CHAPTER 19

Configuring SRST Poll Settings

The following topics describe using SRST:

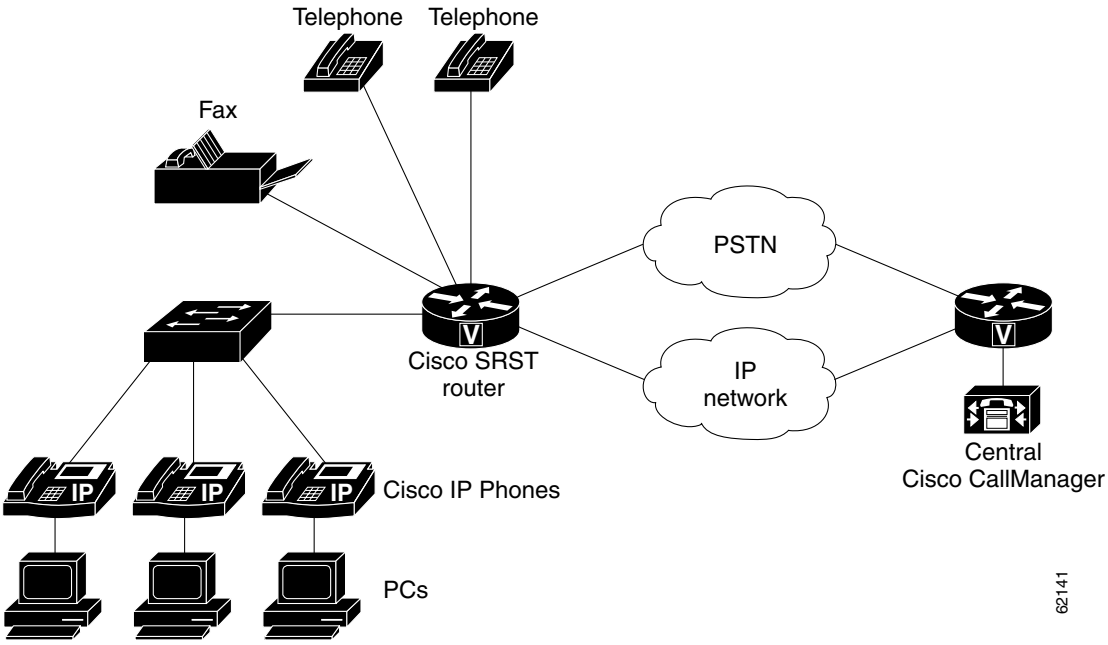
Understanding How Operations Manager Monitors SRST

Figure 19-1 shows a branch office configured for Survivable Remote Site Telephony (SRST). The branch office normally relies on a central Cisco Unified Communications Manager for call processing. If the Cisco Unified Communications Manager becomes inaccessible, phones can use a Cisco voice router for call processing. Phones go into SRST mode when either of the following happens:

- The WAN link to the Cisco Unified Communications Manager at the central site goes down
- The connection to the Cisco Unified Communications Manager is lost

SRST allows phones in branch offices to continue to function until the WAN link comes up or until the phones can register with a Cisco Unified Communications Manager again.

Figure 19-1 Branch Office Cisco Unified IP Phones Connected to a Remote Central Cisco Unified Communications Manager



For Operations Manager to display phones in SRST mode and generate related alerts, you must configure SRST poll settings, identifying the SRST components for Operations Manager to test. Operations Manager does the following:

- Configures IP SLA jitter tests on the source router (at the central Cisco Unified Communications Manager site). Jitter tests run from the source router to detect the reachability of the target SRST router (at the branch office).
- Generates an SRSTEntered event when a jitter test fails, which happens in response to the WAN link being down. See Appendix E, "Events Processed," for information about the SRSTEntered and SRSTSuspected events.
- Displays a list of Cisco Unified IP Phones that are in SRST mode on phone reports. See Generating the SRST IP Phones Report, page 13-8 and Generating the All IP Phones/Lines Report, page 13-8.

Before you configure SRST poll settings, review the recommendations for your deployment of SRST.

Note If you ever need to uninstall Operations Manager, be sure to delete all the SRST tests from the application before you uninstall it. If you do not delete these tests, they will continue to run on the router. For instructions on deleting, see Deleting SRST Poll Settings, page 19-5.

Requirements and Recommendations for SRST Poll Settings

Note This topic does not explain how to configure Cisco Unified Communications Manager, Cisco routers, or Cisco Unified IP Phones for SRST. See the documentation for these products at http://www.cisco.com.

Table 19-1 lists recommendations and requirements for selecting the source router, near the central Cisco Unified Communications Manager, and configuring the SRST target router, at the branch office. See Figure 19-1 for an illustration of a sample configuration.

Table 19-1 Choosing and Configuring Source and Target Routers

Router	Requirements	Recommendations
Source	Choose the source router in such a way that the following paths are the same: • Path of the IP phone TCP keepalive message to the central site Cisco Unified Communications Manager • IP SLA jitter test packet path	Select a source router that is as close to the Cisco Unified Communications Manager as possible.
Target	Enable Cisco IOS IP SLA (IP SLA) Responder on the SRST target router.	**Note** If you disable IP SLA Responder on the target router, spurious SRSTEntered events might occur. See the SRSTEntered event in Appendix E, "Events Processed."

Note Operations Manager creates IP SLA tests on the source routers. These routers must have adequate probe capacity for Operations Manager to successfully create the IP SLA tests.

Monitoring SRST when Source or Target Routers Are Down

Table 19-2 shows how Operations Manager handles SRST activities when devices are down or unreachable.

Table 19-2 Creating SRST Poll Settings or Monitoring for SRST when Devices Are Down

Device Down or Unreachable	During the following SRST activity	Result
Source or target router	Import SRST information	The poll setting will be imported successfully, but will not be created on the routers. **Workaround**: Import SRST poll settings again after the routers become reachable.
	Create SRST poll setting	The poll setting will not be created. **Workaround**: Import SRST poll settings again after the routers become reachable.
Source router	SRST polling	Operations Manager cannot retrieve SRST results. Operations Manager does not detect SRST or generate SRST events. **Note** Operations Manager will generate appropriate events for devices that are unreachable.

Viewing SRST-Related Event Details

When Operations Manager generates an SRSTEntered or SRSTSuspected event, an alert appears on the Alerts activities window. You can drill down through the Alert Details page to view event details. Although multiple phones might be included in an SRST poll setting, only one MAC address and one phone extension are displayed in the Event Properties window.

For more information, see the following topics:

- Viewing Events Associated with an Alert, page 3-12
- Viewing Event Details, page 3-14
- Events Processed, page E-1

Maintaining SRST Poll Settings

When you configure SRST poll settings, based on the poll settings name you provide, Operations Manager either adds a new SRST poll setting or updates an existing SRST poll setting. Operations Manager also creates or updates IP SLA jitter tests on source routers, as needed.

To remove existing SRST poll settings, you must delete them; see Deleting SRST Poll Settings, page 19-5.

Note Be sure to edit SRST poll settings after you change the SRST configuration in your network. For example, if you change MAC addresses or extension numbers on IP phones, you must reconfigure SRST poll settings.

You can configure:

- A single SRST poll setting from various launch points in the Operations Manager user interface. See Configuring a Single SRST Test as Needed, page 19-9.
- Multiple SRST poll settings by importing them from a seed file. See Importing SRST Poll Settings, page 19-5.

Viewing SRST Poll Setting Status

Step 1 Select **Administration > SRST Poll Settings > SRST Operations**. The SRST Operations page appears with the following information.

Field	Description
Test Name	SRST poll setting name
Source Router	Router in the central site on which the IP SLA test is created
Target Router	Router in the branch office
Status	• Active—SRST poll setting is running as configured. • Pending—SRST poll setting is briefly in a transient state after you click Delete. **Note** If device monitoring is suspended for a source router, any associated SRST poll setting is also suspended. See Suspending Device Monitoring, page 3-24.

Deleting SRST Poll Settings

This procedure explains how to delete one or more SRST poll settings.

Note If you delete an IP SLA router from Operations Manager device inventory, any associated SRST poll settings are automatically deleted; see Deleting Devices, page 16-31.

Step 1 Select **Administration > SRST Poll Settings > SRST Operations**. The SRST Operations page appears.

Step 2 Select any of the following:

- Check box in the table heading—Select to delete all SRST poll settings.
- One or more individual check boxes—Select individual SRST poll settings that you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears, asking if you want to continue with the deletion.

Step 4 Click **OK**.

Importing SRST Poll Settings

When you import SRST information, Operations Manager adds any new poll settings from the seed file and updates any existing poll settings that you edited. To remove existing poll settings, you must delete them; see Deleting SRST Poll Settings, page 19-5.

Note Be sure to edit SRST poll settings after you change the SRST configuration in your network. For example, if you change MAC addresses or extension numbers on IP phones, do one of the following:

- Update the seed file and import SRST information again.
- Update poll settings from the Service Level View or an IP Phones and Applications report. See Configuring a Single SRST Test as Needed, page 19-9.

Before You Begin

- Verify that your deployment of SRST meets the requirements specified in Table 19-1.
- Verify that Operations Manager monitors the devices to be polled. See Verifying that Devices Are Monitored by Operations Manager Before Import, page 19-9.
- Verify that the phones that are listed in your seed file have been discovered. To view IP phone discovery status, select **Devices > Device Management > Inventory Collection > IP Phone**.
- Verify that your seed file is formatted correctly. For details, see Formatting an SRST Monitoring Seed File, page 19-6.
- Place the seed file on the server, in the NMSROOT\ImportFiles directory. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

Step 1 Select **Administration > SRST Poll Settings > SRST Import**. The Import SRST Information page appears.

Step 2 Enter the name of the seed file in the Filename field and click **OK**.

Operations Manager verifies that the data in the seed file is syntactically correct and formatted properly. If there are errors in the seed file, an error dialog box is displayed:

a. Check the srst_import.log file at NMSROOT\logs\itemlogs\srst for details.

b. Correct the problems in the seed file and import the SRST information again.

If the seed file is correct, an information dialog box is displayed.

Step 3 Click **OK**. Operations Manager verifies that the routers are reachable and then creates IP SLA jitter tests on the routers. This might take some time.

Step 4 Verify that all IP SLA jitter tests were created successfully, by examining the srst_test_creation_results.log file in NMSROOT\logs\itemlogs\srst.

Note If you do not have access to this directory, contact a local administrator for the Operations Manager server.

Step 5 If IP SLA jitter tests were not successfully created, do the following:

a. Use the log file to identify problems.

b. Make corrections in the import file and return to Step 1 to import SRST information again.

Formatting an SRST Monitoring Seed File

Note The read and write community strings that you supply in the SRST seed file are used only when community strings for the source or target device do not exist in the Device and Credentials Repository (DCR). For more information, see Editing Device Configuration and Credentials, page 16-25.

Operations Manager supports two seed file formats:

- Table 19-3 lists the preferred format. In general, you should use this format.
- Table 19-4 lists another supported format.

To format the seed file correctly, do the following:

- Include up to 256 poll settings in the seed file, one poll setting per line.

  Note If you include more than 256 poll settings, Operations Manager discards the excess poll settings.

- Include the following for each poll setting:
  - A name
  - A unique combination of source and target router
  - Up to 48 phones

    Note If you include more than 48 phones, Operations Manager discards the excess phones.

  - Information for all columns listed in Table 19-3 (or Table 19-4), delimited by a comma (,)

Table 19-3 SRST Seed File–Preferred Format

Column Number	Description
1	SRST poll settings name—Must be unique.
2	IP address or DNS name of the source router—Source router and target router (column 5) combination must be unique.
3	Read community string of the source router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
4	Write community string of the source router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
5	Username—Enter a username for the source router (if you are supplying SNMPV3 credentials).
6	Password—Enter the password for the source router (if you are supplying SNMPV3 credentials).
7	IP address or DNS name of the SRST target router—Source router (column 2) and target router combination must be unique.
8	Read community string of the SRST target router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
9	Write community string of the SRST target router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.

Table 19-3 SRST Seed File–Preferred Format (continued)

Column Number	Description
10	Phone extension numbers of IP telephones associated with SRST target router, delimited by a colon (:).
11	MAC addresses of IP telephones associated with SRST target router, delimited by a colon (:). **Note** MAC addresses must be sequenced in corresponding order with the phone extensions (see column 10).
12	Polling interval—Default (!{[NOVALUE]}!) = 30 seconds (minimum value).
13	Interpacket interval in milliseconds—Default (!{[NOVALUE]}!) = 30 milliseconds (minimum value).
14	Number of packets in each poll setting—Default (!{[NOVALUE]}!) = 10 packets (minimum value).

Example 19-1 shows a sample seed file.

Example 19-1 Sample SRST Seed File in Preferred Format

```
SRST2,10.76.34.194,public,private,admin,admin,10.76.34.222,public,private,0009e847060e:00049afc920b,
4013:4017,30,30,20
```

Table 19-4 SRST Seed File—Secondarily Supported Format

Column Number	Description
1	SRST poll settings name—Must be unique.
2	IP address or DNS name of the source router—Source router and target router (column 5) combination must be unique.
3	Read community string of the source router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
4	Write community string of the source router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
5	IP address or DNS name of the SRST target router—Source router (column 2) and target router combination must be unique.
6	Read community string of the SRST target router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
7	Write community string of the SRST target router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
8	MAC addresses of IP telephones associated with SRST target router, delimited by a colon (:).

Table 19-4 SRST Seed File—Secondarily Supported Format (continued)

Column Number	Description
9	Phone extension numbers of IP telephones associated with SRST target router, delimited by a colon (:). **Note** Phone extensions must be sequenced in corresponding order with the MAC addresses (see column 8).
10	Sample interval specification—Default (!{[NOVALUE]}!) = 30 seconds (minimum value).
11	Interpacket interval in milliseconds—Default (!{[NOVALUE]}!) = 30 milliseconds (minimum value).
12	Number of packets in each poll setting—Default (!{[NOVALUE]}!) = 10 packets (minimum value).

Example 19-2 shows a sample seed file.

Example 19-2 Sample SRST Seed File in Secondarily Supported Format

```
Test1,10.76.34.194,public,private,10.76.34.218,public,private,0009e8470515:00075079c2da,4015:1016,30,30,10
```

Verifying that Devices Are Monitored by Operations Manager Before Import

Before you import SRST poll settings, verify that the following devices are monitored by Operations Manager:

- The media server that runs the Cisco Unified Communications Manager at the central site. (Phones at the remote site are registered to this Cisco Unified Communications Manager.)
- Switches to which the phones at the remote site are connected.
- Source and target routers.

Configuring a Single SRST Test as Needed

You can create an SRST poll setting wherever the SRST Test menu item is available, in either of the following ways:

- On a right-click menu—For example, when you right-click an appropriate device in the Service Level View.
- From a Launch button or Launch Tools menu—For example, when you open the Alert Details window from Alerts and Events for an appropriate device.

When you select the SRST Test menu item, the SRST Test Creation window opens.

Note SRST test names must be unique. If you enter an existing test name, the existing test will be updated. To see a list of existing tests, open the SRST Operations page; for more information, see Viewing SRST Poll Setting Status, page 19-4.

Step 1 Specify a source device that is IP SLA-enabled by entering or selecting the following:

- Name—IP address or DNS name of a device. This field might already contain a name; this might happen, for example, if you select a device on a monitoring dashboard and launch an SRST test for it. You can:
  - Enter an IP address or DNS name for an IP SLA-enabled device.
  - Expand device groups in the selector and select a device.
- Interface—(Optional) Enter an IP address or DNS name to set up the test from a particular interface on the device.

The IP SLA test will be created on the source device.

Note You can switch the name and interface for the source device with those for the destination device by clicking the **Swap Source and Destination** button.

Step 2 Select a destination SRST device by entering or selecting the following:

- Name—Enter an IP address or DNS name or select one from the device selector.
- Interface—(Optional) Enter an IP address or DNS name to set up the test from a particular interface on the device.

Step 3 Add phones to the Selected Phones list in one of the following ways:

- Click **Add > From Known List**. The Add Phone From Known List dialog box appears:
  - Enter phone extensions and MAC addresses formatted like the following:

    ```
    extension:MAC, extension:MAC
    ```

  - Click **Apply**. The dialog box closes and the Selected Phones list is updated.
- Click **Add > From Phone Report**. The All Phones Display window opens.
  - Select a check box for each phone that you want to add to the test.
  - Scroll to the bottom right corner of the window and click **Select**. The All Phones Display closes and the Selected Phones list is updated.
- Type directly into the Selected Phones list to add or remove phones.

Step 4 Enter a test name in the Test Name field.

Step 5 Click **OK**. Additional windows might appear:

- If there are no credentials in the DCR for the source or target device, the SRST Get Credentials dialog box appears:
  - Enter the requested (Read or Write) community string twice.
  - Click **OK**.
- An informational dialog box appears, displaying a message similar to the following:

  ```
  Number of tests updated =0.
  Number of new tests =1.
  For details on errors and validation, see
  NMSROOT/log/itemlogs/srst/srst_import_errors.log.
  Test creation is in progress.
  ```

Note In this example, one new test is being created.

Step 6 Verify that the test was created successfully:

a. Select **Administration > SRST Polling Settings > SRST Operations**. The SRST Operations page appears.

b. Locate the test in the Test Name column. If you cannot locate the test, see the *NMSROOT*\log\itemlogs\srst\srst_import_errrors.log file.

Note NMSROOT is the directory where you installed Operations Manager. If you accepted the default installation directory, NMSROOT is C:\Progra~1\CSCOpx.