CHAPTER 12

Network Tree View

This section provides a description of the network tree view available in the Network Manager. Topics in this section include:

About the Network Tree View

The Network Tree view organizes the information about the IP conferencing network into one or more tabbed views, each of which lists the elements in the network in a tree structure. By default, the tree divides the elements by zones.

Topics in this section include:

Managing Zones

The Network Tree displays the network according to zones which are defined by gatekeepers. There is a zone node in the tree for each gatekeeper in the network, or pair of gatekeepers where an alternate gatekeeper is used. Each zone includes a gatekeeper element with which the zone is defined and other elements such as MCUs and gateways which are registered in that zone. An element can be managed, unmanaged or inferred. A zone is not an element that can be managed.

Elements

- Managed—The element exists in the Network Manager database and provides monitoring information and access to configuration settings.
- Inferred—The element does not exist in the Network Manager database, but may appear as an inferred element because a managed element refers to that element.

For example, a gatekeeper is inferred when a managed element is registered to that gatekeeper zone, but the gatekeeper is not managed by the Network Manager.

- Unmanaged—The element exists in the Network Manager database but has no open communication channels with the Network Manager and provides no monitoring information or access to configuration settings.

An element may be unmanaged when the Network Manager license limitations have been exceeded or when the user manually sets the element as unmanaged.

Zones

Gatekeeper zones can be managed in a hierarchical structure with parents, neighbors and children. This hierarchical structure is reflected in the Network Tree view and can be arranged using the Network Manager drag and drop capabilities.

A zone cannot be deleted manually from the tree but is automatically deleted in one of the following circumstances:

- A managed gatekeeper in the zone is deleted from the tree.
- The gatekeeper is inferred and the last remaining managed element in the zone is deleted from the tree.

Dragging and Dropping

The drag and drop feature enables quick configuration of the network hierarchy and automatically reconfigures element relationships by automatically assigning and updating the appropriate details of the elements with which the managed element registers.

The following element relationships can be configured using the drag and drop feature:

- Gatekeeper Parent - Child
- Gatekeeper - MCU/Gateway
- MCU - MP

Gatekeeper parent and child element tables are updated for each element in the relationship. MCU and gateway elements are updated with the appropriate gatekeeper IP address. MP elements are updated with the relevant IP address and configuration details for registering with the MCU.

Using The Network Tree Interface

The Network Tree view enables you to select an element in the tree to display specific information, such as alarms, traps and services related to the element. In addition to the default view where elements are divided into zones, custom views can be added to organize the elements according to criteria you define, such as location or customer use. Folders can be added to the custom views and the elements can be organized in these folders, as required. For more information, see Chapter 18, "Finding and Managing Elements".

The Network Tree contains one default tab—the Network tab—which displays the network root, the zones into which the network is divided and the elements contained in each zone. The tree can be expanded and collapsed, as required. Each element type is represented by a different icon, and the current status of the element is superimposed on that icon.

Controlling an Element

The Network Map view contains five buttons which allow you to perform the following:

- Add element
- Edit element
- Delete element
- Find element
- Auto-detect elements

For more information about these actions, see Chapter 18, "Finding and Managing Elements".

Note These buttons are also available in the Network Table view and the Network Map view.

Perform auto-detect in the Network Tree view, which enables you to search the network for new or modified elements and add them to the Network Manager database.

When you select an element (or endpoint) in the tree, the main display area changes to display the relevant tabs. Some of the tabs are common to the different elements types, while others are unique to a particular element type. The main display area also contains the Network Tree buttons, which are described in the following section.

Using Network Tree Buttons

Selected tabs in the Network Tree view also include the following buttons:

- Upload—On all tabs where you can enter information directly into a field, to update the information in the database, click **Upload**.
- Refresh—To download updated information from the database, click **Refresh**.

Note To enable information about two elements in the tree to be displayed simultaneously, click the pin button at the top of any tab.

Using Network Tree Tabs

Selecting items in the Network Tree displays one or more tabs on the right-hand side of the main display area. Network Tree tabs provide a variety of information about the selected item, such as its current status and alarms, the services configured for the item, and any special access information. In addition, configure the most commonly used parameters of each element type.

Displaying General Information

The Monitor tab, which is the default tab displayed when an item is selected in the Network Tree view, displays general information about the item.

Note When the gatekeeper in a zone is unmanaged or inferred, the calls, bandwidth and registration information appears as zero.

The information displayed on the Monitor tab is dependent on the item selected in the tree.

At the network and zone level, the tab displays the following information:

- Display name—Name of the selected zone or element
- Status
- Number of elements
- Calls
- Point-to-point calls
- Number of conferences
- Number of endpoints registered in the network
- Number of B channels
- Bandwidth information—Inter-zone, intra-zone, available bandwidth

At the element level, the Monitor tab displays the name of the element, the IP address, the version number and its current online status. In addition, the tab includes information relevant to the type of element selected. For example, when an MCU is selected in the tree, the Monitor tab includes the current alarm status, the current number of conferences, and so on.

Note To display the element manager for the selected element, click the link.

Displaying Elements

The Elements tab displays a table of all elements related to the network, zone or folder selected in the tree.

The table in the Elements tab includes the following information about each element:

- Element status, indicated by an icon, as follows:
  - Online
  - Unmanaged

Offline

Faulty

- Element type (MCU, gatekeeper and so on)
- Element name (acts as a link to its element manager)
- IP address
- Version number
- Location (as defined on the Configure tab of each element)
- Number of calls
- Traffic usage versus capacity

Any element listed in the tree with a question mark (?) is considered to be an inferred element by the system. This means that the element is not listed in the database, but is presumed to exist because another known element refers to the element. Inferred elements cannot be managed, therefore we recommend that you either initiate auto-detect to discover an element, add an element manually or manually connect an inferred element.

Adding an Element

To manually add an element to the network, zone or folder selected in the tree, use the following procedure:

Procedure

Step 1 Click **Add**.

Step 2 Enter a display name and the IP address.

Step 3 Select an element type and indicate whether the element is managed and configurable offline.

Step 4 To add the element to the network tree, click **OK**.

In addition, modify, remove and find existing elements.

For more information, see Chapter 18, “Finding and Managing Elements”.

Displaying Alarms

The Alarms tab displays a table of all current alarms related to the item selected in the tree. Alarms can be viewed per element, zone or the entire network in one view.

The Alarms tab includes the severity of each alarm, the time the event occurred and the alarm message that is related to the selected element. Alarm severity levels include the following:

Major/Minor/Critical

Information

Warning

To access the relevant element managers, click the link in the right-hand column. For more information, see Chapter 15, “Alarms View”.

Displaying Events

The Events tab displays a table of the events that have occurred in the system, which are related to the item selected in the tree.

The Events tab includes the event severity level, the date and time of the event and the event message.

To access the relevant element managers, click the link in the Element column.

To display the Filter Traps window, which enables you to filter the events displayed in the tab by date and severity level, click the link above the table.

For more information, see Chapter 15, "Alarms View".

Displaying Conferences

The Conferences tab provides a table for viewing the current status of all conferences being hosted on the network, zone or selected MCU.

The table includes the following information:

- MCU—IP address of the MCU on the which the conference is being hosted. Click on the link to view the element manager of the MCU (Administrator).
- Conference ID—Conference ID number. Click on the link to view the conference manager of the MCU (Conference Control).
- Layout icon—Video layout configuration of the conference.
- Camera icon—Indicates whether video is enabled for the conference.
- Speaker icon—Indicates whether audio is enabled for the conference.
- Data icon—Indicates whether data support is enabled for the conference.
- Total Participants—Number of current participants.
- Reserved Participants—Number of reserved participants.
- Video Bit Rate—Maximum bit rate for the conference.
- Zone—Zone in which the conference is taking place.

To display the Find Conference window, which enables you to locate a particular conference in the table, click **Find** above the table. For more information about the fields displayed on the Conferences tab, see Chapter 17, "Conferences and Calls View".

Note Access the element manager of the MCU (Administrator) by clicking the link in the left hand column of each table row.

Finding a Conference

To locate a particular conference in the table, use the following procedure:

Procedure

Step 1 Click **Find**.

Step 2 Enter the conference ID or the zone prefix and click **Find**.

The row in the table matching your search criteria is highlighted.

Note Use the asterisk [*] wildcard when searching for conferences.

Displaying Calls

The Calls tab displays a table providing details of each call currently taking place on the selected element including the source and destination aliases and gatekeepers of the calling parties, call start time and allocated bandwidth.

The Calls tab allows you to disconnect calls either for each selected call or globally for all calls. Extended calls can be displayed by clicking on the table row and a call search option allows you to search by alias, IP address of the endpoint, service or conference ID.

Displaying a Configuration

The Configure tab displays the most commonly needed configuration parameters for the element selected in the tree.

The information displayed on the Configure tab is dependent on the type of element selected in the tree including the following:

- Configuring an MCU, page 12-7
- Configuring a Gateway, page 12-8
- Configuring a Cisco IOS H.323 Gatekeeper, page 12-8

Note When a network or a zone is selected in the tree, the Configure tab is not available.

Configuring an MCU

The MCU Configure tab enables you to set the unit type and configure addressing details.

Configure the parameters on the Configure tab of an MCU as follows:

- Unit Type:
  - MCU—The MCU and MP components in the unit work together to provide Call Setup, conference control and media processing.
  - MP Only—The MP (Multipoint Processor) unit works in a clustered arrangement operating under the control of an MCU.
- Location—Enter a string identifying the physical location of the MCU device.
- MCU IP Address—MCU IP address. Configurable only on MP units.
- Port—MCU communication port. Configurable only on MP units.

Configuring a Gateway

Configure the parameters on the Configure tab of a gateway, as follows:

- The IP address of the gatekeeper which the gateway registers
- A string identifying the physical location of the gateway.

Configuring a Cisco IOS H.323 Gatekeeper

Configure the parameters on the Configure tab of a Cisco IOS H.323 Gatekeeper, as follows:

- Gatekeeper enabled (no shutdown)—When selected, enables the Cisco IOS H.323 Gatekeeper.
- GKTMP port—The port via which the Network Manager communicates with the Cisco IOS H.323 Gatekeeper using the GKTMP communication protocol to get calls and registration information from the Cisco IOS H.323 Gatekeeper.

Displaying Logs

The Logs tab enables the Network Manager to keep a log of operations for the element selected in the tree.

Note A log of operations is not available for endpoints supported by the Network Manager. A log tab is not available for endpoints when selected in the Network Tree view.

The information displayed on the Logs tab is dependent on the type of element that is selected in the tree.

Define the log for the various elements, as follows:

- Internal Gatekeeper—Check **Save logs** and select the level of detail to include in the log.
- MCU—Check **Save logs**, type the log file name and define the level of detail to include in the log.
- Gateway—Check **Save logs**, type the log file name and define the level of detail to include in the log.
- Cisco IOS H.323 Gatekeeper—Check **Save logs**, type the log file name and define the level of detail to include in the log.

Note In addition, to view the logs directory from any of the Log tabs described above, click the link. For more information on log parameters, see Chapter 16, “Settings View”.

Configuring SNMP Access

The Access tab allows you to define custom SNMP access settings for the currently selected element. Custom settings differ from the default settings configured for elements of this type on the Element Access tab of the Settings view.

Access settings allow access to element managers without having to first go through the Login windows for each element. For more information about access settings, see Chapter 16, “Settings View”.

Configure the parameters on the Access tab, as follows:

Procedure

Step 1 Check **Use default** to use the default access settings for the element type. When unchecked, all other tab options are disabled. Availability of the following access configuration parameters depends on the element type selected.

Step 2 The Element type list appears when the selected element is an inferred gatekeeper. Select to display the appropriate access configuration parameters for the inferred gatekeeper.

Step 3 Click **Connect** to connect to an inferred element and add it to the Network Manager database. The access parameters of the element must be correctly configured for the operation to succeed.

Step 4 Configure the following parameters:

- SNMP read community
- SNMP write community
- User name
- Password
- HTTP port
- Telnet password (MCU, Cisco IOS H.323 Gatekeeper)
- Telnet user name (Cisco IOS H.323 Gatekeeper only)
- Enable Telnet (Cisco IOS H.323 Gatekeeper only)

Caution The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed.

Tip View SNMP Community names by selecting the View SNMP Community names option in the View menu, if the option is already enabled using the Configuration Utility.

Configuring the Internal Gatekeeper

When Internal Gatekeeper is selected in the tree, additional tabs are displayed, which enable you to define the manage services, define subzones, control bandwidth and configure parent, neighbor and child gatekeepers, including the following:

- Displaying Services, page 12-9
- Configuring a Parent, page 12-10
- Configuring Children, page 12-12
- Configuring a Neighbor, page 12-13

Displaying Services

The Services tab displays the list of predefined and online services supported by the Internal Gatekeeper selected in the tree.

The Global Services tab displays the list of global services which can be configured for the selected Internal Gatekeeper.

The Services tab displays the following information:

- Prefix used to access the service
- Service description
- Whether the service is predefined or online (meaning, service status)
- Whether conference hunting is enabled for the service
- Default policy for in-zone endpoints
- Service policy for out-of-zone endpoints

Adding a Service

To configure new services supported by the selected Internal Gatekeeper, use the following procedure:

Procedure

Step 1 To display the Add Service window, click **Add**.

Step 2 Type the prefix used to access the service.

Step 3 Select the service type (Phone number, Name, URL address, E-mail address).

Step 4 Type a description of the service.

Step 5 Select whether to enable conference hunting.

Step 6 Select whether to allow access to in-zone endpoints.

Step 7 Select whether to allow access to out-of-zone endpoints.

Step 8 Click **OK**.

The new service is added to the displayed list.

Note To modify and delete existing services, use the Edit and Delete buttons.

Configuring a Parent

The Parent tab enables you to configure a parent gatekeeper for the Internal Gatekeeper, to define a list of parent filters and to choose whether or not to route calls to unresolved zones via the Cisco Proxy.

Note The parent gatekeeper can also be configured automatically using the Network Manager Drag and Drop feature. In the Network Tree, drag and drop the Internal Gatekeeper element into the zone of the gatekeeper you wish to configure as the parent gatekeeper. The Internal Gatekeeper Parent tab is automatically updated with the parent gatekeeper details.

About Parent Filters

The Internal Gatekeeper sends an LRQ to the parent gatekeeper when the zone prefix of the call matches one of the defined parent filters. If the Internal Gatekeeper fails to match the zone prefix of the call with any of the defined parent filters, the Internal Gatekeeper either rejects the call or forwards the call according to the Call Fallback settings configured in the Internal Gatekeeper element manager. Where no filters are defined, the Internal Gatekeeper passes the call to the parent gatekeeper. The Internal Gatekeeper allows a maximum of ten parent filters.

Configure the parameters on the Parent tab, as follows:

- Enable—When checked, enables you to add a parent gatekeeper to the Internal Gatekeeper.
- IP Address—Enter the IP address of the parent gatekeeper.
- Port—Enter the port number of the parent gatekeeper.
- Description—Enter a description of the parent gatekeeper.
- Parent Filters—Displays the list of defined parent filters.
- Add—To add a new parent filter to the Internal Gatekeeper database, click **Add**.
- Edit—To modify an existing parent filter, double-click a parent filter from the list or select a parent filter from the list and click **Edit**.
- Delete—To remove the specified parent filter from the list, select a parent filter from the list and click **Delete**.

Note The parent tab is enabled when the Internal Gatekeeper is configured to support Dial Plan Version 2.0 and Use Central Database is deselected on the Configure tab of the selected Internal Gatekeeper. The Parent tab is not available in Internal Gatekeeper v1.0.

Adding a Parent Filter

To add a parent filter, use the following procedure:

Procedure

Step 1 To open the Add Filter window, click **Add**,

-or-

Double-click the relevant parent filter from the list or select a parent filter from the list and click **Edit**.

Step 2 Enter or modify the prefix that identifies the filter in the **Filter** parameter.

Step 3 Click **OK** to add the new parent filter information to the Internal Gatekeeper database.

Note To modify and delete existing filters, use the Edit and Delete buttons.

Configuring Children

The Children tab enables you to view, configure and modify child gatekeepers of the Internal Gatekeeper.

Note To automatically configure a child gatekeeper, use the Network Manager Drag and Drop feature. In the Network Tree, drag and drop the Internal Gatekeeper element you wish to configure as the child gatekeeper into the zone of the current Internal Gatekeeper. The Children tab of the parent Internal Gatekeeper is automatically updated with the child gatekeeper details.

The Children tab displays the following information:

- Description—Displays the child gatekeeper description in free text. This field appears when the Use Central Database option is unchecked in the Configure tab.
- Prefixes—Displays the zone prefix.
- IP Address—Displays the IP address of the child gatekeeper.
- Port—Displays the port number of the child gatekeeper.
- Proxy—Indicates whether or not the Internal Gatekeeper routes calls from this zone to the neighbor gatekeeper through the Cisco Proxy.
- Central Database—Indicates whether or not the child gatekeeper was retrieved from the central database.

Note Where available, the Parent tab is enabled when the Internal Gatekeeper is configured to support Dial Plan Version 2.0 and Use Central Database is deselected on the Configure tab of the selected Internal Gatekeeper. The Parent tab is not available in Internal Gatekeeper v1.0.

Adding a Child

To add a child gatekeeper, use the following procedure:

Procedure

Step 1 Click **Add**.

-or-

Double-click the relevant child gatekeeper on the Children tab or select a child gatekeeper and click **Edit**.

Step 2 Configure the parameters in the Add Child or Edit Child window, as follows:

- IP Address—Enter or modify the IP address of the child gatekeeper.
- Port—Enter or modify the port number of the child gatekeeper.
- Description—Enter or modify the description of the child gatekeeper.
- Use Cisco Proxy—Select to indicate whether or not the Internal Gatekeeper should route calls from this zone to the neighbor gatekeeper through the Cisco Proxy.

– Prefixes—Displays the list of defined child prefixes. The Internal Gatekeeper sends an LRQ to the child gatekeeper when the zone prefix of the call matches one of the defined child prefixes. If the Internal Gatekeeper fails to match the zone prefix of the call with any of the defined child gatekeeper prefixes, the Internal Gatekeeper passes the call to a neighbor gatekeeper.

Step 3 Click **OK** to add the child gatekeeper to the Internal Gatekeeper database.

Note The Add, Edit and Delete options are disabled when you check Use Central Database on the Configure tab.

Adding or Modifying a Child Prefix

To add or modify a child prefix, use the following procedure:

Procedure

Step 1 To open the Add Prefix window, click **Add**.

-or-

Double-click the relevant child prefix from the list or select a child prefix from the list and click **Edit**.

Step 2 Type or modify the child prefix in the **Prefix** parameter.

Step 3 Click **OK** to add the new child prefix to the Internal Gatekeeper database.

Note To modify and delete existing child gatekeeper prefixes, use the Edit and Delete buttons.

Configuring a Neighbor

The Neighbors tab enables you to view, configure and modify neighbor gatekeepers of the Internal Gatekeeper for resolving destination IP addresses when the source endpoint is not in the same zone as the destination endpoint.

The Neighbors tab displays the following information:

- Description—Displays the neighbor gatekeeper description.
- Prefix—Displays the zone prefix.
- ID Address—Displays the neighbor gatekeeper IP address.
- Port—Displays the port number of the neighbor gatekeeper.
- Proxy—Indicates whether or not the Internal Gatekeeper routes all calls from this zone to the neighbor gatekeeper through the Cisco Proxy.
- GK ID—Displays the neighbor gatekeeper identifier.
- Central DB—Indicates whether or not the neighbor gatekeeper was retrieved from the central database.
- LDAP—Indicates whether or not the neighbor gatekeeper was retrieved from the LDAP server.

Adding a Neighbor

To add a neighbor gatekeeper, use the following procedure:

Procedure

Step 1 To open the Add Neighbor window, click **Add**.

-or-

Double-click the relevant neighbor gatekeeper from the list or select a neighbor gatekeeper from the list and click **Edit**.

Step 2 Configure the following parameters:

- Prefix—Enter or modify the neighbor gatekeeper zone prefix.
- Description—Type or modify the description of the neighbor gatekeeper.
- IP Address—Type or modify the IP address of the neighbor gatekeeper.
- Port—Type or modify the port number of the neighbor gatekeeper.
- Use Cisco proxy—Check to instruct the Internal Gatekeeper to route all calls from this zone to the neighbor gatekeeper through the Cisco Proxy.

Step 3 Click **OK** to add the new neighbor gatekeeper information to the Internal Gatekeeper database.

Note The Add, Edit and Delete buttons are disabled when you check Use Central Database on the Configure tab.

Configuring Endpoints

The Endpoints tab displays endpoint information for the zone and allows you to manage endpoint access, addressing and dialing.

The Endpoints tab displays the following buttons:

- Configure—see the "Controlling an Endpoint" section on page 12-14

The Endpoints tab displays for each endpoint the following information:

- IP address
- Name
- Number

Controlling an Endpoint

You manage an endpoint by selecting the endpoint and clicking Configure to open the Endpoint Control window. Alternatively, double-click the relevant endpoint row in the list. The window enables you to modify endpoint configuration and access parameters and to dial to other endpoints on the network.

If the endpoint type is not configured, the Access tab displays. You select from a range of endpoint types recognized by the Network Manager and provide security details as required in order to manage the endpoint.

The Endpoint Control window includes the following tabs:

- Configuring Endpoint Control
- Configuring Access Settings
- Configuring Dialing

Configuring Endpoint Control

The Configure tab of the Endpoint Control window allows you to modify the endpoint gatekeeper addressing, E.164 number and alias.

Procedure

Step 1 Configure the Configure tab as follows:

- Gatekeeper IP—Select a gatekeeper IP address from the list of gatekeepers available on the network.
- Enter an E.164 number for the endpoint.
- Enter an H.323 alias for the endpoint.

Step 2 Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.

Configuring Access Settings

The Access tab of the Endpoint Control window allows you to view and configure the access settings that enable the Network Manager to manage the endpoint.

Procedure

Step 1 Configure the Access tab as follows:

- Endpoint Type—Select an endpoint from the list of supported endpoints.
- Use default access—Check to use default access settings defined by the endpoint. When unchecked, Remote API port and Telnet prompt for Tandberg endpoints only can be modified.
- Remote API port—The endpoint API port. Editable for Tandberg endpoints only.
- Telnet prompt—The Telnet prompt character string. Editable for Tandberg endpoints only.
- User name—The user name required for communicating with the endpoint.
- Password—The password required for communicating with the endpoint.

Step 2 To add the new settings to the endpoint, click **Upload** or to update the new settings, click **Refresh**.

Configuring Dialing

The Dial tab of the Endpoint Control window allows you to specify an address or endpoint to which the current endpoint dials.

Procedure

Step 1 Configure the Dial tab as follows:

- Dial to address—When selected, the endpoint makes a call to the specified address.
- Dial to network endpoint—Select from a list of endpoints on the network to which the endpoint dials a call.
- Log—Displays a log events for the current call.
- Connect—Connects the endpoint in a call at the specified address or with the selected endpoint.
- Dial Parameters—Displays the Dial Parameters window in which you specify the call type and whether the call is restricted to other incoming callers.

Step 2 To add the new settings to the endpoint, click **Upload** or to update the new settings, click **Refresh**.

Configuring an MCU

When an MCU is selected in the tree, additional tabs are displayed allowing you to view services and manage MP units, including the following:

- Configuring Protocols, page 12-16
- Displaying Registered MPs, page 12-17
- Configuring Multipoint Processors, page 12-17
- Displaying Services, page 12-18

Note The tabs displayed vary according to the MCU version.

Configuring Protocols

The Protocols tab allows you to configure how the MCU works with H.323 and SIP call routing devices.

The Protocols tab displays the following information:

- Use H.323 Gatekeeper
- Gatekeeper IP
- Port
- Use SIP Server
- SIP Server IP
- Port

Displaying Registered MPs

The Registered MPs tab allows you to view the list of MPs currently registered with the MCU.

The Registered MPs tab displays the following information:

- Type—Displays the type of MP unit registered with the current MCU. MP unit types supported include:
  - MP—The local MP component of the current MCU or an MCU operating in *MP Only* mode. Performs basic media processing such as audio transcoding, video processing and video switching.
  - EMP—Unit performing advanced media processing such as video processing and video switching.
- Address—Address of the MP unit. This may be the same as the current MCU if the MP is the media processing component of the current unit.
- Description—Version number and type.

Configuring Multipoint Processors

The MP List tab enables you to define the MPs being controlled by an MCU in a clustered layout (local MPs or MCUs configured as MP only). Up to six MPs can be controlled by a single MCU in this type of layout.

The MP List tab displays the following information about each MP:

- Description of the MP
- IP address
- Current status (enabled or disabled)

Adding an MP

To add an MP, use the following procedure:

Procedure

Step 1 Click **Add**.

The Add MP window appears, which enables you to define the IP address and optional description of MPs being controlled by the selected MCU.

Step 2 To activate the MP, select **Enable**.

Step 3 Click **OK**.

The new MP is added to the displayed list.

Note To modify and delete existing MPs, use the Edit and Delete buttons.

Displaying Services

The Services tab displays the list of services supported by the selected MCU Services can be edited by clicking on the link to the MCU element manager

The Services tab displays the following information:

- Prefix used to access the service
- Service description
- Number of parties allowed in the conference
- Media (such as video)
- Layout setting
- Bit rate (maximum bit rate)
- T.120 setting (enabled or disabled)
- Video format
- Picture format
- Frame rate

Note To edit the information in the table, click the link above the table to access the element manager.

Configuring a Gateway

When a gateway is selected in the tree, an additional tab appears, enabling you to view and add services.

Services

The Services tab displays the list of services supported by the selected gateway.

The Services tab displays the following information:

- Prefix used to access the service
- Service description
- Status
- Conference Hunting
- In-Zone Default
- Out of Zone

Adding a Service

To add a service, use the following procedure:

Procedure

Step 1 Click **Add**.

Step 2 Enter the prefix of the service and the service description, then select the call type (Video or Voice) and the bit rate.

Step 3 Click **OK**.

The new service is added to the displayed list.

Note To modify and delete existing services, use the Edit and Delete buttons.

Configuring a Cisco IOS H.323 Gatekeeper

When a Cisco IOS H.323 Gatekeeper is selected in the tree, additional tabs are displayed, enabling you to view and configure Cisco IOS H.323 Gatekeeper–specific tabs, including the following:

- Configuring Local Zones, page 12-19
- Configuring Remote Zones, page 12-19
- Configuring Prefixes, page 12-20
- Configuring Bandwidth Rules, page 12-21
- Configuring Debug Flags, page 12-22
- Configuring Commands, page 12-22

Configuring Local Zones

The Local Zones tab enables you to view and configure local Cisco IOS H.323 Gatekeeper sub-zones used for bandwidth control purposes.

The Local Zones tab displays the following information:

- Zone Name
- Domain

Adding a Local Zone

Click **Add** to display the Add Local Zone window which enables you to define local zones for the Cisco IOS H.323 Gatekeeper. Enter a zone name and the zone domain. Click **OK** and the zone is added to the Local Zones list.

Note To modify and delete existing local zones, use the Edit and Delete buttons.

Configuring Remote Zones

The Remote Zones tab enables you to view, configure and modify remote Cisco IOS H.323 Gatekeepers for resolving destination IP addresses when the source endpoint is not in the same zone as the destination endpoint.

The Remote Zones tab displays the following information:

- Zone Name
- Domain
- IP Address
- Port

Adding a Remote Zone

To add a remote zone:

Procedure

Step 1 Click **Add**.

Step 2 Enter a zone name, zone domain, IP address and port.

Step 3 Click **OK** and the zone is added to the Remote Zones list.

Note To modify and delete existing remote zones, use the Edit and Delete buttons.

Configuring Prefixes

The Prefixes tab enables you to assign prefixes to local and remote Cisco IOS H.323 Gatekeeper zones, configure the method for sending LRQ messages to each destination for address resolution and assign gateway priorities.

The Prefixes tab displays the following information:

- Zone Name
- Prefix
- Search Mode—Blast or sequential
- Gateway Priority
- Gateway Aliases

Adding a Prefix

To add a prefix, use the following procedure:

Procedure

Step 1 Click **Add**.

The Add Prefix window appears, which enables you to configure prefixes with which the Cisco IOS H.323 Gatekeeper performs address resolution, specify prefix values, send LRQ messages simultaneously and configure gateway priorities per zone.

Step 2 Select a zone, enter a prefix number and select **Blast** for sending LRQ messages simultaneously.

Step 3 Click **OK** to add the zone to the Prefixes list.

Note To modify and delete existing prefixes, use the Edit and Delete buttons.

Configuring Bandwidth Rules

The BW Rules tab enables you control the bandwidth of H.323 traffic both in the Cisco IOS H.323 Gatekeeper zone and between the Cisco IOS H.323 Gatekeeper and other zones. Bandwidth rules per session or specific zones can also be specified. A default setting specifies a bandwidth rule for all zones with which the Cisco IOS H.323 Gatekeeper operates.

The BW Rules tab displays the following information:

- Scope:
  - Total—Indicates the total amount of bandwidth for H.323 traffic allowed in this zone.
  - Remote—Indicates the total amount of bandwidth for H.323 traffic from this zone to all other zones.
  - Interzone—Indicates the total amount of bandwidth for H.323 traffic from this zone to another zone.
  - Session—Indicates the maximum bandwidth allowed for a session in the zone.
- Default—Indicates the default value for all zones is configured in this rule.
- Zone
- Bandwidth

Adding a Bandwidth Rule

To add a bandwidth rule, use the following procedure:

Procedure

Step 1 Click **Add**.

The Add Bandwidth Rules window appears, which enables you to specify bandwidth limitations on H.323 traffic between both within the zone and between other zones either per session or per zone.

Step 2 Select the scope of the bandwidth rule, indicate whether the rule is the default for all zones, select a zone and maximum bandwidth rate.

Step 3 Click **OK** and the bandwidth rule is added to the BW Rules list.

Note To modify and delete existing bandwidth rules, use the Edit and Delete buttons.

Configuring Debug Flags

The Debug Flags tab enables you to view and configure Cisco IOS H.323 Gatekeeper debugging commands.

The Debug flags tab displays the following information:

- Debug Command
- Description
- Status

Adding a Debug Flag

To add a debug flag, use the following procedure:

Procedure

Step 1 Click **Add**.

Step 2 Enter the debug flag name, a description and select to enable the flag.

Step 3 Click **OK** and the debug flag is added to the Debug Flags list and if selected, the debug flag is enabled.

Caution Set debug flags with caution as too many may inhibit the performance of the Cisco IOS H.323 Gatekeeper on the network.

Note To modify and delete existing debug commands, use the Edit and Delete buttons.

Configuring Commands

The Command tab enables you to use the Network Manager Web interface to view Cisco IOS H.323 Gatekeeper monitoring information and perform configuration. A default set of commands are available and you may also enter additional commands in the Command text box. The tab window displays the results.

Using Cisco IOS H.323 Gatekeeper Commands

Information can be automatically retrieved from the Cisco IOS H.323 Gatekeeper using a set of predefined commands from the list or manually by entering Cisco IOS H.323 Gatekeeper commands in the text box and clicking Show. The results are displayed on the tab window.

To configure a Cisco IOS H.323 Gatekeeper, enter the command in the text box and click **Configure**. Clicking the Configure button performs all the Telnet commands necessary to access the appropriate Cisco IOS H.323 Gatekeeper gatekeeper configuration level for performing the command you specified in the text box.