CHAPTER 21

Configuring Cisco TelePresence MSE 8000 Series

The following sections describe how to configure the Cisco TelePresence MSE 8000 Series products and the Cisco VCS products:

About the Cisco TelePresence MSE 8000 Series Products

The Cisco TelePresence MSE 8000 Series products support carrier-class telepresence services. The chassis contains a supervisor module and provides nine slots for optional service modules.

The Cisco TelePresence Exchange System uses the following types of service modules:

- Cisco TelePresence MCU MSE 8510—Provides inter-working with single-screen telepresence endpoints that support SIP, H.323, or ISDN standard.
- Cisco TelePresence Server MSE 8710—Provides inter-working with single-screen and multi-screen telepresence endpoints.
- Cisco TelePresence ISDN GW MSE 8321—Provides inter-working with ISDN endpoints.

For additional information, see the Cisco TelePresence MSE 8000 Series website at http://www.cisco.com/en/US/products/ps11340/index.html.

Note When an enterprise wants to deploy Cisco or third-party standards-based (H.323 or ISDN standard) endpoints, the enterprise must install at least one Cisco VCS.

- The required media resources and ISDN gateways used by the Cisco TelePresence Exchange System register directly with the Cisco VCS.
- There are some configuration settings that must be made on the Cisco VCS and SBC that is used within the network. For details, see the "Configuring Call Control" section on page 21-11.
- For additional details on the Cisco VCS, see the Cisco TelePresence Video Communication Server (VCS) website at http://www.cisco.com/en/US/products/ps11337/index.html.

Configuring Cisco TelePresence MSE 8000 Series Settings

The following sections describe how to configure the optional Cisco TelePresence MSE 8000 Series service modules to be used with the Cisco TelePresence Exchange System:

Accessing the Web Interface

After you install the Cisco TelePresence MSE 8000 Series chassis and supervisor module, you can configure the other modules in the chassis by using the supervisor web interface.

Procedure

To access the web interface, do the following procedure:

Step 1 Browse to http://<*IP address of the supervisor module*>.

Step 2 Log in to the system by using a valid administrator username and password.

Step 3 From the navigation pane, choose the **Hardware** tab.

The Blades window is displayed, which lists the available service modules.

Step 4 In the Type column, click the IP address of the applicable service module.

Note You can also configure the service module directly by entering its IP address (as listed under the Port A address column) in a browser window (http://<*IP address of the service module*>). However, there might be a short delay in reporting changes to the supervisor module. Changes made directly from the supervisor module update immediately.

The system displays a summary window for the selected module. Subsequent sections in this chapter provide details about configuring each module.

Configuring SNMP Traps

Procedure

To configure the SNMP traps, do the following procedure:

Step 1 From the navigation pane, choose the **Network** tab.

The supervisor Port A window is displayed.

Step 2 Click the **SNMP** tab.

The SNMP window is displayed.

Step 3 Check the **enable traps** check box, and then enter the IP address of a trap receiver.

Step 4 To save the configuration, click **Update SNMP Settings**.

Configuring Cisco TelePresence Server MSE 8710 Settings

The Cisco TelePresence Server MSE 8710 is a media service module for the Cisco TelePresence MSE 8000 Series platform. The Cisco TelePresence Server MSE 8710 provides conferencing services between Cisco TelePresence and multi-screen standards-based endpoints.

The Cisco TelePresence Server MSE 8710 web interface provides context-sensitive help. Click the information (i) icon in any window to see a description of the fields.

The procedures in this section assume that you browse directly (http://*<IP address of the module>*) to the Cisco TelePresence Server MSE 8710 rather than through the supervisor module. For more details, see the "Accessing the Web Interface" section on page 21-2.

Note Cisco TelePresence Server MSE 8710 modules support master/slave redundancy. Only the master module requires configuration of its parameters. The slave module inherits the configuration from the master.

The following sections describe how to configure the Cisco TelePresence Server MSE 8710:

Configuring Services

Procedure

To configure and enable services, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu.

Step 2 Click the **Services** tab.

The Services window is displayed with the available TCP and UDP services.

Step 3 For Port A, check the check boxes for the following services:

- Web
- Incoming H.323
- Incoming SIP (TCP)
- FTP
- SIP (UDP)

For each service, you can leave the default port number value or you can configure a custom value.

Step 4 If you enabled port B, check the check boxes for the following services:

- Web
- Incoming H.323
- Incoming SIP (TCP)
- FTP
- SIP (UDP)

Step 5 To save the updates, click **Apply changes**.

Configuring H.323 Gatekeeper

Procedure

To configure the H.323 gatekeeper settings, do the following procedure:

Step 1 After logging in, choose **Configuration** from the navigation menu.

Step 2 Click the **System Settings** tab.

The System settings window is displayed.

Step 3 In the H.323 gatekeeper window section, check the **Use gatekeeper** check box, and then enter the IP address of the Cisco TelePresence Video Communication Server in use.

Step 4 In the H.323 ID to register field, enter a registration identifier.

Ensure that you provide a unique identifier for each media server that registers with the same H.323 gatekeeper. Cisco recommends that the registration identifier be 10 digits.

Step 5 To save the updates, click **Apply changes**.

Configuring SIP for Dial-Out Calls

Procedure

To configure the SIP dial-out call settings, do the following procedure:

Step 1 After logging in, choose **Configuration** from the navigation menu.

Step 2 Click the **System Settings** tab.

The System settings window is displayed.

Step 3 From the Outbound call configuration drop-down list, choose **Use trunk**.

Step 4 In the Outbound address field, enter the IP address of the ACE virtual IP (VIP).

Step 5 In the Outbound transport drop-down list, choose **TCP**.

Step 6 To save the configuration, click **Apply changes**.

Configuring API User

Procedure

To configure the API user, do the following procedure:

Step 1 After logging in, choose **Users** from the navigation menu.

The Users window is displayed.

Step 2 Click **Add new user**.

Step 3 In the User ID field, enter **apitest**.

Step 4 To give API administration privileges to the module, check the **Administrator** check box.

Privileges include actions such as adding and deleting conferences.

Step 5 To save the configuration, click **Add user**.

Configuring Cisco TelePresence MCU MSE 8510 Settings

The Cisco TelePresence MCU MSE 8510 is a media service module that provides conferencing service for single-screen H.323 and ISDN standards-based endpoints.

Note The Cisco TelePresence MCU MSE 8510 does not support Cisco TelePresence TIP-based endpoints running CTS Software Release 1.7 or earlier.

The Cisco TelePresence MCU MSE 8510 web interface provides context-sensitive help. Click the information (i) icon in any window to see a description of the fields.

The procedures in this section assume that you browse (http://<*IP address of the module*>) directly to the IP address of the Cisco TelePresence MCU MSE 8510 rather than through the supervisor module. For more details, see the "Accessing the Web Interface" section on page 21-2.

Note Cisco TelePresence Server MCU MSE 8510 modules support master/slave redundancy. Only the master module requires configuration of its parameters. The slave module inherits the configuration from the master.

The following sections describe the configuration tasks:

Configuring Services

Procedure

To configure and enable services, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu (top of window).

The system displays the port A network settings.

Step 2 From the Network window that is displayed, click the **Services** tab.

The Services window is displayed.

Step 3 For port A, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

For each service, you can leave the default port number value or you can configure a custom value.

Step 4 If you have enabled port B, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

Step 5 To save the updates, click **Apply changes**.

Configuring SNMP Traps

Procedure

To configure the SNMP traps, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu.

The system displays the port A network settings.

Step 2 Click the **SNMP** tab.

The system displays the SNMP configuration.

Step 3 Check the **Enable traps** check box, and then enter an IP address for a trap receiver in an available field.

Step 4 To save the updates, click **Update SNMP settings**.

Configuring Conference Settings

Procedure

To configure conference settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

The system displays the conference settings.

Step 2 From the Failed preconfigured participants redial behavior drop-down list, choose **Never redial**.

You do not need to make any additional changes on the **Settings** tab.

Step 3 To save the updates, click **Apply changes**.

Configuring Media Port Settings

Procedure

To configure media port settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **Media ports** tab.

The Media port allocation window is displayed.

Step 3 From the Media port mode drop-down list, choose **HD**.

Step 4 To save the updates, click **Apply changes**.

Configuring H.323 Settings

Procedure

To configure H.323 settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **H.323** tab.

The system displays the H.323 gatekeeper settings.

Step 3 In the H.323 gatekeeper address field, enter the Cisco VCS IP address.

Step 4 In the H.323 ID to register field, enter a registration identifier.

Ensure that you provide a unique identifier for each media server that registers with the same H.323 gatekeeper. Cisco recommends that the registration identifier be 10 digits.

Step 5 To save the updates, click **Apply changes**.

Configuring SIP Dial-Out Call Settings

Procedure

To configure the SIP dial-out call settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **SIP** tab.

The system displays the SIP and SIP call settings.

Step 3 From the SIP registrar usage drop-down list, choose **Disabled**.

Step 4 From the SIP registrar type drop-down list, choose **Standard SIP**.

Step 5 In the Username field, enter a unique number identifier for all dial out calls from the Cisco TelePresence MCU MSE 8510.

Step 6 In the SIP proxy address field, enter the IP address of the ACE virtual IP (VIP).

Step 7 From the Maximum bit rate from Microsoft OCS/LCS clients drop-down menu, choose **<limit disabled>**.

Step 8 At the Outgoing transport option, click the TCP radio button.

Step 9 To save the updates, click **Apply changes**.

Configuring API User

Procedure

To configure the API user, do the following procedure:

Step 1 After logging in, choose **Users** from the navigation menu.

The system displays the configured users window.

Step 2 To add API as a user, click **Add new user**.

Step 3 In the User ID field, enter **apitest**.

Step 4 From the Privilege level drop-down list, choose **administrator** to give API user administration privileges to the module.

Privileges include actions such as adding and deleting conferences.

Step 5 Click **Add user** to save the updates.

Configuring Cisco TelePresence ISDN GW MSE 8321 Settings

The Cisco TelePresence ISDN GW MSE 8321 service module enables the Cisco TelePresence Exchange System to dial out to ISDN endpoints.

The procedures in this section assume that you browse (http://*<IP address of the module>*) directly to the IP address of the Cisco TelePresence ISDN GW MSE 8321 rather than through the supervisor module.

The following sections describe how to configure the ISDN gateway settings:

Configuring Services

Procedure

To configure and enable services, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu (top of window).

The system displays the port A network settings.

Step 2 Click the **Services** tab.

The Services window is displayed, summarizing TCP and UDP services.

Step 3 For Port A, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

For each service, you can leave the default port number value or you can configure a custom value.

Step 4 If you have enabled port B, check the check boxes for all of the TCP and UDP services except for Tunneled Media.

Step 5 To save the updates, click **Apply changes**.

Configuring SNMP Traps

Procedure

To configure the SNMP traps, do the following procedure:

Step 1 After logging in, choose **Network** from the navigation menu.

The system displays the port A network settings.

Step 2 Click the **SNMP** tab.

The system displays the SNMP configuration.

Step 3 Check the **Enable traps** check box, and then enter an IP address for a trap receiver in an available address field.

Step 4 To save the updates, click **Update SNMP settings**.

Configuring ISDN Settings

Procedure

To configure the ISDN settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **ISDN** tab.

The ISDN window is displayed.

Step 3 In the ISDN codec settings section, check the **H.263** and **H.264** check boxes if they are not already checked.

By default, the system enables all video codecs.

The Content video and Audio codecs allowed fields remain at the default settings.

Step 4 To save the updates, click **Apply changes**.

Configuring ISDN Ports

Procedure

To configure ISDN ports, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **ISDN ports** tab.

The system displays settings for ports 1 through 8. You can use the default setting for most of the fields.

Step 3 In the Directory Number (DN) field, no entry is required.

Step 4 Enter the prefix for national numbers.

For example, in North America, enter 1.

Step 5 Enter the prefix for international numbers.

For example, in North America, enter 011.

Note The above examples only apply to North America. Use appropriate rules for other countries.

Step 6 To save the updates, click **Apply changes**.

Configuring H.323 Settings

Procedure

To configure H.323 settings, do the following procedure:

Step 1 After logging in, choose **Settings** from the navigation menu.

Step 2 Click the **H.323** tab.

The system displays the H.323 gatekeeper settings. You can use the default setting for most of the fields.

Step 3 From the H.323 gatekeeper usage drop-down list, choose **Enabled**.

Step 4 In the H.323 gatekeeper address field, enter the IP address of the Cisco VCS.

Step 5 (Optional) If you provision more than one ISDN gateway module, you can use the **Dial plan prefixes** field to select a subset of traffic for each module.

When the start of the dialed digits matches a prefix in the dial plan prefix list, an ISDN call will be scheduled on this gateway.

Step 6 To save the updates, click **Apply changes**.

Configuring IP to ISDN Dial Plan

When configuring the dial plan, note the following:

- By default, the Cisco TelePresence Exchange System applies a prefix of 9 to all numbers. The service provider can change the prefix default during system installation.
- All numbers are defined in an E164 format such as 14085551212.
- At a minimum, a dial plan should remove the prefix of 9, and prepend or append the modified number, as necessary, to allow successful termination on the ISDN network.

Procedure

To configure IP to ISDN dial plan settings, do the following procedure:

Step 1 After logging in, choose **Dial plan** from the navigation menu.

The system displays the IP to ISDN dial plan.

Step 2 To add a rule, click **Add rule**.

The system displays the Add IP to ISDN dial plan rule window.

Step 3 At a minimum, Cisco recommends defining the following rules to recognize numbers that are forwarded from the Cisco TelePresence Exchange System:

a. At the Condition option, click the **Called number matches** radio button, and then enter **9(D*)** in the field next to that option.

b. At the Action option, click the **Call this number** radio button, and then enter **$1** in the field next to that option.

Step 4 Click **Add Rule** to save the configuration.

The system displays the IP to ISDN dial plan window, which displays the new rule.

Step 5 To test the dial plan rules, enter the number in the Number to test field, and then click **Test number**.

Configuring Call Control

The Cisco TelePresence Exchange System provides the capability to communicate with standards-based endpoints by using H.323 signaling. The Cisco VCS acts as an H.323 gatekeeper for the interop endpoints. The Cisco TelePresence Exchange System communicates with the Cisco VCS through an H.323 SBC.

The following sections include information about configuring call control settings on the Cisco VCS and SBC:

- Configuring Cisco VCS Settings, page 21-12
- Configuring H.323 Gateway Settings on the SBC, page 21-12

Configuring Cisco VCS Settings

When an enterprise wants to deploy Cisco TelePresence and third-party standards-based endpoints, the enterprise must install at least one Cisco VCS. The required media resources and ISDN gateways used by the Cisco TelePresence Exchange System register directly with the Cisco VCS.

For dial out calls made from the Cisco TelePresence Exchange System to provisioned endpoints that are registered with a Cisco VCS using a SIP URI, you must add a transform rule (also known as search rule) on the Cisco VCS. This transform rule should replace the IP address of the Cisco VCS with the appropriate domain name in the SIP URI of the provisioned endpoint. The following example shows a transform rule that could be configured on a Cisco VCS. In this example, 1.2.3.4 is the IP address of the Cisco VCS and cisco.com is the domain name in the SIP URI of the provisioned endpoint.

```
Priority  State    Description             Pattern          Type    Behavior   Replace

1         Enabled  Transform IP to Domain  (\w+)@1.2.3.4    Regex   Replace    \1@cisco.com
```

Product information for the Cisco VCS, can be found at http://www.cisco.com/en/US/products/ps11337/index.html.

Configuring H.323 Gateway Settings on the SBC

The Cisco TelePresence Exchange System communicates with the Cisco VCS through an SBC that supports the H.323 protocol.

The required media resources and ISDN gateways used by the Cisco TelePresence Exchange System register directly with the Cisco VCS.

To configure an SBC that supports the H.323 protocol, do the following configuration tasks:

- Configuring Adjacencies with Each Cisco VCS, page 21-12
- Configuring Call Policies, page 21-13

Configuring Adjacencies with Each Cisco VCS

On an SBC that supports the H.323 protocol, configure an adjacency to each Cisco VCS.

Procedure

To configure an adjacency, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)# adjacency (sip | h323) adjacency-name`	Enters configuration mode for the specified SIP or H.323 adjacency. For a Cisco VCS adjacency, enter **h323** as the type of adjacency.
Step 2	`Router(config-sbc-sbe-adj-h323)# signaling-address{ipv4_IP_address|ipv6_IP_address}`	Configures the local IP address of the signaling link to the Cisco VCS.
Step 3	`Router(config-sbc-sbe-adj-h323)# signaling-port port-num [max-port-num]`	Configures the port number for the signaling link to the Cisco VCS.

	Command	Purpose
Step 4	`Router(config-sbc-sbe-adj-h323)#` **`remote-address ipv4`** *`remote-address`*	Configures the IP address of the remote end of the signaling link to the Cisco VCS.
Step 5	`Router(config-sbc-sbe-adj-h323)#` **`signaling-peer`** *`peer-name`*	Configures the H.323 adjacency to use the specified remote signaling-peer. Specify the signaling IPv4 address of the Cisco VCS in dotted-decimal format.
Step 6	`Router(config-sbc-sbe-adj-h323)#` **`signaling-peer-port`** *`peer-name`*	Specify the port number for use with the signaling peer.
Step 7	`Router(config-sbc-sbe-adj-h323)#` **`tech-prefix`** *`prefix-num`*	Specify a prefix number. Calls with this prefix (in the dialed number) are routed to the SBC if the Cisco VCS cannot find any other route for the call.
Step 8	`Router(config-sbc-sbe-adj-h323)#` **`attach`**	Attaches the adjacency to the SBC instance. The adjacency is now available for H.323 call processing.

The following example shows how to create an adjacency between the SBE and a hosted Cisco VCS:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 SBC-VCS
Router(config-sbc-sbe-adj-h323)# signaling-address ipv4 10.22.141.100
Router(config-sbc-sbe-adj-h323)# signaling-port 1719
Router(config-sbc-sbe-adj-h323)# remote-address ipv4 10.22.141.98 255.255.255.255
Router(config-sbc-sbe-adj-h323)# signaling-peer 10.22.141.98
Router(config-sbc-sbe-adj-h323)# signaling-peer-port 1719
Router(config-sbc-sbe-adj-h323)# tech-prefix 1
Router(config-sbc-sbe-adj-h323))# attach
```

The following example shows how to create an adjacency between the SBC and an enterprise Cisco TelePresence Video Communication Server:

```
Router(config)# sbc mmsbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 SBC-VCS-ent1
Router(config-sbc-sbe-adj-h323)# signaling-address ipv4 10.22.141.100
Router(config-sbc-sbe-adj-h323)# signaling-port 1719
Router(config-sbc-sbe-adj-h323)# remote-address ipv4 10.22.141.98 255.255.255.255
Router(config-sbc-sbe-adj-h323)# signaling-peer 10.22.141.98
Router(config-sbc-sbe-adj-h323)# signaling-peer-port 1719
Router(config-sbc-sbe-adj-h323))# attach
```

Configuring Call Policies

Procedure

To create a call policy set and configure the route tables, do the following procedure:

	Command	Purpose
Step 1	`Router(config-sbc-sbe)#` **`call-policy-set`** *`policy-set-id`*	Creates a new policy set for processing calls within the SBE.
Step 2	`Router(config-sbc-sbe-rtgpolicy)#` **`first-call-routing-table`** *`table-name`*	Configures the name of the first routing table for new-call events.
Step 3	`Router(config-sbc-sbe-rtgpolicy)#` **`rtg-src-adjacency-table`** *`table-id`*	Creates a new routing table whose entries match the source adjacency.

	Command	Purpose
Step 4	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry entry-id`	Creates an entry in the routing table.
Step 5	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-adjacency key`	Configures the source adjacency as the match value for this table entry.
Step 6	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action {complete | {next-table go-to-table-name } }`	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.
Step 7	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-cic replace ds`	Replaces the carrier ID in the SIP message with the specified digit string.
Step 8	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# exit`	Exits the routing table entry (rtgtable-entry) mode.
Step 9	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# exit`	Exits the routing table (rtgtable) mode.
Step 10	`Router(config-sbc-sbe-rtgpolicy)# rtg-dst-adjacency-table table-id`	Creates a new routing table whose entries match the source adjacency.
Step 11	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# entry entry-id`	Creates an entry in the routing table.
Step 12	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# match-address key`	Configures the carrier ID match value of the entry.
Step 13	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency target-adjacency`	Configures the destination adjacency of an entry in a routing table.
Step 14	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# action {complete | {next-table go-to-table-name } }`	Specifies the next routing table to process if the event matches the entry. Action complete specifies that no further action is required.
Step 15	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# edit-dst del-prefix ds`	Replaces the carrier ID in the SIP message with the specified digit string.
Step 16	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# dst-adjacency target-adjacency`	Configures the destination adjacency of an entry in a routing table.
Step 17	`Router(config-sbc-sbe-rtgpolicy -rtgtable-entry)# exit`	Exits the routing table entry (rtgtable-entry) mode.
Step 18	`Router(config-sbc-sbe-rtgpolicy -rtgtable)# exit`	Exits the routing table (rtgtable) mode.
Step 19	`Router(config-sbc-sbe-rtgpolicy)# complete`	Marks the end of a call policy set definition.
Step 20	`Router(config-sbc-sbe-rtgpolicy)# exit`	Exits the routing policy (rtgpolicy) mode.
Step 21	`Router(config-sbc-sbe)# active-call-policy-set policy-set-id`	Activates the call policy set.

The following example shows how to create a call policy set and configure route tables:

```
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table INCOMING
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table INCOMING
```

```
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 200
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency SBC-UNCM
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action next-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# exit

Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table OUTGOING
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1922 digits
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1922 digits
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-dst del-prefix 1
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 3
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 139 digits
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency WMT-ADJ1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# prefix
Router(config-sbc-sbe-rtgpolicy-rtgtable)# exit
Router(config-sbc-sbe-rtgpolicy)# complete
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)# active-call-policy-set 1
```