CHAPTER 46

How to Diagnose a Problem

This chapter contains the following procedures that you can perform to help troubleshoot issues:

Troubleshooting from the Health Summary Page

Accessing the Health Summary page is the first step that you perform when you troubleshoot.

The Health Summary page provides status about your system and assistance with troubleshooting issues. The Health Summary page displays subsystems (Table 46-1) and status messages for each subsystem. If no problem occurs in the subsystem, a green check mark and the message, *This subsystem is operating normally*, displays for the subsystem. If an issue occurs in the subsystem, a red X displays next to the category, and a status message indicates that an issue occurred.

The status of the system gets checked every 30 seconds. When a check occurs, the status that currently displays is compared to the status that is returned from the server. If the status does not match, the status message and icon get updated on the page. (For example, if an issue occurred and the system check indicates that the issue resolved itself, the status for the subsystem changes from a red cross to a green check mark.)

Perform the following procedure to troubleshoot through the Health Summary page.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface.

Step 2 To access the Health Summary page, select **Monitoring > Health Summary**. Under each subsystem, the status displays. If an X displays next to a category, an issue has occurred.

Table 46-1 describes the subsystems that display on the Health Summary page (**Monitoring > Health Summary**).

Table 46-1 Subsystems on the Health Summary Page

Subsystems	Description
System Health	This category provides status for your server and the services that are running on your server. It also provides status of system parameters such as CPU Voltage, Temperature, and fan speed, if these parameters exceed the threshold values.
Telephony Network Gateways	This category displays status of your internal and external gateways; for example, this category identifies whether the gateway is unregistered from the system.
Telephony Network Connection	This category displays status on the health of your telephony network connection; for example, whether your telephony network connection is operational, whether your gateway is connecting properly to the telephony network, and so on.
Internet Connection	This category displays status information for your Internet network; for example, this category identifies issues with IP addresses, DNS, and host configuration.
Internal Network	This category displays the status of registered devices such as phones, gateways and trunks. If the number of registered devices is less than 66.67%, the status of registered devices is displayed as down.

Tip Multiple issues may display on this page at the same time.

Step 3 To review information on how to troubleshoot the issue, click the **here** link that displays in the status message. Follow the steps in the online help to resolve the issue.

Step 4 If the online help indicates that you need to collect logs or enable detailed logging during the event, you must perform additional tasks to troubleshoot the issue. See the "Troubleshooting From the Diagnostics Page" section on page 46-41.

Additional Information

- Troubleshooting From the Diagnostics Page, page 46-41
- Troubleshooting Issues, page 47-51

Troubleshooting From the Diagnostics Page

The Diagnostics page allows you to run diagnostics for your system, gather diagnostic information for your system, and download the diagnostic information. If your Value Added Reseller (VAR), Cisco Technical Assistance Center (TAC), or the online help for the Health Summary page indicate that you need to use the Diagnostic page to continue to a diagnose an issue, perform the following procedure.

Tip The system zips up the logs by using WinZip. The system only allows you to keep one zip file at a time on your Cisco Unified Communications Manager Business Edition 3000 server. When you generate a log file, you automatically overwrite the last zip file on the server. Make sure that you download the log file to a location on your PC that can handle the size of the zip file.

Procedure

Step 1 If you have not already done so, select **Monitoring > Diagnostics** in the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface.

Step 2 Determine your next steps:

- You can generate a log file immediately without enabling detailed logging. (See Step 3.) The online help for the Health Summary page indicates when you can immediately generate a log file.
- You can enable detailed logging and attempt to reproduce the event. (See Step 4.) Enable detailed logging under the following circumstances:
  - The online help for the Health Summary page indicates that you need to attempt to reproduce the issue.
  - Your technical support team indicates that you need to enable detailed logging before you attempt to reproduce the issue; for example, the Value Added Reseller (VAR) or Cisco Technical Assistance Center (TAC) recommends that you enable detailed logging.

Caution Turning on detailed logging, which increases the trace level that is running on the Cisco Unified Communications Manager Business Edition 3000 server, impacts system performance. Only turn on detailed logging when it is recommended that you do so.

Step 3 To generate a log file immediately without enabling detailed logging, click **Generate Log File**. The generation of the log file may take awhile, so wait while the generation occurs. After the log file is generated, download the log file to your PC.

Step 4 If you need to enable detailed logging, perform the following tasks:

a. Click **Enable Logging**.

b. Attempt to reproduce the issue.

c. After you reproduce the issue or if you cannot reproduce the issue for some reason, click **Disable Logging**.

d. Generate the log file by clicking **Generate Log File**.

e. After the log file is generated, download the file to your PC.

Step 5 Send the zip file to your technical support team; for example, either the Value Added Reseller (VAR), or if you are the reseller, send it to the Cisco Technical Assistance Center (TAC).

Step 6 Work with the technical support team to analyze the log file.

Troubleshooting Using MCS 7890-C1 LEDs

The LEDs on the front of the MCS 7890-C1, as shown in Figure 46-1 on page 46-42, are color coded to indicate the status of the MCS 7890-C1.

Figure 46-1 MCS 7890-C1 LEDs

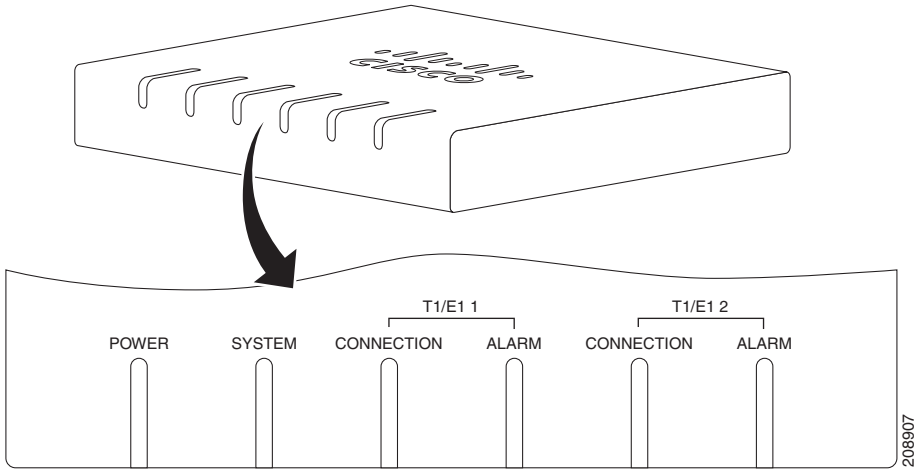

Table 46-2 describes the MCS 7890-C1 LEDs and explains their meanings.

Note The Power LED is also the front power button.

Table 46-2 MCS 7890-C1 LEDs

Name	Color	Meaning	When you see this LED, do this:
Power	Green	Power is on.	--

Table 46-2 MCS 7890-C1 LEDs (continued)

Name		Color	Meaning	When you see this LED, do this:
System **Note** This LED color matches the status information in the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface Health Summary window.		Green	MCS 7890-C1 is operating normally.	--
		Orange	Cisco Unified Communications Manager Business Edition 3000 Administrative Interface Health Summary window displays a warning.	Log in to CUCM Business Edition 3000 admin page to determine if there are any red "X" marks. If yes, check the online troubleshooting. If problem persists, reboot. If that does not resolve the issue, contact your Cisco-certified partner.
		Red blinking	Cisco Unified Communications Manager Business Edition 3000 Administrative Interface Health Summary window displays an error.	Same as above. If problem persists, reboot. If that does not resolve the issue, contact your Cisco-certified partner.
T1 / E1 1	Connection	None (LED is off.)	MCS 7890-C1 detects no carrier signal.	Ensure that the PSTN connection is correct.
		Green on	MCS 7890-C1 detects carrier signal.	--
		Yellow blinking	This port is in loopback mode.	This is not an error condition, but rather an indication that the port has been put in loopback mode for maintenance.
	Alarm	None (LED is off.)	MCS 7890-C1 detects no alarms.	--
		Yellow	The device that is sending the signal has an error.	This is due to a framing error which reports an error in the far end. Check the connection between the far end and the MCS 7890-C1.
		Red	MCS 7890-C1 detects an alarm.	The result of an MCS 7890-C1 framing error. Check the connection between the MCS 7890-C1 and the far end.

Table 46-2 MCS 7890-C1 LEDs (continued)

Name		Color	Meaning	When you see this LED, do this:
T1 / E1 2	Connection	None (LED is off.)	MCS 7890-C1 detects no carrier signal.	Same as T1/E1 1
		Green on	MCS 7890-C1 detects carrier signal.	--
		Yellow blinking	This port is in loopback mode.	Same as T1/E1 1
	Alarm	None (LED is off.)	MCS 7890-C1 detects no alarms.	Same as T1/E1 1
		Yellow	The device that is sending the signal has an error.	--
		Red	MCS 7890-C1 detects an alarm.	Same as T1/E1 1

Troubleshooting When You Cannot Access the Graphical User Interfaces

If you cannot access the GUIs, you may need to perform the following procedures, especially if your technical support team advises that you do so:

- Troubleshooting by Using Cisco Diagnostics USB, page 46-44
- Troubleshooting with the Network USB Key When You Cannot Access the Administrative Interface, page 46-47

Troubleshooting by Using Cisco Diagnostics USB

Cisco Diagnostics USB key allows you, the Value Added Reseller (VAR), to perform the servers diagnostics and collect the required log files when the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface is not accessible and before you reboot or reimage the Cisco Unified Communications Manager Business Edition 3000 server.

Cisco Diagnostics USB key contains the Cisco Diagnostics USB Signature file named **diagnose.xml** file, which can be downloaded from www.cisco.com or generated from the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface. The diagnostics starts automatically after you insert the Cisco Diagnostics USB key in Cisco Unified Communications Manager Business Edition 3000, and collects the required log files, generates a static HTML report and saves the logs and the html report to the USB key.

The Cisco Diagnostics USB Signature file consists of components for which system diagnostic is executed and associated log files are collected.

The following steps explain the USB Diagnostics process:

Procedure

Step 1 To generate the Cisco Diagnostics USB Signature file, click **Save File** in the Diagnostics page in the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface. (Select **Monitoring > Diagnostics**.)

Tip You can also obtain the Cisco Diagnostics USB Signature file, **diagnose.xml**, from www.cisco.com.

Step 2 Save the Cisco Diagnostics USB Signature file on the Cisco Diagnostics USB key.

Step 3 Insert the Cisco Diagnostics USB key on the Cisco Unified Communications Manager Business Edition 3000 server.

The system diagnostics is automatically triggered and the following components are diagnosed. Table 46-3 describes the contents on the diagnose.xml file.

Table 46-3 Scanning of System Health through Cisco Diagnostics USB Key

HardDisk	Configure the value to either **Yes** or **No**. The following system attribute is diagnosed: • Diskspace—Checks disk space and verifies critical operating system files
Network	Configure the value to either **Yes** or **No**. The following system attributes are diagnosed: • Validate Network—Validate network settings • NTP Reachability—Checks the availability of external NTP servers • NTP Clock Drift—Checks the local clocks drift from NTP servers • NTP Stratum—Checks the stratum level of the reference clock
System	Configure the value to either **Yes** or **No**. The following system attributes are diagnosed: • Service Manager—Checks if service manager is running • System Info—Collects system information into diagnostic log
WebServer	Configure the value to either **Yes** or **No**. The following system attributes are diagnosed: • Tomcat—Checks for the Tomcat process • Tomcat Deadlocks—Checks Tomcat for deadlocked threads • Tomcat Keystore—Checks Tomcat for keystore issues • Tomcat Connectors—Checks Tomcat for connector issues • Tomcat Threads—Checks Tomcat for thread issues • Tomcat Memory—Checks Tomcat for memory issues • Tomcat Sessions—Checks Tomcat for session issues
FileSystem	Configure the value to either **Yes** or **No**. The following system attributes are diagnosed: • disk_files—Checks for usually large files in root • sdl_fragmentation—Checks the fragmentation of files in SDL directory • sdi_fragmentation—Checks the fragmentation of files in SDI directory **Note** The FileSystem attributes explained above are CPU intensive diagnostics and consume substantial time for completion.
CollectLogs	Configure the value to either **none** or **min** or **max**. • none—No logs are collected. • min—Minimum number of system logs are collected. • max—Maximum number of system logs are collected.

Step 4 When the system diagnostics is completed, the following files are generated and stored on the Cisco Diagnostic USB key.

Table 46-4 describes the files that are generated after diagnostic completion.

Table 46-4 Generated Files After Diagnostic Completion

Cisco_Diagnostics_Report.html	A static HTML file that displays • System Configuration • Diagnostics Log and • Old Reports
usbdiag.log.txt	Log file generated after a USB Diagnostics
css	Cascading Style Sheet folder
archive	Collects information of the previous three diagnostic reports. It also includes a compressed image file (.tar.gz) which must be uploaded to www.cisco.com.

To troubleshoot a problem, analyze the HTML report and log files and then perform corrective action to resolve the error.

Note If the Cisco Diagnostic USB key is short of free space but has enough space to only save the static HTML report, then an error report is generated and saved in the Cisco Diagnostic USB key. This error report lists the total available free space, required space to save the logs and amount of space that must be freed manually.

If you need assistance with evaluating the diagnostic report, send the diagnostic report and logs to the Cisco TAC for further analysis.

The log files for analysis are located in the archive folder in a compressed format with **.tar.gz** extension. The archive folder contains a separate folder for each host for which the USB Diagnostics is executed. You can identify the compressed file for each host from its time and date stamp. Select the required file and upload it on www.cisco.com.

If the issue persists after rebooting, you can reimage the server as described in the "Reimaging or Replacing the Cisco Unified Communications Manager Business Edition 3000 Server" section on page 48-77. Only reimage the server when your technical support team advises that you do so.

Troubleshooting with the Network USB Key When You Cannot Access the Administrative Interface

If you cannot access the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface because your network configuration is not correct, you can use an updated configure.xml file on a USB key to set up temporary access to the network. By performing the following procedure, you can access the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface and then verify and update the network configuration. The following procedure allows you to

- Access and update the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface when the server is moved to a new network with a different subnet.
- Access and update the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface when your network configuration is not correct.

Timesaver Cisco recommends that you perform Step 1 through Step 4 before an issue occurs. If you perform these steps before an issue occurs, you can start with Step 5 if a network configuration issue is identified. If you do not perform Step 1 through Step 4 before an issue occurs, you must perform all of the steps if an issue occurs.

Perform the following procedure to use the Cisco Network Configuration USB key to obtain access to the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface:

Procedure

Step 1 Perform one of the following tasks:

- Download **configure.xml** from www.cisco.com and save it to your laptop.
- If you can access the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface, click **Save File** on the **Connections > Network** page to download the USB Network Diagnostics file (filename: configure.xml).

Step 2 Open the configure.xml file on your laptop and update its contents. Table 46-5 describes the contents of the configure.xml file.

Table 46-5 Contents of configure.xml

Parameter	Description
Configure Network	By default, the value is no. To create a temporary network interface, which assumes that you want to update the IP address, subnet mask, and the default gateway, change this value to **yes**. This temporary network interface exists along with the current configuration in the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface. The temporary network interface gets removed from the system after you restart the server.
IPAddress	Enter the appropriate IP Address based on the customer LAN. This is a mandatory requirement to change the network configuration.
SubnetMask	Enter the appropriate subnet mask of the customer LAN. This is a mandatory requirement to change the network configuration.
Gateway	Enter the default gateway details of the customer LAN. This is optional.

Step 3 Save the updated configure.xml file to the root directory of a USB key that is used exclusively for this purpose (setting up temporary access to the network).

Step 4 Remove the USB Key from the laptop. Label the USB key, and put it in a location that you will remember. For example, call it Cisco Network Configuration.

Step 5 Run diagnostics, as described in the "Troubleshooting by Using Cisco Diagnostics USB" section on page 46-44. In the diagnostics report, verify that the network information is incorrect.

Step 6 If the network information is incorrect, insert the Cisco Network Configuration USB Key in the Cisco Unified Communications Manager Business Edition 3000 server.

Note Before you insert the USB key, make sure that the server is running.

Step 7 Log in to the Cisco Unified Communications Manager Business Edition 3000 Administrative Interface by using the IP address that is in the configure.xml file.

Step 8 After you log in, verify that the network configuration is correct in the Network page (**System Settings > Network**). If necessary, update the configuration.

Step 9 Restart the server (**Maintenance > Restart/Shutdown**).

For More Information

USB Support, page 1-4

Troubleshooting Using the System LED

You, as a VAR administrator, can also monitor the health of the Cisco Unified Communications Manager Business Edition 3000 system through the status of the System LED mounted on the MCS 7890 server. This LED gives you primary information about the system health without having to access the web interface. However, you need to log in to the web interface to diagnose the problem in detail.

The System LED status will reflect the health of the following subsystems:

- System Health
- Telephony Network Gateways
- Internet Connection

The LED displays different colors depending on the health of the system. If there are no issues in the system, the LED displays solid green color. If an issue occurs in either of the subsystems, the color of the LED changes to orange or red depending on the severity of the problem.

Table 46-6 describes the various categories of the system health and the corresponding LED status:

Table 46-6 System Health Categories

System Health	LED Status	Possible Issues
Good	Solid Green	—
In Progress	Blinking Green	—

Table 46-6 System Health Categories (continued)

System Health	LED Status	Possible Issues
Warning	Solid Orange	• Insufficient disk space • Low virtual memory • DNS configured but failed to resolve
Error	Blinking Red	• One or more critical services not running • One or more ports of the internal gateway not registered • Hardware failure • System temperature, fan speed, or CPU voltage exceeding the prescribed limits

Note The status of System LED will be Blinking Green when the system is rebooting.

For information on resolving the issues mentioned above, see "Troubleshooting Issues, page 47-51".