT, SERVER, UNKNOWN)

**TIMEOUTSECS**

TIMEOUT TIME USED (SECONDS)

**TOTALBYTESRCVD**

TOTAL BYTES RECEIVED

**TOTALBYTESENT**

TOTAL BYTES SENT

**TOTALDISCPKTS**

TOTAL DISC PACKETS RECEIVED (EG CHKSUM ERR)

**TOTALRTDBYESIN**

TOTAL ROUTED BYTES RECEIVED

**TOTALRTDBYESOUT**

TOTAL ROUTED BYTES SENT

**TOTALRTDPKTSIN**

TOTAL ROUTED PACKETS RECEIVED

**TOTALRTDPKTSOUT**

TOTAL ROUTED PACKETS SENT

**UDPPAYLOADBYTESIN**

UDP PAYLOAD BYTES IN

**UDPPAYLOADBYTESOUT**

UDP PAYLOAD BYTES OUT

**USERID**

USER ID

**VIRTTNET**

VIRTUAL TELNET INDICATOR

**VIRTUAL**

VIRTUAL RECORD INDICATOR

**WS**

YES IF TCN CREATED BY WARM START

**XCF**

XCF INTERFACE INDICATOR



# Index

---

## A

- accessing
  - alert monitor • 90
  - IP security management functions • 185, 186
  - transient logs • 329
- action lists • 41
- actions, connection
  - Drop • 86
  - VTAM Display • 84
- actions, router
  - Interfaces • 192
  - Lookup • 192
  - MIBinsight • 192
  - Ping • 192
  - Routing Table • 192
  - System Information • 192
  - Telnet • 192
- active traces • 233
- activity logs
  - browsing online • 333
  - FTP activity • 335
  - Obeyfile processing • 122
  - record additional information • 334
  - Telnet activity • 334
- address spaces
  - activities on stack • 125
  - IP traffic • 177
  - performance • 176
- alert history • 95
- Alert Monitor
  - accessing • 90
- alerts
  - closure • 95
  - monitoring • 90
  - operator notes • 94
  - problem tickets • 94
  - transient log, and • 93
- analyzing SNA sessions • 85
- applications
  - traffic by interfaces • 60
- APPN
  - APPN multisystem RTP health • 163
  - APPN RTP health • 163
  - connectivity • 161

- CP-CP sessions • 161
- directory • 162
- local RTP health • 163
- LU requestors • 160
- performance • 159
- resources monitor • 158
- RTP health thresholds • 164
- RTP pipes • 160
- topology • 162
- transport resources • 160
- VTAM commands • 165
- architecture, peer-to-peer • 29
- AT-TLS • 84

## B

- baselines • 279
- Broadcast Services
  - overview • 23
- business applications, traffic by interfaces • 60

## C

- canceling changes to a record • 44
- channel card • 134
- channel card information • 135
  - application • 136
  - channel • 138
  - CLAW • 141
  - internal LAN • 143
  - SNA (CSNA) • 142
  - TCP offload • 142
- channel card information, TN3270 server
  - displaying • 139
  - log • 139, 140
- Channel Interface Processor (CIP) • 134
- Channel Port Adapter (CPA) • 134
- CICS (Customer Information Control System)
  - command server interface • 182
  - server, starting • 183
  - socket connections • 75
  - Socket Management, connections • 181
  - traffic • 63, 184
  - transaction, starting • 183
- CICS resources
  - information • 182
  - IP traffic • 184

---

- performance • 184
- Cisco channel cards
  - overview • 134
- Cisco Mainframe Channel Connection (CMCC) • 134
- CLAW
  - information • 141
  - subchannels • 141
- CLOSE command • 95
- commands
  - Telnet • 252
- commands, specific
  - \$LOG • 122
  - CTTRACE • 232
  - LOCATE • 43, 78, 236, 239
  - NETSTAT • 324
  - NSLOOKUP • 324
  - PING • 193
  - PROFILE • 330
  - SORT • 78, 142, 235, 238
  - SPLIT • 48, 49
  - SWAP • 48, 49
  - TELNET • 254
- communication • 24
- configuration
  - data sets • 120
  - FTP • 120
  - Obeyfile • 121
- connection lists • 73
  - FTP • 74
  - general • 75
  - multiple systems • 81
  - sort • 78
- connections
  - AT-TLS • 84
  - diagnosing • 86
  - dropping • 86
  - locating information • 78
  - searching • 295
  - Socket Management • 181
  - sorting lists • 78
  - specific • 79
  - statistics • 81
  - Telnet • 245
  - testing • 193
  - to remote host • 254
- connectivity
  - problem diagnosis • 73, 80
  - testing • 73, 80
- console commands • 115

- contacting technical support • 4
- control codes, Telnet • 258
- CP-CP sessions • 161
- CSM
  - performance • 180
  - usage • 179
- CSNA information • 142
- CTTRACE
  - saving trace data • 234
  - starting • 232
- customer support, contacting • 4

## D

- data
  - DRDA packets, decoded • 216
  - entry panels • 43
  - IPSec packets, decoded • 217
  - packet • 212, 213, 219, 225
  - reassembly, • 229
  - SOAP packets, decoded • 218
  - TLS and SSL handshake packets, decoded • 217
  - validation • 44
- data transfer problems, diagnosis • 73
- DB2 traffic • 63
- devices
  - dropping a connection • 86
  - links • 115, 117
  - OSA • 130
  - tracing a route • 187
- diagnosing
  - connections • 86
  - data and protocol problems • 86
  - IP conditions • 56
  - performance and connectivity • 73, 80
  - resource attributes • 278
  - throughput • 88
- diagnosing Telnet problems
  - connection • 138
  - response time • 87
- displaying
  - activity log from the transient log • 329
  - alert history • 95
  - logs • 329
  - transient logs • 329
- Domain Name Server • 123
- DRDA (Distributed Relational Database Architecture)
  - packets • 213, 216
  - reports • 229



---

dropping a connection • 86

## E

entering data • 43

Enterprise Extender

- bytes by connection • 66

- bytes by direction • 68

- bytes by VIPA • 65

- bytes through port • 66

- bytes through protocol layer • 67

- check connectivity • 146

- EE packets by type • 69

- EE Traffic Explorer • 64

- overview • 145

- payload • 68

- performance • 154

- port activity • 147

- RTP pipes • 147

- summarized information • 155

- traffic analysis • 156

- traffic statistics • 148

- transmission group health • 150

- UDP connections • 147

- XCA major nodes • 155

errors, packet tracing • 240, 241

## F

fields

- mandatory • 43

- optional • 43

- prompted • 44

file transfer events, searching • 295

filing data • 44

Find function • 43

Firefox, setup • 352

focal point regions • 29

FTP (File Transfer Protocol)

- activity in the log • 335

- configuration (FTP.DATA) • 120

- connections • 74

- events, searching • 295

full-screen Telnet, starting connections • 246

function keys

- Telnet-specific • 247

## H

header data

- ICMP • 223

- TCP • 223

- UDP • 223

help, online

- facilities for messages • 331

- overview • 46

historical displays

- IP activities • 302

horizontal scrolling • 42

## I

icons

- traffic light • 30

IMS (Information Management System)

- traffic • 63

Index Menu • 45

Initialization in Progress panel • 36

interface traffic by applications • 58

Interfaces action • 192

internal LAN

- adapters • 143

- channel card information • 143

Internet Explorer, setup • 350

interpreting responses

- to a ping • 194

- to a traceroute • 188

IP address, finding • 62, 80, 124

IP conditions

- diagnosis • 56

- summaries • 53

IP node monitor • 97, 98

- node status • 107

- performance history of a node • 281

IP resource classes

- ASMON • 173

- CIP • 135

- CSM • 179

- EE • 146

- STACK • 111

IP resource monitor • 107

- performance history of a resource • 280

- resource status • 107

IP security management • 185

IP Summary Display • 30, 53, 57

IP traffic • 177, 184

- application traffic by interfaces • 60

- interface traffic by applications • 58

- statistics by stack • 114

- subsystems • 63

---

- summaries • 57
- IPSec
  - packets • 213, 217
- issuing console commands • 115

## K

- knowledge base
  - multisystem • 29
- knowledge base definitions
  - customizing panel access • 46

## L

- line commands
  - SmartTrace • 197
- list types • 41
- listeners • 75
- LOCATE command • 43, 78, 236, 239
- locating records • 43
- logging off • 36
- logon • 35
- logs
  - displaying • 329
  - TN3270 server • 140
  - transient • 329
- Lookup action • 192
- LUs (logical units)
  - finding name • 79
  - for a PU • 140

## M

- Managed Object Development Services • 25
- mandatory fields • 43
- masks
  - connections, listing • 79
- menus, specific
  - Network Diagnosis Functions • 187
- messages
  - help for • 48, 331
  - session awareness • 88
  - TPA • 87
- MIBinsight • 263
  - action • 192
  - updating values • 272
- MIBinsight browser
  - access • 190, 264
  - adding definitions to browser • 267
  - deleting objects from browser • 273
  - information available on browser • 264

- MIB object values • 269, 270
- overview • 264
- reformatting octet strings • 272
- table values • 271
- user security • 274
- mini trace, Cisco Telnet LU • 138
- monitoring
  - active alerts • 90
  - channel cards • 134
  - performance • 33
- monitors
  - IP nodes • 98
  - IP resources • 107
- multiple select lists • 41
- multisystem environment, knowledge bases • 29
- multisystem support
  - defined • 29
  - focal point regions • 29
  - multisystem support, listing connections • 81
  - overview • 29
  - subordinates • 29

## N

- navigation
  - menus • 38
  - splitting screens • 49
  - swapping screens • 49
  - toggleing between windows • 49
  - working in two windows • 48
- NETSTAT command • 324
- NSLOOKUP command • 324
- numbered lists • 41

## O

- Obeyfile
  - changing the configuration • 121
  - data set member • 123
  - viewing contents and results • 122
- OCS
  - SmartTrace, and • 199
- online help
  - messages • 48
  - overview • 46
- optional fields • 43
- OSA • 127
  - configuration • 131
  - device list • 130
  - performance • 129

---

utilization • 128

## P

### Packet Analyzer

IP activity lists • 302  
records • 359

### packet tracing • 232

active traces • 233  
connections within a trace • 238  
CTRACE • 232, 233  
data for a selected packet • 240  
data, decoding • 213  
data, locating • 212  
errors • 240, 241  
formatted packets • 219  
header data • 223  
IP header fields • 221  
IP options • 222  
packet details • 221  
packets in a trace • 240  
protocol data • 223  
protocol header fields • 222  
saved traces • 234, 237  
saving trace data • 234  
TCP options • 223

### Packet Tracing Menu • 231

### panels

customizing access • 46  
data entry • 43

### panels, specific

Cisco CLAW TN3270 LU List • 140  
Confirm Stop • 233  
Connection List Criteria • 76  
Device Links List • 115  
Edit PROFILE Dataset • 121  
Formatted Packet Display • 219  
Initialization In Progress • 36  
IP Connections to a VIPA • 170  
IP Node Monitor • 98  
IP Resource Monitor • 107, 179  
Monitor Address Space Performance • 278  
Monitor Enterprise Extender Performance • 154  
Monitor Stack IP Performance History • 113  
Monitor VIPA Performance • 170  
Packet Details on the Formatted Packet Display • 221  
Packet List • 242  
Packet Trace IP Address List • 234

Packet Trace IP Connection List • 238

Resource Detail Graph • 278

Resource Summary Graph • 278

Save Trace Warnings/Errors • 234

Saved Trace List • 237

Stack IP Performance Metrics • 114

System Information • 191

Telnet • 246

Telnet Connections to a VIPA • 170

TN3270 Server Log • 140

Transaction Path Analysis • 88

User Password Change • 37

VIPA Connection Routing Table • 171

VIPA Modify Command • 171

parameters library • 118

### PARMS data set

browsing • 119  
changing • 119  
creating a new member • 119

### passwords

changing • 37

### performance

address space • 176  
CICS resource • 184  
CSM • 180  
Enterprise Extender • 154  
OSAs • 129  
problem diagnosis • 73, 80  
VIPAs • 170

### performance history • 275, 276, 278

access • 280  
baselines • 279  
monitors, from • 280, 281  
performance overviews • 282  
resource attributes • 278

### performance monitoring • 33

### performing

a ping • 193  
a traceroute • 188

### ping

connectivity • 193  
responses • 194  
routers • 192

### primary menu

profile • 35

### printers

deleting print queue entry • 261  
managing problems • 259  
querying status • 260

---

- sending test print • 261
- printing
  - reports • 298
- problem ticket
  - raising for an alert • 94
- problems
  - diagnosis • 73
  - SNA • 84
- PROFILE commands
  - menu format • 35
  - transient log • 330
- prompted fields • 44
- protocols
  - data • 223
  - header fields • 222
- PU's for a server • 139

**R**

- records
  - canceling changes • 44
  - Packet Analyzer • 359
- region, logging on • 35
- remote addresses • 62, 124
- ReportCenter • 34
- reports
  - checking print queue • 299
  - defining to TCP/IP management region • 299
  - DRDA • 229
  - offline archival system • 301
  - packet trace • 229
  - printing • 298
  - reassembled data, data flow reports • 229
- Resource Detail Graph • 278
- Resource Summary Graph • 278
- resources
  - diagnosing attributes • 278
  - TCP/IP, status • 324
  - VIPA names • 168
- response time
  - diagnosing problems • 87
  - Telnet • 87
- responses, interpreting
  - ping • 194
  - traceroute • 188
- REXX
  - programs, starting from OCS • 326
  - support • 25
- routing table • 191, 192

- Routing Table action • 192
- RTP pipes
  - define health thresholds • 150
  - display • 160
  - health • 149
  - in red status • 149

## S

- saving
  - data • 44
  - packet trace data • 226, 234
- screens
  - splitting • 49
  - swapping • 49
- scrolling • 41
- searching
  - connections • 295
  - custom • 295
  - events database • 295
  - FTP events • 295
  - Telnet connections • 295
  - Telnet display data • 249
- security
  - IP network • 185
- selecting panels
  - all panels • 45
  - by Index Menu • 45
  - by Panel Display List • 45
  - by sequence number • 45
- services
  - application development • 24
  - Broadcast Services • 23
  - communication • 24
  - MODS • 25
  - NCL • 24
  - OCS • 22
  - PSM • 23
  - report writer • 24
  - security • 23
- single select lists • 41
- SmartTrace
  - commands • 197
  - defined • 196
  - schedules • 199
- SmartTrace definitions
  - lists • 207
  - maintenance • 204, 205, 206
- SmartTrace traces

- 
- control • 205, 206
  - export • 226
  - import • 228
  - of local VIPA • 153
  - of remote CP • 152
  - of RTP pipe • 152
  - of UDP connection • 152
  - of UDP port • 153
  - packets • 208
  - reports • 229
  - saving • 226
- SNA
- analyzing sessions • 85
  - checking VTAM status of an LU • 84
  - problems • 84
- SOAP packets • 213, 218
- Socket Management
- CICS resource performance • 184
  - connections • 181
  - shutting down and restarting • 182
  - starting a CICS server • 183
  - starting a CICS transaction • 183
  - stopping and restarting command server interface • 182
- SORT command • 78, 142, 235, 238
- special characters, Telnet • 258
- SPLIT command • 48, 49
- SSL (Secure Sockets Layer)
- handshake packets • 213, 217
- stack IP performance
- history • 113
  - metrics • 114
  - traffic statistics • 114
- statistics, connections • 81
- status of resources • 324
- subordinates • 29
- subsystem traffic • 63
- support, contacting • 4
- SWAP command • 48, 49
- swapping screens • 49
- system information • 190
- System Information action • 192
- T**
- TCP
- activities • 125
  - offload information • 142
  - options • 223
- TCP/IP
- stack workload • 123
  - tracing routes • 187
- TCP/IP connections
- dropping • 86
- TCP/IP listener, displaying information • 75
- technical support, contacting • 4
- Telnet
- activity on the user log • 334
  - commands • 252
  - connecting to remote hosts • 245
  - connection details • 253
  - Connection List • 138
  - control codes • 258
  - editing display text • 248
  - ending connection • 253
  - function keys • 249
  - LUs • 175
  - printing from display • 250
  - response times • 87
  - router, to • 138
  - searching display data • 249
  - server workload • 124
  - setting options • 251
  - SNA-related problems • 84
  - special characters • 258
  - starting connections • 139, 246
- Telnet action • 192
- TELNET command • 254
- Telnet events, searching • 295
- testing connectivity • 193
- throughput
- application traffic by interfaces • 60
  - interface traffic by applications • 58
  - throughput, diagnosing • 88
- tip of the day • 47
- TLS handshake packets • 213, 217
- TN3270 server
- information • 139
  - log • 140
- tooggling between windows • 49
- trace modes • 196
- traceroute • 188
- traces
- control • 205, 232
  - export • 226, 243
  - import • 228
  - packets • 208, 234
  - saving • 226, 232, 234

---

- schedules • 199
- SmartTrace • 196
- tracing
  - IP packets in TCP/IP • 231
- Transaction Path Analyzer • 87, 88
- transient logs • 329
  - displaying an activity log • 329
  - message help • 331
  - printing • 332
  - resetting • 332
  - specifying what to display • 330

## U

- UPDATE mode, switching to • 43
- utilization, OSAs • 128

## V

- validating data • 44
- vertical scrolling • 41
- VIPA (virtual IP address) • 167
  - bytes through • 65
  - Connection Routing Table • 171
  - IP connections • 170
  - modify command • 171
  - names • 168
  - performance • 170
  - Telnet connections • 170
- VTAM
  - Display action • 84
  - EE commands • 148
  - RTP commands • 165
  - status • 84

## W

- WebCenter
  - Firefox setup • 352
  - Internet Explorer setup • 350
  - overview • 33
- WebSphere MQ traffic • 63
- working in two windows • 48
- workload
  - multiple TCP/IP stacks • 123
  - Telnet servers • 124
- Workload Manager (WLM) • 123

## X

- XCA major nodes, Enterprise Extender • 145
  - summarized information • 155