Using IPM to Measure Network Performance

This chapter provides details on using IPM to measure latency, jitter, availability, packet loss, and errors. It includes the following sections:

- Measuring Network Performance for DHCP, page 3-2
- Measuring Network Performance for DLSw, page 3-6
- Measuring Network Performance for DNS, page 3-11
- Measuring Network Performance for IP, page 3-15
- Measuring Network Performance for SNA, page 3-24
- Measuring Network Performance for TCP, page 3-28
- Measuring Network Performance for UDP, page 3-32
- Measuring Network Performance for Voice Over IP, page 3-36

Tips

You can zoom in on any of the graphs by clicking and dragging over the area of the graph that you want to enlarge. To return to the normal view, click anywhere outside the graph.
Measuring Network Performance for DHCP

The DHCP operation measures the round trip latency time taken to discover a DHCP server and obtain a lease from it. After obtaining an IP address, SAA releases the IP address that was leased by the server. By default, the DHCP operation sends discovery packets on every available IP interface on the source router. However, if a specific DHCP server is configured on the router, then discovery packets are sent to only that DHCP server. The DHCP operation also measures availability and errors for DHCP services.

To measure end-to-end performance for DHCP:

---

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** To control how statistics are collected, use the DefaultDHCP operation or define your own DHCP operation. For details on defining a DHCP operation, see the “Defining a DHCP Operation” section on page 3-3.

**Step 3** Define a collector to measure performance between the source router and the DHCP servers. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

**Step 4** (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

**Step 5** View the statistics in the DHCP Historical Statistics window. For details on viewing statistics for DHCP, see the “Viewing Statistics for DHCP” section on page 3-5.
Defining a DHCP Operation

IPM provides a default DHCP operation for measuring performance in leasing an IP address from a DHCP server. In addition, IPM provides the option from the DHCP Operation Configuration window to create, modify, or delete your own DHCP operations.

To define a DHCP operation:

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **DHCP**. The DHCP Operation Configuration window (Figure 3-1) is displayed.
Step 4  In the Name field, type a descriptive name to assign to the operation.

Step 5  (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6  Click Add. IPM adds the newly defined operation to the IPM database.

Step 7  Click Close to close the Configuration window.

For more detailed information about the options available from the DHCP Operation Configuration window, see the “DHCP Operation Configuration Window” topic in the online help.
Viewing Statistics for DHCP

The DHCP Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected DHCP collector.

To view end-to-end statistics for DHCP:

**Step 1** From the IPM Main window, select the collector.

**Step 2** Select View > Statistics. The DHCP Historical Statistics window (Figure 3-2) is displayed.

**Figure 3-2 DHCP Historical Statistics Window**
Measuring Network Performance for DLSw

DLSw+ is the enhanced Cisco version of RFC 1795. DLSw+ tunnels SNA traffic over IP backbones via TCP. The routers performing the tunneling of SNA traffic onto TCP/IP are referred to as DLSw peers.

The DLSw operation measures the DLSw+ protocol stack and round-trip latency between DLSw peers. Normally DLSw peers communicate through TCP port 2065. A prerequisite to successfully running the DLSw operation is having a connected DLSw+ peer between the source and destination Cisco devices. On the source DLSw+ device, an operation can be defined for a DLSw+ partner peer. The peer, target router, does not have to be running a version of the Cisco IOS software that supports SAA. The DLSw operation also measures availability and errors for DLSw services.

Note

To measure the round-trip latency between two DLSw peers, the IP address that you define as the source router must be one of the DLSw peers and the IP address that you define as the target router must be configured as the DLSw peer to the source router.

To measure end-to-end performance for DLSw:

Step 1 Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

Step 2 Define a device as the target of DLSw requests from the source router. For details on defining a target, see the “Defining a Target” section on page 2-9.

Step 3 To control how statistics are collected, use the DefaultDLSw operation or define your own DLSw operation. For details on defining a DLSw operation, see the “Defining a DLSw Operation” section on page 3-7.
Step 4 Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

Step 5 (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

Step 6 View the statistics in the DLSw Historical Statistics window. For details on viewing end-to-end statistics for DLSw, see the “Viewing Statistics for DLSw” section on page 3-9.

---

### Defining a DLSw Operation

IPM provides a default DLSw operation for measuring performance between a source and target. In addition, IPM provides the option from the DLSw Operation Configuration window to create, modify, or delete your own DLSw operations.

To define a DLSw operation:

---

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **DLSw**. The DLSw Operation Configuration window (Figure 3-3) is displayed.
Figure 3-3  DLSw Operation Configuration Window

Step 4  In the Name field, type a descriptive name to assign to the operation.

Step 5  (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6  In the Request Size field, type the number of bytes to use for the size of the payload of the request packet. The default setting is 64 bytes.

Step 7  In the Response Size field, type the number of bytes to use for the size of the payload of the response packet. The default setting is 64 bytes.

Step 8  Click Add. IPM adds the newly defined operation to the IPM database.

Step 9  Click Close to close the Configuration window.

For more detailed information about the options available from the DLSw Operation Configuration window, see the “DLSw Operation Configuration Window” topic in the online help.
Viewing Statistics for DLSw

The DLSw Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected DLSw collector.

To view end-to-end statistics for DLSw:

**Step 1**  From the IPM Main window, select the collector.

**Step 2**  Select View > Statistics. The DLSw Historical Statistics window (Figure 3-4) is displayed.
For more detailed information about the statistics displayed in the DLSw Historical Statistics window, see the “DLSw Historical Statistics Window” topic in the online help.
Measuring Network Performance for DNS

DNS operation latency is computed by taking the difference between the time taken to send a DNS request and receiving a reply. The operation queries for an IP address if you specify a hostname or queries for a hostname if you specify an IP address. The DNS operation also measures availability and errors for DNS services.

To measure end-to-end performance for DNS:

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** To control how statistics are collected, use the DefaultDNS operation or define your own DNS operation. For details on defining a DNS operation, see the “Defining a DNS Operation” section on page 3-12.

**Step 3** Define a collector to measure performance between the source router and DNS server. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

**Step 4** (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

**Step 5** View the statistics in the DNS Historical Statistics window. For details on viewing end-to-end statistics for DNS, see the “Viewing Statistics for DNS” section on page 3-13.
Defining a DNS Operation

IPM provides a default DNS operation for measuring performance between a source and a DNS server. In addition, IPM provides the option from the DNS Operation Configuration window to create, modify, or delete your own DNS operations.

To define a DNS operation:

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **DNS**. The DNS Operation Configuration window (Figure 3-5) is displayed.

**Figure 3-5  DNS Operation Configuration Window**
Measuring Network Performance for DNS

Step 4  In the Name field, type a descriptive name to assign to the operation.

Step 5  (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6  In the DNS Name Server field, type the hostname or IP address for the DNS name server. IPM automatically creates the DefaultDNS operation at startup based on the system `resolve.conf` file.

Step 7  In the DNS Lookup Name field, type the DNS lookup name to use in the DNS request.

Step 8  Click Add. IPM adds the newly defined operation to the IPM database.

Step 9  Click Close to close the Configuration window.

For more detailed information about the options available from the DNS Operation Configuration window, see the “DNS Operation Configuration Window” topic in the online help.

Viewing Statistics for DNS

The DNS Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected DNS collector.

To view end-to-end statistics for DNS:

Step 1  From the IPM Main window, select the collector.

Step 2  Select View > Statistics. The DNS Historical Statistics window (Figure 3-6) is displayed.
Figure 3-6  DNS Historical Statistics Window

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>95</td>
</tr>
<tr>
<td>Average Minimum</td>
<td>82</td>
</tr>
<tr>
<td>Minimum Latency</td>
<td>82</td>
</tr>
<tr>
<td>Maximum Latency</td>
<td>1,440</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total TimeOuts</td>
<td>33</td>
</tr>
<tr>
<td>Total Busy</td>
<td>0</td>
</tr>
<tr>
<td>No Connections</td>
<td>0</td>
</tr>
<tr>
<td>Total Verify Errors</td>
<td>0</td>
</tr>
</tbody>
</table>

**Completion Summary**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Attempts</td>
<td>11,417</td>
</tr>
<tr>
<td>All Completions</td>
<td>11,379</td>
</tr>
<tr>
<td>Over Threshold</td>
<td>5</td>
</tr>
<tr>
<td>Total Errors</td>
<td>33</td>
</tr>
</tbody>
</table>

For more detailed information about the statistics displayed in the DNS Historical Statistics window, see the “DNS Historical Statistics Window” section in the online help.
Chapter 3 Using IPM to Measure Network Performance

Measuring Network Performance for IP

In an IP network there are two types of measurements that you can take:

- **IP Echo**—Measures the total round-trip latency from the source router to the target device. The Cisco IOS SAA feature in the source router issues an Internet Control Message Protocol (ICMP) ping to the target device and extracts the latency data from the reply.

- **IP Path Echo**—Measures the total round-trip latency as well as the incremental latency for each hop in all paths between the source router and the target device. PathEcho is available only for the IP protocol. The Cisco IOS SAA feature first issues a `traceroute` command to determine the path through the network from the specified source router to the specified target device. The data returned from the `traceroute` command contains the host name or IP address of each of the routers in the path. SAA then issues ICMP pings to each of the routers listed in the traceroute data. The ICMP ping returns statistics regarding the latency, availability, and errors between the specified source and each of the routers.

Measuring End-to-End Performance for IP

IPM’s Echo operations measure end-to-end performance between a Cisco router and any IP-enabled device. Latency is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. The IP Echo operation also measures availability and errors for IP services.

With an IP Echo operation you can also determine performance on a specific path by using Loose Source Routing. IPM also provides an option for measuring quality of service (QoS) between endpoints by setting the type of service (ToS) bits on the IP packet.

To measure end-to-end performance for IP:

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** Define a device as the target of ICMP echo requests from the source router. For details on defining a target, see the “Defining a Target” section on page 2-9.
Step 3  To control how statistics are collected, use the DefaultIPEcho operation or define your own IP Echo operation. For details on defining an IP Echo operation, see the “Defining an IP Echo Operation” section on page 3-16.

Step 4  Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

Step 5  (Optional) If you set the collector’s schedule to On Demand, start the collector when desired.

Step 6  View the statistics in the Echo Historical Statistics window. For details on viewing end-to-end statistics for IP, see the “Viewing End-to-End Statistics for IP” section on page 3-18.

---

### Defining an IP Echo Operation

IPM provides a default IP Echo operation for measuring performance between a source and target. In addition, IPM provides the option from the Echo Operation Configuration window to create, modify, or delete your own IP Echo operations. To define an IP Echo operation:

---

Step 1  From the IPM Main window, select Edit > Configuration. The Configuration window is displayed.

Step 2  Click Operation. The Operation Configuration window is displayed within the Configuration window.

Step 3  Click Echo. The Echo Operation Configuration window (Figure 3-7) is displayed.
Figure 3-7  IP Echo Operation Configuration Window

Step 4  In the Name field, type a descriptive name to assign to the operation.

Step 5  (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6  In the Protocol field, select IP.

Step 7  In the Packet Priority field, select the priority to set for the ICMP echo request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.

Step 8  In the Request Size field, type the number of bytes to use for the size of the payload of the ICMP echo request packet. The default setting is 64 bytes.
Step 9  (Optional) To measure performance for a specific path, enable the Loose Source Routing option and add the hops for the operation to use.

Step 10  Click Add. IPM adds the newly defined operation to the IPM database.

Step 11  Click Close to close the Configuration window.

For more detailed information about the options available from the Echo Operation Configuration window, see the “Echo Operation Configuration Window” topic in the online help.

Viewing End-to-End Statistics for IP

The IP Echo Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected Echo collector.

To view end-to-end statistics for IP:

Step 1  From the IPM Main window, select the collector.

Step 2  Select View > Statistics. The Echo Historical Statistics window (Figure 3-8) is displayed.
Figure 3-8  IP Echo Historical Statistics Window

For more detailed information about the statistics displayed in the Echo Historical Statistics window, see the “Echo Historical Statistics Window” topic in the online help.
Measuring Hop-by-Hop Performance for IP

IPM’s IP Path Echo operation determines hop-by-hop performance between a Cisco router and any IP device on the network by discovering the path using traceroute and then measuring performance between the source router and each intermittent hop in the path. If there are multiple equal cost routes between the source router and the target, the Path Echo operation can identify the correct path by using Loose Source Routing, if this option is enabled on the intermediate hop devices. This feature enables SAA to discover paths more accurately compared to a regular traceroute. The IP Path Echo operation also measures availability and errors for IP services.

To measure hop-by-hop performance for IP:

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** Define a device as the target of ICMP echo requests from the source router. For details on defining a target, see the “Defining a Target” section on page 2-9.

**Step 3** To control how statistics are collected, use the DefaultIpPathEcho operation or define your own IP Path Echo operation. For details on defining an IP Path Echo operation, see the “Defining an IP Echo Operation” section on page 3-16.

**Step 4** Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

**Step 5** (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

**Step 6** View the statistics in the Path Echo Historical Statistics window. For details on viewing hop-by-hop statistics for IP, see the “Viewing Hop-by-Hop Statistics for IP” section on page 3-23.
Defining an IP Path Echo Operation

IPM provides a default IP Path Echo operation for measuring performance between a source and target. In addition, IPM provides the option from the Path Echo Operation Configuration window to create, modify, or delete your own IP Path Echo operations.

To define an IP Path Echo operation:

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **Path Echo**. The Path Echo Operation Configuration window (Figure 3-9) is displayed.

---

**Figure 3-9  IP Path Echo Operation Configuration Window**

![IP Path Echo Operation Configuration Window]
Step 4 In the Name field, type a descriptive name to assign to the operation.

Step 5 (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6 In the Packet Priority field, select the priority to set for the ICMP echo request packet. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.

Step 7 In the Request Size field, type the number of bytes to use for the size of the payload of the ICMP echo request packet. The default setting is 64 bytes.

Step 8 To specify the maximum number of paths to discover, type a value in the Maximum Paths field. The default setting is 5. To ensure that you do not miss collecting statistics for relevant paths, set this value to a number slightly higher than the expected number of paths.

Step 9 To specify the maximum number of hops to discover, type a value in the Maximum Hops field. The default setting is 28. To ensure that you do not miss collecting statistics for relevant hops, set this value to a number slightly higher than the expected number of hops.

Step 10 Click Add. IPM adds the newly defined operation to the IPM database.

Step 11 Click Close to close the Configuration window.

Note The sample interval must be greater than the timeout value multiplied by the number of hops.

---

For more detailed information about the options available from the Path Echo Operation Configuration window, see the “Path Echo Operation Configuration Window” topic in the online help.
Viewing Hop-by-Hop Statistics for IP

The IP Path Echo Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected Path Echo collector.

To view hop-by-hop statistics for IP:

Step 1. From the IPM Main window, select the collector.
Step 2. Select View > Statistics. The Path Echo Historical Statistics window (Figure 3-10) is displayed.

**Figure 3-10  IP Path Echo Historical Statistics Window**

To view the list of hops for a path, click on the path folder. To view the graphs for a specific path or a specific hop, click on the path or hop.
Measuring Network Performance for SNA

For SNA environments, IPM allows you to measure the round-trip latency to an MVS mainframe using the following types of SNA sessions:

- System services control point-logical unit (SSCP-LU)
- LU 0
- LU 2

Because SNA is a connection-oriented protocol, the only type of measurement you can request is Echo.

When measuring latency to an SNA mainframe, IPM measures round-trip latency between a source router and an echo program in an SNA mainframe. A program in the SNA mainframe is responsible for providing the echo back to the router. IPM provides a mainframe echo program (NSPECHO) that you can install on an MVS mainframe for this purpose. You can customize both the request and response sizes to model traffic flow for various applications. The SNA operations also measure availability and errors for SNA services.

To measure end-to-end performance for SNA:

Step 1: Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

Step 2: Define a device as the target of SNA pings from the source router. For details on defining a target, see the “Defining a Target” section on page 2-9.

Step 3: To control how statistics are collected, use one of the default SNA operations or define your own SNA Echo operation. For details on defining an SNA Echo operation, see the “Defining an SNA Echo Operation” section on page 3-25.

Step 4: Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.
Step 5  (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

Step 6  View the statistics in the Echo Historical Statistics window. For details on viewing end-to-end statistics for SNA, see the “Viewing Statistics for SNA” section on page 3-26.

---

### Defining an SNA Echo Operation

The SNA Echo Operation Configuration window allows you to create, modify, or delete an SNA Echo operation.

To define an SNA Echo operation:

**Step 1**  From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2**  Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3**  Click **Echo**. The Echo Operation Configuration window (Figure 3-7) is displayed.

**Step 4**  In the Name field, type a descriptive name to assign to the operation.

**Step 5**  (Optional) In the Description field, type a brief description of the operation, including its purpose.

**Step 6**  In the Protocol field, select one of the following protocols:

- SNA LU 0
- SNA LU 2
- SNA SSCP

**Step 7**  In the Request Size field, type the number of bytes to use for the size of the payload of the request packet. The default setting is 64 bytes.

**Step 8**  In the Response Size field, type the number of bytes to use for the size of the payload of the response packet. The default setting is 64 bytes.

**Step 9**  (Optional) To check for connection loss, click **Enable Connection Lost Action**.


**Chapter 3 Using IPM to Measure Network Performance**

**Measuring Network Performance for SNA**

*Step 10*  (Optional) To increment the Verify Data counter whenever a response contains unexpected data, click **Enable Data Verification**.

*Step 11*  Click **Add**. IPM adds the newly defined operation to the IPM database.

*Step 12*  Click **Close** to close the Configuration window.

For more detailed information about the options available from the Echo Operation Configuration window, see the “Echo Operation Configuration Window” topic in the online help.

**Viewing Statistics for SNA**

The SNA Echo Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected Echo collector.

To view end-to-end statistics for SNA:

*Step 1*  From the IPM Main window, select the collector.

*Step 2*  Select **View > Statistics**. The SNA Echo Historical Statistics window (Figure 3-11) is displayed.
Figure 3-11  SNA Echo Historical Statistics Window

For more detailed information about the statistics displayed in the Echo Historical Statistics window, see the “Echo Historical Statistics Window” topic in the online help.
Measuring Network Performance for TCP

IPM’s TCP Connect operation measures round-trip latency between a Cisco router and any IP-enabled device running TCP services. Latency is computed by measuring the time taken by the source to perform a TCP connect operation to the target device. If the target is a Cisco router running a version of the Cisco IOS software that supports the SAA feature, then you can communicate with the SAA responder (which is capable of responding on any defined port) or using a well-known port. If the target is not a Cisco router, then you must use a well-known port number. This operation is useful for simulating Telnet or HTTP connection times. Some well known ports are: 21 for FTP, 23 for Telnet, and 80 for HTTP server. IPM also provides default TCP Connection operations for several of these common TCP services. The TCP operation also measures availability and errors for TCP services.

To measure end-to-end latency for TCP:

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** Define a device as the target of connection requests from the source router. For details on defining a target, see the “Defining a Target” section on page 2-9.

**Step 3** To control how statistics are collected, use one of the default operations for TCP or define your own TCP operation. For details on defining a TCP operation, see the “Defining a TCP Operation” section on page 3-29.

**Step 4** Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

**Step 5** (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

**Step 6** View the statistics in the TCP Historical Statistics window. For details on viewing end-to-end statistics for TCP, see the “Viewing Statistics for TCP” section on page 3-30.
Defining a TCP Operation

IPM provides several default TCP operations for measuring performance between a source and target. In addition, IPM provides the option from the TCP Operation Configuration window to create, modify, or delete your own TCP operations.

To define a TCP operation:

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **TCP**. The TCP Operation Configuration window (Figure 3-12) is displayed.

**Figure 3-12 TCP Operation Configuration Window**
Measuring Network Performance for TCP

**Step 4**  In the Name field, type a descriptive name to assign to the operation.

**Step 5**  (Optional) In the Description field, type a brief description of the operation, including its purpose.

**Step 6**  In the Packet Priority field, select the priority to set for the TCP connection request. The default setting is 0 (no priority). This option sets the ToS bits in the IP packet.

**Step 7**  In the Target Port field, type the TCP port number for the target device to use when sending a response to a connection request.

**Step 8**  Click **Add**. IPM adds the newly defined operation to the IPM database.

**Step 9**  Click **Close** to close the Configuration window.

For more detailed information about the options available from the TCP Operation Configuration window, see the “TCP Operation Configuration Window” topic in the online help.

**Viewing Statistics for TCP**

The TCP Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected TCP collector.

To view end-to-end statistics for TCP:

**Step 1**  From the IPM Main window, select the collector.

**Step 2**  Select **View > Statistics**. The TCP Historical Statistics window (Figure 3-13) is displayed.
Figure 3-13  TCP Historical Statistics Window

For more detailed information about the statistics displayed in the TCP Historical Statistics window, see the “TCP Historical Statistics Window” topic in the online help.
Measuring Network Performance for UDP

IPM’s UDP operation measures round-trip latency between a Cisco router and any IP-enabled device running UDP services. Latency is computed by measuring the time taken to send a datagram and receive a response from the target device. If the target is a Cisco router running a version of the Cisco IOS software that supports the SAA feature, then you can communicate with the SAA responder (which is capable of responding on any defined port). If the target is not a SAA router, then you must use UDP port 7 as the target port. The UDP operation also measures availability and errors for UDP services.

To measure end-to-end performance for UDP:

---

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** To control how statistics are collected, use the DefaultUDP operation or define your own UDP operation. For details on defining a UDP operation, see the “Defining a Target” section on page 2-9.

**Step 3** Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.

**Step 4** (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

**Step 5** View the statistics in the UDP Historical Statistics window. For details on viewing end-to-end statistics for UDP, see the “Viewing Statistics for UDP” section on page 3-34.
Defining a UDP Operation

IPM provides a default UDP operation for measuring performance between a source and target. In addition, IPM provides the option from the UDP Operation Configuration window to create, modify, or delete your own UDP operations.

To define a UDP operation:

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **UDP**. The UDP Operation Configuration window (Figure 3-14) is displayed.

*Figure 3-14 UDP Operation Configuration Window*
Chapter 3 Using IPM to Measure Network Performance

Measuring Network Performance for UDP

Step 4 In the Name field, type a descriptive name to assign to the operation.

Step 5 (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6 In the Packet Priority field, select the priority to set for the request packet. The default setting is 0 (no priority).

Step 7 In the Request Size field, type the number of bytes to use for the size of the payload of the request packet. The default setting is 64 bytes.

Step 8 In the Target Port field, type the UDP port number for the target device to use when sending response packets. The default setting is 7.

Step 9 Click Add. IPM adds the newly defined operation to the IPM database.

Step 10 Click Close to close the Configuration window.

For more detailed information about the options available from the UDP Operation Configuration window, see the “UDP Operation Configuration Window” topic in the online help.

Viewing Statistics for UDP

The UDP Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected UDP collector.

To view end-to-end statistics for UDP:

Step 1 From the IPM Main window, select the collector.

Step 2 Select View > Statistics. The UDP Historical Statistics window (Figure 3-15) is displayed.
Figure 3-15  UDP Historical Statistics Window

For more detailed information about the statistics displayed in the UDP Historical Statistics window, see the “UDP Historical Statistics Window” topic in the online help.
Measuring Network Performance for Voice Over IP

The Enhanced UDP operation for Voice over IP measures round-trip latency, packet loss, and jitter in IP networks by generating synthetic UDP traffic. The Enhanced UDP operation sends a defined number of packets of a defined size from the source router to a target router with a defined interpacket delay. Both the source router and the target must be running Cisco IOS software that supports SAA and the SAA responder must be enabled on the target. To enable the SAA responder on the target, use the `rtr responder` IOS configuration command. The packets that are sent out to measure jitter contain packet sequence information as well as sending and receiving timestamps from the source and the responder.

The Enhanced UDP operation measures the following network performance statistics:

- round-trip network latency
- per-direction packet loss
- per-direction interpacket delay variance (jitter)
- network availability and errors

To measure end-to-end performance for Enhanced UDP:

---

**Step 1** Define a router as the source router from which to measure performance. For details on defining a source router, see the “Defining a Source Router” section on page 2-7.

**Step 2** Define a device as the target of discovery requests from the source router. For details on defining a target, see the “Defining a Target” section on page 2-9.

**Step 3** To control how statistics are collected, use one of the default Enhanced UDP operations or define your own Enhanced UDP operation. For details on defining a Enhanced UDP operation, see the “Defining an Enhanced UDP Operation” section on page 3-37.

**Step 4** Define a collector to measure performance between the source router and target that you have defined. For details on defining a collector, see the “Defining a Collector” section on page 2-12.
**Step 5** (Optional) If you set the collector’s schedule to **On Demand**, start the collector when desired.

**Step 6** View the statistics in the Enhanced UDP Historical Statistics window. For details on viewing end-to-end statistics for Enhanced UDP, see the “Viewing Statistics for Enhanced UDP” section on page 3-39.

---

**Defining an Enhanced UDP Operation**

IPM provides several default Enhanced UDP operations for measuring performance between a source and target. In addition, IPM provides the option from the Enhanced UDP Operation Configuration window to create, modify, or delete your own Enhanced UDP operations.

To define an Enhanced UDP operation:

**Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window is displayed.

**Step 2** Click **Operation**. The Operation Configuration window is displayed within the Configuration window.

**Step 3** Click **Enhanced UDP**. The Enhanced UDP Operation Configuration window (Figure 3-16) is displayed.
Figure 3-16  Enhanced UDP Operation Configuration Window

Step 4  In the Name field, type a descriptive name to assign to the operation.

Step 5  (Optional) In the Description field, type a brief description of the operation, including its purpose.

Step 6  In the Packet Priority field, select the priority to set for the UDP request packet. The default setting is 0 (no priority). For the DefaultVoice operations, the default packet priority setting is 5.

Step 7  In the Request Size field, type the number of bytes to use for the size of the payload of the UDP request packet. The default setting is 64 bytes.

Step 8  In the Packet Interval field, type the number of milliseconds to use for the interpacket delay between packets that are sent from the source router to the target router. The default setting is 20 ms.

Step 9  In the Number of Packets field, type the number of packets to send to the target to measure latency. The default setting is 10 packets.
Step 10 In the Target Port field, type the UDP port number for the target device to use when sending a response packet. The default setting is 16400 for Voice and 2000 for other traffic.

Step 11 Click Add. IPM adds the newly defined operation to the IPM database.

Step 12 Click Close to close the Configuration window.

For more detailed information about the options available from the Enhanced UDP Operation Configuration window, see the “Enhanced UDP Operation Configuration Window” topic in the online help.

Viewing Statistics for Enhanced UDP

The Enhanced UDP Historical Statistics window displays statistical and graphical information gathered over the monitoring period for the selected Enhanced UDP collector.

To view statistics for Enhanced UDP:

Step 1 From the IPM Main window, select the collector.

Step 2 Select View > Statistics. The Enhanced UDP Historical Statistics window (Figure 3-17 and Figure 3-18) is displayed.
Figure 3-17 Enhanced UDP Historical Statistics Window—Part 1
Figure 3-18  Enhanced UDP Historical Statistics Window—Part 2

For more detailed information about the statistics displayed in the Enhanced UDP Historical Statistics window, see the “Enhanced UDP Historical Statistics Window” topic in the online help.