Troubleshooting Features and Services

This chapter provides information to help you resolve common issues with Unified Communications Manager features and services.

Troubleshooting Barge

This section covers the solution for the most common issue that is related to the Barge feature.

Symptom

When the Barge softkey is pressed, the message No Conference Bridge Available displays on the IP phone.

Possible Cause

Built in Bridge setting in Phone Configuration for the target phone did not get set properly.

Corrective Action

To resolve the problem, perform the following steps:

Procedure

1. From Unified Communications Manager Administration, go to **Device** > **Phone** and click **Find the phone** to find the phone configuration of the phone that is having the problem.
2. Set the Built In Bridge parameter to **On**.
3. Click Update.
4. Reset the phone.

Troubleshooting Call Back

This section provides symptoms, possible causes, recommended actions, and error messages when Call Back does not work as expected.

Related Topics

Error Messages for Call Back, on page 4
Locating the Call Back Log Files, on page 4
Problems Using Call Back, on page 2

Problems Using Call Back

This section describes problems, possible causes, recommended actions, and error messages, if applicable to the problem.

User presses Callback softkey before phone rings

Symptom

During a call, the CallBack softkey may display on the phone, even though the phone is not ringing yet.

Possible Cause

User may not be pressing the CallBack softkey at the appropriate time.

Corrective Action

Users must press the CallBack softkey after a ringing or busy signal is received. Pressing the softkey at the wrong time may cause an error message to display on the phone.

User unplugs or resets phone after pressing the CallBack softkey but before Call Back occurs

Symptom #1

Caller phone reset occurs after CallBack softkey is pressed but before Call Back is activated.

Possible Cause

The user reset the phone.

Corrective Action #1

The caller phone does not display the Call Back activation window after the reset, and the caller must press the CallBack softkey to view the active Call Back service. Call Back notification occurs on the phone.

Symptom #2

Caller phone reset occurs after Call Back is activated but before called party becomes available.

Possible Cause

The user reset the phone.

Corrective Action #2

You do not need to perform a corrective action. If the reset occurs before the called party becomes available, Call Back occurs as expected.

Symptom #3

Caller phone reset occurs after Call Back is activated, but called party becomes available before the reset completes on the caller phone.

Possible Cause

The user reset the phone.

Corrective Action #3

CallBack notification does not occur automatically, so the caller must press the CallBack softkey to view the active Call Back service.

Caller misses availability notification before phone reset. Replace/retain screen does not explicitly state that availability notification occurred.

Symptom

In an intracluster or intercluster call back scenario, a caller initiates Call Back for a user, for example, user B, who is unavailable. When user B becomes available, the availability notification screen displays on the caller phone, and a tone plays. The caller misses the availability notification for some reason, and the phone resets.

The caller contacts a different user, user C, for example, and presses the CallBack softkey because user C appears busy. The replace/retain screen displays on the caller phone, but the screen does not state that the availability notification already occurred for user B.

Possible Cause

The user reset the phone.

Corrective Action

After a phone reset but not during an active call, review the call back notifications on the phone. Press the CallBack softkey.

Error Messages for Call Back

This section provides a list of error messages that may display on the phone.

Error Message `Call Back is not active. Press Exit to quit this screen.`

Explanation User presses the CallBack softkey during the idle state.

Recommended Action The error message provides the recommended action.

Error Message `CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit this screen.`

Explanation A user tried to activate Call Back, but it is already active.

Recommended Action The error message provides the recommended action.

Error Message `CallBack cannot be activated for xxxx.`

Explanation A user tried to activate Call Back, and the extension is not found in the database.

Recommended Action The user must try again, or the administrator must add the directory number to Unified Communications Manager Administration.

Error Message `Service is not active.`

Explanation You set the Callback Enabled Flag service parameter to **False**, which means that the feature remains disabled.

Recommended Action For the Call Back feature, configure the Cisco CallManager service parameter, Callback Enabled Flag, to **True**.

Locating the Call Back Log Files

Traces for the Call Back feature exist as Unified Communications Manager and CTIManager SDL and SDI records. To access the traces, refer to the *Cisco Unified Serviceability Administration Guide*.

Troubleshooting Call Control Discovery

The following alarms support the call control discovery feature. To access the alarm definitions in Cisco Unified Serviceability, choose **Alarm** > **Definitions**. The alarms support the CallManager alarm catalog (choose **CallManager Alarm Catalog** > **CallManager**).

- SAFUnknownService
  - Informational alarm
  - Unified Communications Manager does not recognize the service ID in a publish revoke or withdrawal message that the SAF forwarder issued.
- SAFPublishRevoke
  - Informational alarm

    - You issued a CLI command on the SAF Forwarder router to revoke the publish action for the service or subservice ID that is specified in this alarm.

- DuplicateLearnedPattern
    - Error alarm
    - The call control discovery requesting service received the same hosted DN from multiple remote call-control entities. The parameter, Issue Alarm for Duplicate Learned Patterns, controls whether this alarm gets issued.
    - In RTMT, open the Learned Pattern report and find the duplicate pattern that is specified in this alarm. Ensure that the learned patterns are unique. Determine which remote call-control entity needs to be changed so duplicate patterns do not exist.

- CCDIPReachableTimeOut
    - Error Alarm
    - The CCD requesting service detected that it can no longer reach the learned patterns through IP. All learned patterns from this SAF forwarder get marked as unreachable (via IP), and all calls to learned patterns get routed through the PSTN. Calls get routed through the PSTN for a specific amount of time before PSTN failover times out.
    - Check IP connectivity and resolve any TCP or IP problems in the network.

- CCDPSTNFailOverDurationTimeOut
    - Error Alarm
    - When learned patterns are not reachable through IP, Unified Communications Manager routes calls through the PSTN. When this alarm occurs, the PSTN failover duration has expired, and calls to learned patterns cannot be routed. All learned patterns get purged from Unified Communications Manager.
    - Troubleshoot your network to get IP connectivity restored. After IP connectivity is restored, Unified Communications Manager automatically relearns patterns and calls to learned patterns automatically proceed through IP.

- CCDLearnedPatternLimitReached
    - Warning Alarm
    - This alarm indicates that the CCD requesting service has met the maximum number of allowed learned patterns.
    - This alarm displays the value that is configured for the parameter, CCD Maximum Numbers of Learned Patterns, as well as the maximum number of learned patterns that are allowed by the system (20,000). Consider whether the specified maximum number of learned patterns is correct for your deployment. If the value is too low, compare it with the number that displays in the SystemLimitCCDLearnedPatterns in this alarm. If the maximum number is below the system limit, which is 20,000 learned patterns, increase the value for the CCD Maximum Numbers of Learned Patterns parameter.

- LostConnectionToSAFForwarder

- Error alarm
- A TCP connection failure caused the connection between the SAF forwarder and Unified Communications Manager to be lost. When the TCP connection is restored, Unified Communications Manager attempts to connect to the SAF forwarder automatically. If IP connectivity is unreachable for longer than the duration of the CCDLearnedPatternIPReachableDuration feature parameter, calls to learned patterns get routed through PSTN instead of through IP. Calls through PSTN to learned patterns get maintained for a specific period of time before PSTN failover times out.
- Investigate possible causes of a TCP connection failure, such as power failure, loose cables, incorrect switch configuration, and so on.

- SAFForwarderError
  - Unified Communications Manager received an error from the SAF forwarder.
  - Refer to the reason code and description for specific information and actions (where applicable) about the reason that this alarm occurred.

    For example, reason code 472 indicates that the external client, in this case, Unified Communications Manager, did not increment the service version number correctly. For example, reason code 474 indicates that the external client, in this case, Unified Communications Manager, sent a publishing request over a TCP connection to the SAF forwarder before the client registers to the forwarder. For example, reason code 400 indicates that the external client, in this case, Unified Communications Manager, did not construct the SAF message correctly.

Troubleshooting Call Park

The following table provides troubleshooting recovery tips for common call park problems.

Table 1: Troubleshooting Tips for Call Park

Problem Description	Recommended Action
User cannot park calls. When the user presses the Park softkey or feature button, the call does not get parked.	Ensure that a unique call park number is assigned to each Unified Communications Manager in the cluster. See the System Configuration Guide for Cisco Unified Communications Manager. The partition that is assigned to the call park number does not match the partition that is assigned to the phone directory number. See the System Configuration Guide for Cisco Unified Communications Manager.
The call park number does not display long enough for the user.	Set the Call Park Display Timer to a longer duration. For information on setting parameters for call park, see the System Configuration Guide for Cisco Unified Communications Manager.

Troubleshooting Ciphers

The Cipher Management page has no default values. Instead, the Cipher Management feature takes effect only when you configure Ciphers.

For information about Ciphers, see Security Guide for Cisco Unified Communications Manager

This section provides information to help you troubleshoot problems with Unified Communications Manager Ciphers:

Troubleshooting DRS and CDR Functionality

Symptom

Breakage to DRS and CDR functionality.

Possible Cause

Configuring `hmac-sha2-512` in SSH MAC interface affects the DRS and CDR functionality.

Configuring Ciphers

- `aes128-gcm@openssh.com`
- `aes256-gcm@openssh.com`

in **SSH Cipher's** field or configuring only `ecdh-sha2-nistp256` algorithm in "SSH KEX" breaks the DRS and CDR functionalities.

Recommended Action

1. From Cisco Unified OS Administration, choose **Security** > **Cipher Management**
2. Remove or Delete the above mentioned ciphers if they are already configured and **Save** the settings.
3. Reboot the server for the changes to take effect.

Troubleshooting Cisco Extension Mobility

Cisco Extension Mobility provides troubleshooting tools for the administrator. These tools include performance counters (also known as perfmons) and alarms that are part of Cisco Unified Serviceability. For information about performance counters (perfmons), refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about alarms, refer to the *Cisco Unified Serviceability Administration Guide*.

This section provides information to help you troubleshoot problems with Cisco Communications Manager Extension Mobility:

Related Topics

Troubleshooting Cisco Extension Mobility Error Messages, on page 8
Troubleshooting General Problems with Cisco Extension Mobility, on page 8

Troubleshooting General Problems with Cisco Extension Mobility

If any problems occur with Cisco Extension Mobility, start with these troubleshooting tips:

- Configure the Cisco Extension Mobility trace directory and enable debug tracing by performing the following procedures:
  - From Cisco Unified Serviceability, choose **Trace > Trace Configuration**
  - From the Servers drop-down list, choose a server.
  - From the drop-down menu of Configured Services, choose **Cisco Extension Mobility**.
- Make sure that you entered the correct URL for the Cisco Extension Mobility service. Remember that the URL is case sensitive.
- Check that you have thoroughly and correctly performed all the configuration procedures.
- If a problem occurs with authentication of a Cisco Extension Mobility user, go to the user pages and verify the PIN.

If you are still having problems, use the troubleshooting solutions in the following table.

Table 2: Troubleshooting Cisco Unified Communications Manager Extension Mobility

Problem Description	Recommended Action
After a user logs out and the phone reverts to the default device profile, the user finds that the phone services are no longer available.	**1.** Check the Enterprise Parameters to make sure that the Synchronization Between Auto Device Profile and Phone Configuration is set to **True**. **2.** Subscribe the phone to the Cisco Extension Mobility service.
After logging in, the user finds that the phone services are not available.	This problem occurs because the User Profile did not have any services that were associated with it when the profile was loaded on the phone. Perform the following steps: **1.** Change the User Profile to include the Cisco Extension Mobility service. **2.** Change the phone configuration where the user is logged in to include Cisco Extension Mobility. After the phone is updated, the user can access the phone services.
After performing a login or logout, the user finds that the phone resets instead of restarting.	Locale change may provide the basis for reset. If the User Locale that is associated with the login user or profile is not the same as the locale or device, after a successful login, the phone will perform a restart that is followed by a reset. This occurs because the phone configuration file is being rebuilt.

Troubleshooting Cisco Extension Mobility Error Messages

Use the information in the following table to troubleshoot the error codes and error messages that display on the phone when Cisco Extension Mobility is used.

Table 3: Troubleshooting Error Messages That Display on the Phone

Error Code	Message on Phone	Recommended Action
201	[201]-Authentication error	The user should check that the correct UserID and PIN were entered; the user should check with the system administrator that the UserID and PIN are correct.
22	[22]-Dev.logon disabled	Make sure that you have chosen "Enable Extension Mobility" check box on the Phone Configuration window. Refer to the Feature Configuration Guide for Cisco Unified Communications Manager.
205	[205]-User Profile Absent	Make sure that you have associated a Device Profile to the user Feature Configuration Guide for Cisco Unified Communications Manager.
208	[208]-EMService Conn. error	Verify that the Cisco Extension Mobility service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.
25	[25]-User logged in elsewhe..	Check whether the user is logged in to another phone. If multiple logins need to be allowed, ensure the Multiple Login Behavior service parameter is set to Multiple Logins Allowed.
	Host not found	Check that the Cisco Tomcat service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Network Services**.
	Http Error [503]	If you get this error when Services button is pressed, check that the Cisco Communications Manager Cisco IP Phone Services service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Network Services**. If you get this error when you select Extension Mobility service, check that the Cisco Extension Mobility Application service is running by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Network Services**.
202	[202]-Blank userid or pin	Enter a valid userid and PIN.
26	[26]- Busy, please try again	Check whether the number of concurrent login/logout requests is greater than the Maximum Concurrent requests service parameter. If so, lower the number of concurrent requests. To verify the number of concurrent login/logout requests, use Unified Communications Manager Cisco Unified Real-Time Monitoring Tool to view the Requests In Progress counter in the Extension Mobility object.
6	[6]-Database Error	Check whether a large number of requests exists If large number of requests exists, the Requests In Progress counter in the Extension Mobility object counter specifies a high value. If the requests are rejected due to large number of concurrent requests, the Requests Throttled counter also specifies a high value. Collect detailed database logs.

Error Code	Message on Phone	Recommended Action
207	[207]-Device Name Empty	Check that the URL that is configured for Cisco Extension Mobility is correct.

Troubleshooting Cisco Unified Communications Manager Assistant

This section covers solutions for the most common issues that relate to Cisco Unified Communications Manager Assistant.

The following table describes troubleshooting tools for Unified CM Assistant and the client desktop.

Table 4: Cisco Unified Communications Manager Assistant Troubleshooting Tools and Client Desktop

Tool Description	Location
Cisco UnifiedCM Assistant server trace files	The log files reside on the server that runs the Cisco IP Manager Assistant service. You can download these files from the server by using one of the following methods: • Use the CLI command: **file get activelog tomcat/logs/ipma/log4j** • Use the trace collection features in the Unified CM Cisco Unified Real-Time Monitoring Tool (RTMT). Refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for more information. You can enable debug tracing by choosing **Cisco Unified Serviceability** > **Trace** > **Configuration**.
Cisco IPMA client trace files	`$INSTALL_DIR\logs\ACLog*.txt` on the client desktop in the same location where the Unified CM Assistant assistant console resides. To enable debug tracing, go to the settings dialog box in the assistant console. In the advanced panel, check the Enable Trace check box. **Note** This enables only debug tracing. Error tracing always remains On.
Cisco IPMA client install trace files	`$INSTALL_DIR\InstallLog.txt` on the client desktop in the same location where the Unified CM Assistant assistant console resides.
Cisco IPMA Client AutoUpdater trace files	`$INSTALL_DIR\UpdatedLog.txt` on the client desktop in the same location where the Unified CM Assistant assistant console resides.
Install directory	By default—`C:\Program Files\Cisco\Unified Communications Manager Assistant Console\`

Related Topics

IPMAConsoleInstall.jsp Displays Error: HTTP Status 503-This Application is Not Currently Available, on page 11
IPMAConsoleInstall.jsp Displays Error: No Page Found Error, on page 11
Exception: java.lang.ClassNotFoundException: InstallerApplet.class, on page 12
Automatic Installation of MS Virtual Machine Is No Longer Provided for Download, on page 12
User Authentication Fails, on page 13
Assistant Console Displays Error: System Error - Contact System Administrator, on page 13
Assistant Console Displays Error: Cisco IP Manager Assistant Service Unreachable, on page 14
Calls Do Not Get Routed When Filtering Is On or Off, on page 15
Cisco IP Manager Assistant Service Cannot Initialize, on page 16
Calling Party Gets a Reorder Tone, on page 17
Manager Is Logged Out While the Service Is Still Running, on page 17
Manager Cannot Intercept Calls That Are Ringing on the Assistant Proxy Line, on page 18
Not Able to Call the Manager Phone When Cisco IP Manager Assistant Service is Down, on page 18

IPMAConsoleInstall.jsp Displays Error: HTTP Status 503-This Application is Not Currently Available

Symptom

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp` displays the following error message:

HTTP Status 503—This application is not currently available

Possible Cause

Cisco IP Manager Assistant service has not been activated or is not running.

Corrective Action

Make sure that the Cisco IP Manager Assistant service has been activated by checking the activation status of the service at **Cisco Unified Serviceability** > **Tools** > **Service Activation**.

If the Cisco IP Manager Assistant service has been activated, restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

IPMAConsoleInstall.jsp Displays Error: No Page Found Error

Symptom

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp` displays the following error message:

No Page Found Error

Possible Cause #1

Network problems.

Corrective Action #1

Ensure that the client has connectivity to the server. Ping the server name that is specified in the URL and verify that it is reachable.

Possible Cause #2

Misspelled URL.

Corrective Action #2

Because URLs are case sensitive, ensure that the URL matches exactly what is in the instructions.

Related Topics

Cisco Unified Communications Manager System Issues

Exception: java.lang.ClassNotFoundException: InstallerApplet.class

Symptom

The assistant console fails to install from the web. The following message displays:

Exception: java.lang.ClassNotFoundException: InstallerApplet.class

Possible Cause

Using the Sun Java plug-in virtual machine instead of the Microsoft JVM with the standard Unified Communications Manager Assistant Console install causes failures.

Corrective Action

The administrator directs the user to the following URL, which is a JSP page that supports the Sun Java plug-in: `https://<servername>:8443/ma/Install/IPMAConsoleInstallJar.jsp`

Automatic Installation of MS Virtual Machine Is No Longer Provided for Download

Symptom

The Assistant Console fails to install from the web when you are trying to install on a computer that is running Microsoft Windows XP. A message displays that all the components for the program are not available. When the user chooses Download Now, the following message displays:

Automatic installation of MS Virtual Machine is no longer available for download

Possible Cause

Microsoft does not support Microsoft JVM in IE version 6 of Windows XP.

Note This error does not occur if you have the Microsoft JVM with XP Service Pack 1 installed on your system.

Corrective Action

Perform one of the following corrective actions:

- Install the Netscape browser (version 7.x) and use Netscape to install the assistant console.
- Install the Sun Java Virtual Machine plug-in for IE from the following URL:

  `http://java.sun.com/getjava/download.html`

  When the Sun Java plug-in completes installation, point the browser at the following URL:

  `https://<servername>:8443/ma/Install/IPMAInstallJar.jsp`
- Install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the assistant console installation.

User Authentication Fails

Symptom

User authentication fails when you sign in on the login window from the assistant console.

Possible Cause

The following probable causes can apply:

- Incorrect administration of the user in the database.
- Incorrect administration of the user as an assistant or a manager.

Corrective Action

Ensure that the user ID and the password are administered as a Unified Communications Manager user through Unified Communications Manager.

You must administer the user as an assistant or a manager by associating the Unified Communications Manager Assistant user information, which you access through **Unified Communications Manager Administration** > **User Management** > **End User**.

Assistant Console Displays Error: System Error - Contact System Administrator

Symptom

After launching the Assistant Console, the following message displays:

System Error - Contact System Administrator

Possible Cause #1

You may have upgraded the Unified Communications Manager from 4.x release to a 5.x release. The system cannot automatically upgrade the assistant console from 4.x release to 5.x release.

Corrective Action #1

Uninstall the console by choosing **Start > Programs > Unified Communications Manager Assistant > Uninstall Assistant Console** and reinstall the console from URL `https://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp`.

Possible Cause #2

The user did not get configured correctly in the database.

Corrective Action #2

Ensure that the user ID and the password are administered as a Unified Communications Manager user through Cisco Unified Communications Manager Administration.

You must administer the user as an assistant or a manager by associating the Cisco Unified Communications Manager Assistant user information, which you access through **Unified Communications Manager Assistant** > **User Management** > **End User**. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Possible Cause #3

When you deleted a manager from an assistant, Cisco Unified Communications Manager AdministrationCisco Unified Communications Manager Administration left a blank line for the assistant.

Corrective Action #3

From the Assistant Configuration window, reassign the proxy lines. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Assistant Console Displays Error: Cisco IP Manager Assistant Service Unreachable

Symptom

After launching the assistant console, the following message displays:

Cisco IPMA Service Unreachable

Probable Cause #1

Cisco IP Manager Assistant service may have stopped.

Corrective Action #1

Restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #2

The server address for the Primary and Secondary Cisco Unified Communications Manager Assistant servers may be configured as DNS names, but the DNS names are not configured in the DNS server.

Corrective Action #2

Use the following procedure to replace the DNS name.

Procedure

1. Choose **Unified Communications Manager Administration** > **System** > **Server**.
2. Replace the DNS name of the server with the corresponding IP address.
3. Restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #3

The *Cisco CTI Manager* service may have stopped.

Corrective Action #3

Restart the *Cisco CTI Manager* and *Cisco IP Manager Assistant* services by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Probable Cause #4

The Cisco Unified Communications Manager Assistant service might have been configured to open a CTI connection in secure mode, but the security configuration may not be complete.

If this occurs, the following message displays in the alarm viewer or in the Cisco Unified Communications Manager Assistant service logs:

IPMA Service cannot initialize - Could not get Provider.

Corrective Action #4

Check the security configuration in the service parameters of *Cisco IP Manager Assistant* service. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Restart the Cisco Unified Communications Manager Assistant by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Calls Do Not Get Routed When Filtering Is On or Off

Symptom

Calls do not get routed properly.

Possible Cause #1

Cisco CTI Manager service may have stopped.

Corrective Action #1

Restart the *Cisco CTI Manager* and *Cisco IP Manager Assistant* services by choosing **Cisco Unified Serviceability > Tools > Control Center—Feature Services**.

Possible Cause #2

The Unified Communications Manager route point did not get configured properly.

Corrective Action #2

Use wild cards to match the directory number of the Unified Communications Manager CTI route point and the primary directory numbers of all managers that are configured for Unified Communications Manager.

Possible Cause #3

The status window on the manager phone displays the message, Filtering Down. This can indicate that Unified Communications Manager Assistant CTI route point may be deleted or may not be in service.

Corrective Action #3

Use the following procedure to configure the CTI route point and restart the *Cisco IP Manager Assistant* service.

Procedure

1. From Unified Communications Manager, choose **Device** > **CTI Route Point**.
2. Find the route point, or add a new route point. See System Configuration Guide for Cisco Unified Communications Manager for configuration details.
3. Restart the Cisco IP Manager Assistant services by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Cisco IP Manager Assistant Service Cannot Initialize

Symptom

The *Cisco IP Manager Assistant* service cannot open a connection to CTI Manager, and the following message displays:

IPMA Service cannot initialize - Could not get Provider.

Possible Cause

The *Cisco IP Manager Assistant* service cannot open a connection to CTIManager. You can see the message in the alarm viewer or in the Cisco Unified Communications Manager Assistant service logs.

Corrective Action

Restart the Cisco CTI Manager and *Cisco IP Manager Assistant* services by choosing **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Calling Party Gets a Reorder Tone

Symptom

Calling party gets a reorder tone or a message: “This call cannot be completed as dialed.”

Possible Cause

You may not have configured the calling search space of the calling line correctly.

Corrective Action

Check the calling search space of the line. For the configuration details, see the System Configuration Guide for Cisco Unified Communications Manager.

You can also use the Cisco *Dialed Number Analyzer* service to check any flaws in the calling search space. For more details, see *Cisco Unified Communications Manager Dialed Number Analyzer Guide* for more details.

Manager Is Logged Out While the Service Is Still Running

Symptom

Although the manager is logged out of Unified Communications Manager Assistant, the service still runs. The display on the manager IP phone disappears. Calls do not get routed, although filtering is on. To verify that the manager is logged out, view the application log by using the Cisco Unified Real-Time Monitoring Tool. Look for a warning from the Cisco Java Applications that indicates that the Cisco IP Manager Assistant service logged out.

Possible Cause

The manager pressed the softkeys more than four times per second (maximum limit allowed).

Corrective Action

The Unified Communications Manager administrator must update the manager configuration. Perform the following procedure to correct the problem.

Procedure Action

1. From Unified Communications Manager Administration, choose **User Management** > **End User**.

   The Find and List Users window displays.
2. Enter the manager name in the search field and click the **Find**.
3. Choose the manager from the results list that you want to update.

   The End User Configuration window displays.
4. From the Related Links drop-down list box, choose **Cisco IPMA Manager** and click **Go**.
5. Make the necessary changes to the manager configuration and click **Update**.

Manager Cannot Intercept Calls That Are Ringing on the Assistant Proxy Line

Symptom

The manager cannot intercept the calls that are ringing on the assistant proxy line.

Possible Cause

The calling search space of the proxy line did not get configured properly.

Corrective Action

Check the calling search space of the proxy line for the assistant phone. Perform the following procedure to correct the problem.

Procedure Action

1. From Unified Communications Manager Administration , choose **Device > Phone**.

   The Find and List Phones search window displays.

2. Click the assistant phone.

   The Phone Configuration window displays.

3. Verify the calling search space configuration for the phone and for the directory number (line) and update as appropriate.

Not Able to Call the Manager Phone When Cisco IP Manager Assistant Service is Down

Symptom

Calls do not get routed properly to managers when Cisco IP Manager Assistant service goes down.

Possible Cause

The Cisco Unified Communications Manager Assistant CTI route point did not get enabled for Call Forward No Answer.

Corrective Action

Perform the following procedure to properly configure the Cisco Unified Communications Manager Assistant route point.

Procedure Action

1. From Cisco Unified Communications Manager Administration, choose **Device** > **CTI Route Point**.

   The Find and List CTI Route Point search window displays.

2. Click the **Find** button.

A list of configured CTI Route Points display.

3. Choose the Cisco Unified Communications Manager Assistant CTI route point that you want to update.
4. In the CTI Route Point Configuration window, click the line to update from the Directory Numbers box.

   The Directory Number Configuration window displays.
5. In the Call Forward and Pickup Settings section, check the Forward No Answer Internal and/or the Forward No Answer External check box and enter the CTI route point DN in the Coverage/Destination field (for example, CFNA as 1xxx for the route point DN 1xxx).
6. In the Calling Search Space drop-down list, choose CSS-M-E (or appropriate calling search space).
7. Click the **Update**.

Troubleshooting Cisco Unified Mobility

This section provides information to help you troubleshoot problems with Cisco Unified Mobility.

Related Topics

Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot Resume Call on Desktop Phone, on page 19
Dial-via-Office-Related SIP Error Codes, on page 20

Cisco Unified Mobility User Hangs Up Mobile Phone But Cannot Resume Call on Desktop Phone

Symptom

When a remote destination (mobile phone) is not a smart phone and a call to this mobile phone is anchored through Unified Communications Manager, the user can hang up the mobile phone and expect to see a **Resume** softkey on the user desktop phone to resume the call. The user cannot resume this call on the user desktop phone.

Possible Cause

If the calling party receives busy/reorder/disconnect tone when the mobile phone hangs up, the mobile phone provider probably did not disconnect the media. Unified Communications Manager cannot recognize this circumstance, because no disconnect signals came from the provider. To verify whether this is the case, let the calling party wait 45 seconds, when service provider will time out and send disconnect signals, upon which Unified Communications Manager can provide a **Resume** softkey to resume the call.

Recommended Action

Perform the following actions:

- Add the following command to the gateway:

  voice call disc-pi-off

- For the Cisco CallManager service, set the Retain Media on Disconnect with PI for Active Call service parameter to False.

Dial-via-Office-Related SIP Error Codes

Symptom

A Cisco Unified Mobility Dial-via-Office (DVO) call does not succeed.

Possible Cause

Unified Communications Manager provides specific SIP error codes when a dial-via-office call does not succeed. The following table provides the SIP error codes for unsuccessful dial-via-office calls.

Call Scenario	SIP Error Code
Target number is not routable.	404 Not Found
Target is busy.	486 Busy Here
Cisco Unified Mobile Communicator hangs up before target answers.	487 Request Terminated
Cisco Unified Mobile Communicator sends SIP CANCEL.	487 Request Terminated
Cisco Unified Mobile Communicator tries to make a call without successful registration.	503 Service Unavailable
Cisco Unified Mobile Communicator tries to make a call when there are already two outstanding calls on the enterprise line.	486 Busy Here
Cisco Unified Mobile Communicator tries to make a DVO-F call when there is an outstanding pending DVO-F call (awaiting PSTN call).	487 Request Terminated (on the first call)

Additional Documentation

For more information about configuring the Cisco Unified Mobile Communicator to operate with Unified Communications Manager, see the following documents:

- "Configuring Unified Communications Manager for Use With Cisco Unified Mobility Advantage" chapter in *Installing and Configuring Cisco Unified Mobility Advantage* at *http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html*
- *Configuring Features in Cisco Unified Mobility Advantage: Dial Via Office* at *http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html*

Troubleshooting Cisco Web Dialer

This section covers error messages for the most common issues that relate to Cisco Web Dialer.

Related Topics

Authentication Error, on page 21
Cisco CTIManager Down, on page 22
Destination Not Reachable, on page 23
Directory Service Down, on page 22
Failed to Open Device/Line, on page 23
Service Temporarily Unavailable, on page 21
Session Expired, Please Login Again, on page 22
User Not Logged in on Any Device, on page 23

Authentication Error

Symptom

Cisco Web Dialer displays the following message:

Authentication failed, please try again.

Probable Cause

User entered wrong userID or password

Corrective Action

Check your userID and password. You must log in by using your Unified Communications Manager userID and password.

Service Temporarily Unavailable

Symptom

Cisco Web Dialer displays the following message:

Service temporarily unavailable, please try again later.

Possible Cause

The Cisco CallManager service got overloaded because it has reached its throttling limit of three concurrent CTI sessions.

Corrective Action

After a short time, retry your connection.

Directory Service Down

Symptom

Cisco Web Dialer displays the following message:

Service temporarily unavailable, please try again later: Directory service down.

Possible Cause

The Cisco Communications Manager directory service may be down.

Corrective Action

After a short time, retry your connection.

Cisco CTIManager Down

Symptom

Cisco Web Dialer displays the following message:

Service temporarily unavailable, please try again later: Cisco CTIManager down.

Possible Cause

Cisco CTIManager service that is configured for Cisco Web Dialer went down.

Corrective Action

After a short time, retry your connection.

Session Expired, Please Login Again

Symptom

Cisco Web Dialer displays the following message:

Session expired, please login again.

Possible Cause

A Cisco Web Dialer session expires

- After the Web Dialer servlet gets configured or
- If the Cisco Tomcat Service is restarted.

Corrective Action

Log in by using your Unified Communications Manager userID and password.

User Not Logged in on Any Device

Symptom

Cisco Web Dialer displays the following message:

User not logged in on any device.

Possible Cause

The user chooses to use Cisco Extension Mobility from the Cisco Web Dialer preference window but does not get logged in to any IP phone.

Corrective Action

- Log in to a phone before using Cisco Web Dialer.
- Choose a device from the Cisco Web Dialer preference list in the dialog box instead of choosing the option **Use Extension Mobility**.

Failed to Open Device/Line

Symptom

After a user attempts to make a call, Cisco Web Dialer displays the following message:

User not logged in on any device.

Possible Cause

- The user chose a Cisco Unified IP Phone that is not registered with Unified Communications Manager. For example, the user chooses a Cisco IP SoftPhone as the preferred device before starting the application.
- The user who has a new phone chooses an old phone that is no longer in service.

Corrective Action

Choose a phone that is in service and is registered with Unified Communications Manager.

Destination Not Reachable

Symptom

Cisco Web Dialer displays the following message on the End Call window:

Destination not reachable.

Possible Cause

- User dialed the wrong number.
- The correct dial rules did not get applied. For example, the user dials 5550100 instead of 95550100.

Corrective Action

Check the dial rules.

Troubleshooting Directed Call Park

The following table provides troubleshooting recovery tips for common directed call park problems.

Table 5: Troubleshooting Tips for Directed Call Park

Problem Description	Recommended Action
User cannot park calls. After the Transfer softkey (or Transfer button if available) is pressed and the directed call park number is dialed, the call does not get parked.	Ensure that the partition that is assigned to the call park number matches the partition that is assigned to the phone directory number. See the . Ensure that the partition and calling search space are configured correctly for the device. See the .
User cannot park calls. After pressing the Transfer softkey (or Transfer button if available) and dialing the directed call park number, the user receives a busy tone, and the IP phone displays the message, Park Slot Unavailable.	Ensure that the dialed directed call park number is not already occupied by a parked call or park the call on a different directed call park number.
User cannot park calls. After pressing the Transfer softkey (or Transfer button if available) and dialing the directed call park number, the user receives a reorder tone or announcement.	Ensure that the dialed number is configured as a directed call park number. See the Feature Configuration Guide for Cisco Unified Communications Manager.
Parked calls revert too quickly.	Set the Call Park Reversion Timer to a longer duration. See the Feature Configuration Guide for Cisco Unified Communications Manager
User cannot park calls. The user receives a reorder tone after the reversion timer expires.	Ensure that the user presses the Transfer softkey (or Transfer button if available) before dialing the directed call park number, then presses the Transfer softkey (or Transfer button) again or goes on hook after dialing the directed call park number. Because directed call park is a transfer function, the directed call park number cannot be dialed alone. See the Feature Configuration Guide for Cisco Unified Communications Manager **Note** You can complete the transfer only by going on hook rather than pressing the Transfer softkey (or Transfer button) a second time if the Transfer On-hook Enabled service parameter is set to True. See the Feature Configuration Guide for Cisco Unified Communications Manager.
User cannot retrieve parked calls. After dialing the directed call park number to retrieve a parked call, the user receives a busy tone, and the IP phone displays the message, Park Slot Unavailable.	Ensure that the user dials the retrieval prefix followed by the directed call park number. See the Feature Configuration Guide for Cisco Unified Communications Manager.

Problem Description	Recommended Action
Parked calls do not revert to the number that parked the call.	Check the configuration of the directed call park number to ensure that it is configured to revert to the number that parked the call rather than to a different directory number. See the Feature Configuration Guide for Cisco Unified Communications Manager.
When an attempt is made to delete a directed call park number or range, a message displays that indicates that the number or range cannot be deleted because it is in use.	You cannot delete a directed call park number that a device is configured to monitor (by using the BLF button). To determine which devices are using the number, click the Dependency Records link on the Directed Call Park Configuration window.
After configuring a range of directed call park numbers, user cannot park a call at a number within the range.	Review the syntax for entering a range of directed call park numbers. If incorrect syntax is used, the system may appear to configure the range when it actually does not. See the Feature Configuration Guide for Cisco Unified Communications Manager.

Troubleshooting External Call Control

This section describes how to handle some common external call control issues.

Unified Communications Manager cannot connect to the adjunct route server.

- The URI in the External Call Control Profile window in Cisco Unified Communications Manager Administration is not correct. (**Call Routing** > **External Call Control**)
  - Verify the URI for the adjunct route server. Ensure that the URI uses the following formula:

    ```
    https://<hostnameor IPv4 address of route server>:<port that is
    configured on route server>/path from route server configuration
    ```

  - If the adjunct route server uses https, verify that you imported and exported the required certificates, as described in the “External Call Control” chapter in the System Configuration Guide for Cisco Unified Communications Manager.
  - If the adjunct route server uses https, verify that hostname that you enter for the URI for the Primary Web Service and Secondary Web Services fields in the External Call Control Profile window in Cisco Unified Communications Manager Administration matches the hostname that is in the adjunct route server certificate.
- Network connectivity dropped between Unified Communications Manager and the adjunct route server. Because the Connection Loss and PDP Out Of Service counters are incrementing counters, they indicate that at one time good connections were made to the adjunct route server. Therefore, an event in the network caused the problem, or an event occurred on the adjunct route server.
  - Verify that the adjunct route server is running and that network connectivity is good.
- Unified Communications Manager routing query to the adjunct route server times out because of slow response from the adjunct route server. The adjunct route server may be overloaded because of processing service requests, or network instability occurred.

- Increase the value for the Routing Request Timer in the external call control profile, or increase the value for the External Call Control Routing Request Timer service parameter.
- Increase the value for the External Call Control Maximum Connection Count To PDP service parameter.
- Add a secondary web service (redundant adjunct route server) in the external call control profile and enable load balancing in the profile.

- The Unified Communications Manager routing request failed when Unified Communications Manager failed to parse the routing directive from the adjunct route server.
  - Verify that the XACML or CIXML is correctly formatted. Both the XACML request and response display in the Cisco CallManager SDI trace. The routing response code for each routing request exists in the trace. A value of 0 means the request was received and parsed correctly.

Call failed due to exceed maximum diversion hops or maximum diversion hops to the same translation pattern.

- A caller receives reorder tone.
- Check the Cisco CallManager SDI trace. For example, if the External Call Control Diversion Maximum Hop Count service parameter is 12. the Cisco CallManager SDI trace shows:

```
PER_RoutingCallInfo::isCallDiversionMaximumHopCountExceeded:
callDiversionHopCount(12) >= CallDiversionMaximumHopCountLimit(12)
```

- For example, if the Maximum External Call Control Diversion Hops to Pattern or DN service parameter is 12, the Cisco CallManager SDI trace shows:

```
PER_RoutingCallInfo::isCallDiversionMaximumHopToSamePatternCountExceeded:
CallDiversionHopToSamePatternCount(12) >=
CallDiversionMaximumHopToSamePatternCountLimit(12)
```

- Verify the service parameter configuration, and change, if necessary.
- Verify the obligation configuration on the adjunct route server for call redirection. For example, A calls B; the route for B indicates to divert A to C; the route for C says indicates to divert A to D. D has CFA enabled to E. The route for E says to divert to A to F, and so on.

Unified Communications Manager cannot parse the call routing directives, mandatory parameters, or XACML from the adjunct route server.

- RTMT show the error alarm, ErrorParsingDirectiveFromPDP. This alarm contains one of following reasons.
  - Error parsing the route decision from adjunct route server.
  - The route decision from the adjunct route server is indeterminate.
  - The route decision from adjunct route server is not applicable.

Tip For the preceding bullets, check the adjunct route server route rule and configuration. Unified Communications Manager routes the call based on the failure treatment.

- An adjunct route server diverts a call without a destination in the obligation.

Tip Check the obligation configuration on the adjunct route server. The obligation should have a destination for the call routing directive = divert.

- Call was denied. The adjunct route server denies a call, but the CIXML response contains an obligation other than reject.

Tip On the adjunct route server, check that the obligation for the call routing directive = reject. The preceding bullet supports the case where the route is deny, but the obligation is not reject.

Unified Communications Manager failed to parse one or multiple optional attributes in a call routing response from the adjunct route server.

- RTMT displays the warning alarm, ErrorParsingResponseFromPDP. This alarm contains one or combination of following reasons depending on whether there is one or multiple errors.
  - Request Processing Error—Check adjunct route server trace for error.
  - XACML Syntax Error—Check the route configuration on the adjunct route server.
  - CIXML Missing Optional Attribute—Check obligation configuration on the adjunct route server.
  - CIXML Syntax Error—Check obligation configuration on the adjunct route server.
  - Invalid announcement Id—Check obligation configuration on the adjunct route server.

Unified Communications Manager cannot fulfill a call routing directive returned by the adjunct route server because of Unified Communications Manager feature interaction and/or Unified Communications Manager configuration.

- Unified Communications Manager cannot fulfill a call routing directive. Unified Communications Manager cannot route a call to a destination. A caller receives reorder tone. A caller does not receive announcement. Unified Communications Manager generates the FailedToFulfillDirectiveFromPDP alarm.
- RTMT shows the warning alarm, FailedToFulfillDirectiveFromPDP. This alarm contains one of following reasons.
  - Insert of the announcement failed.—Check whether the Cisco IP Voice Media Streaming App service is running in Cisco Unified Serviceability. If it is running, check that the Annunciator service parameter for the Cisco IP Voice Media Streaming App service is set to True. Furthermore, there

could be codec mismatch. The annunciator supports G.711, G.729, and Cisco Wideband codec, which the caller device may not support.

- Announcement can't be played because no early media capability.—The caller device does not supports the early media capability. Some devices that support the early media capability are SIP trunk and H323 trunk.
- Redirect Call Error with Error Code.—Check the Diversion Rerouting Calling Search Space configured in the external call control profile to determine whether it includes the partition of a redirected destination/device.
- Extend Call Error with Error Code.—Perhaps a destination is busy or unregistered, or the destination pattern is a translation pattern that is not associated with a device.

Unified Communications Manager Administration reports an error processing an uploaded custom announcement.

- Verify that the custom announcement.wav file is in proper format; that is, Windows PCM, 16-bit, (16000, 32000, 48000, or 48100) samples per second, mono or stereo.
- In RTMT, collect the Cisco Audio Translator traces for analysis of the error.

No announcement gets played.

The Cisco IP Voice Media Streaming App service issues the following alarms:

- kANNAudioUndefinedAnnID—The announcement uses an undefined custom announcement identifier or locale identifier. The alarm contain the numeric identifiers.
- kANNAudioFileMissing— Custom and/or Cisco-provided announcement.wav file is not found. The alarm contains file name, Announcement ID, user locale, and network locale.
- Verify ANN device is registered to the Unified Communications Manager.
- If media resource group is being used, verify that the ANN device is in media resource group.
- Verify that the announcement ID is correct.
- Verify that the locale is installed if you are not using English, United States locale.

Troubleshooting Hotline

The following table provides troubleshooting information for cases where hotline calls do not dial correctly.

Table 6: Troubleshooting Hotline—Calls Do Not Dial Correctly

Problem	Solution
Dial tone	Check PLAR configuration.

Problem	Solution
Reorder tone or VCA (intracluster call)	• Check PLAR configuration. • Verify that the phones on both ends are configured as hotline phones.
Reorder tone or VCA (intercluster or TDM call)	• Check PLAR configuration. • Verify that the phones on both ends are configured as hotline phones. • Verify that route class signalling is enabled on trunks. • Check the configuration of route class translations on CAS gateways.

The following table provides troubleshooting information for cases where call screening based on caller ID does not work.

Table 7: Troubleshooting Hotline—Call Screening Based on Caller ID Problems

Problem	Solution
Call not allowed	• Check Caller ID. • Add pattern to screen CSS.
Call allowed	Remove pattern from screen CSS.

Troubleshooting Immediate Divert

This section covers solutions for the most common issues that relate to the Immediate Divert feature.

Related Topics

Busy, on page 30
Key Is Not Active, on page 29
Temporary Failure, on page 30

Key Is Not Active

Symptom

This message displays on the phone when the user presses iDivert.

Possible Cause

The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.

Corrective Action

Configure a voice-messaging pilot in the user voice-messaging profile.

Temporary Failure

Symptom

This message displays on the phone when the user presses iDivert.

Possible Cause

The voice-messaging system does not work, or a network problem exists.

Corrective Action

Troubleshoot your voice-messaging system. See troubleshooting or voice-messaging documentation.

Busy

Symptom

This message displays on the phone when the user presses iDivert.

Possible Cause

Message means that the voice-messaging system is busy.

Corrective Action

Configure more voice-messaging ports or try again.

Troubleshooting Intercom

This section covers the solutions for the most common issues that relate to Intercom.

Related Topics

Getting Busy Tone When Dialing Out of Intercom Line, on page 31
Intercom Calls Do Not Go to Connected State When Going Off Hook by Using Speaker, Handset, or Headset, on page 31
Troubleshooting SCCP, on page 31
Troubleshooting SIP, on page 32
Cisco Extension Mobility User Is Logged In But Intercom Line Does Not Display, on page 32

Getting Busy Tone When Dialing Out of Intercom Line

Symptom

Phone plays busy tone when user is dialing out of intercom line.

Possible Cause

DN is not in the same intercom partition as the calling number.

Recommended Action

1. Ensure that the DN is in the same intercom partition as the calling number.
2. If it is, ensure that the dialed out DN is configured on another phone and that phone is registered with same Unified Communications Manager cluster.

Intercom Calls Do Not Go to Connected State When Going Off Hook by Using Speaker, Handset, or Headset

Symptom

User cannot go into talkback mode for intercom calls by using headset, handset, or speaker.

Possible Cause

This situation exists by design. The only way to go into the connected state for intercom calls is by pressing the corresponding line button.

Recommended Action

User can end call by using speaker, handset, or headset.

Troubleshooting SCCP

This section provides troubleshooting tips for phones that are running SCCP.

Related Topics

Intercom Lines Not Showing Up on Phone When Button Template Has Them, on page 31
Intercom Lines Not Showing Up When Phone Falls Back to SRST, on page 32

Intercom Lines Not Showing Up on Phone When Button Template Has Them

Symptom

Intercom lines do not display on the phone.

Possible Cause

The phone version may be earlier than 8.3(1), or the button template may not be assigned to the phone.

Procedure

1. Check the phone version. Ensure that it is 8.3(1) or above.
2. Determine whether the button template is assigned to the phone.
3. Capture the sniffer trace between Unified Communications Manager and the phone. In the button template response, see whether intercom lines get sent to the phone (button definition = Ox17).

Intercom Lines Not Showing Up When Phone Falls Back to SRST

Symptom

The phone, which was configured with Unified Communications Manager Release 6.0(x) or later, includes two intercom lines. Unified Communications Manager stops and falls back to SRST. The intercom lines do not display.

Possible Cause

The SCCP version of SRST does not support SCCP version 12.

Recommended Action

1. Check the SCCP version of SRST. If SRST supports SCCP version 12, it will support intercom lines.
2. If SRST supports SCCP version 12, capture a sniffer trace and ensure that the button template that the phone sent includes intercom lines.

Troubleshooting SIP

This section provides information to help you determine issues on phones that are running SIP.

Related Topics

Configuration of Phones That Are Running SIP, on page 32
Debugging Phones That Are Running SIP, on page 32

Debugging Phones That Are Running SIP

Use this debug command, **Debug sip-messages sip-task gsmfsmIsm sip-adapter**.

Configuration of Phones That Are Running SIP

Show config - The command on the phone displays if intercom lines are configured as regular lines with featureid-->23.

Cisco Extension Mobility User Is Logged In But Intercom Line Does Not Display

Symptom

The *Cisco Extension Mobility* user is logged into a phone, but the user intercom line does not display.

Possible Cause

Default Activated Device is configured incorrectly.

Recommended Action

1. Check that the Default Activated Device is configured on the intercom directory number.
2. Check that the Default Activated Device matches the device to which the used in logged in.

Where to Find More Information

- "Intercom" chapter, Feature Configuration Guide for Cisco Unified Communications Manager.

Troubleshooting IPv6

This section describes corrective actions for issues that are related to IPv6.

Related Topics

Calls Between Devices Fail, on page 34
Calls Over SIP Trunks Fail, on page 34
Music On Hold Does Not Play on Phone, on page 34
Phones Do Not Register with Cisco Unified Communications Manager, on page 33

Phones Do Not Register with Cisco Unified Communications Manager

Symptom

Cisco Unified IP Phones with an IP Addressing Mode of IPv6 Only do not register with Unified Communications Manager.

Corrective Action

- Via the CLI, verify that you enabled IPv6 on the Unified Communications Manager server.
- In the Enterprise Parameter Configuration window, verify that the Enable IPV6 enterprise parameter is set to True.
- In the Server Configuration window, verify that you configured either the host name or the IPv6 address for the Unified Communications Manager server in the Ipv6 Name field. If you configured a host name, verify that you configured DNS to resolve the host name to an IPv6 address.
- Verify that the Unified Communications Manager server has one non link-local IPv6 address only.
- If the phone gets an IPv6 address via stateless autoconfiguration, verify that you configured the Allow Auto-Configuration for Phone setting as On.
- Verify that the Cisco CallManager and Cisco TFTP services are running.

Calls Over SIP Trunks Fail

Symptom

Incoming calls fail if they come over a SIP trunk that has an IP Addressing Mode of IPv6 Only.

Corrective Action

- Via the CLI, verify that you enabled IPv6 on the Unified Communications Manager server.
- In the Enterprise Parameter Configuration window, verify that the Enable IPV6 enterprise parameter is set to True.
- Verify that the INVITE does not contain IPv4 signaling.

Symptom

Outgoing calls fail if they come over a SIP trunk that has an IP Addressing Mode of IPv6 Only.

Corrective Action

- Via the CLI, verify that you enabled IPv6 for the operating system on the Unified Communications Manager server.
- In the Enterprise Parameter Configuration window, verify that the Enable IPV6 enterprise parameter is set to True.
- In the Trunk Configuration window, verify that you configured an IPv6 destination address for the SIP trunk.

Calls Between Devices Fail

Symptom

Calls between two devices fail.

Corrective Action

- In the device configuration window, verify the IP addressing mode of the devices.
- If one device has an IP Addressing Mode of IPv4 Only and the other device has an IP Addressing Mode of IPv6 Only, ensure that you have an MTP configured that supports both the IPv4 and IPv6 stacks.

Music On Hold Does Not Play on Phone

Symptom

Phone user cannot hear music on hold.

Corrective Action

- Verify the IP addressing mode of the device where music on hold is played. If the IP addressing mode for the device is IPv6 Only and if music on hold is configured for unicast music on hold, ensure that you have an MTP configured that supports both the IPv4 and IPv6 stacks.
- If you configured multicast music on hold, be aware that phones that have an IP addressing mode of IPv6 Only cannot play music on hold.

Troubleshooting Logical Partitioning

This section describes corrective actions for issues that are related to logical partitioning.

Related Topics

Logical Partitioning Does Not Function As Expected, on page 35
Logical Partitioning Policies Require Adjustment, on page 36

Logical Partitioning Does Not Function As Expected

Symptom

Logical partitioning does not function as expected.

Corrective Action

Perform the following actions to correct the problem:

- Check whether the Enable Logical Partitioning enterprise parameter is set to **True**.
- Check that the device is associated with a valid geolocation at the device or device pool level.
- Check that the device is associated with a valid geolocation filter that comprises a selection of some of the geolocation fields at the device or device pool level.
- If the Logical Partitioning Default Policy enterprise parameter specifies **DENY**, check whether ALLOW logical partitioning policies between GeolocationPolicy of a gateway and GeolocationPolicy of a VoIP site are configured.
- Make sure that the case is correct for the fields of the logical partitioning GeolocationPolicy records and matches the case that is configured for geolocation records.
  - **Example:** The following geolocations exist: US:NC:RTP:BLD1 and US:TX:RCDN:bld1.

    When the GeolocationPolicy records get configured from logical partitioning policy records, you can configure the following policy: Border:US:NC:RTP:bld1 to Interior:US:NC:RTP:bld1.

    In this case, the incorrect value was chosen from the drop-down list box for the LOC field in the Location Partitioning Policy Configuration window, which displays both BLD1 and bld1.

    Therefore, the administrator must make sure to choose entries, so the case of the geolocation entry matches the case of the value that is used in GeolocationPolicy.
- No logical partitioning policy check takes place for VoIP-to-VoIP-device calls or features with only VoIP participants.

- Unified Communications Manager Administration allows configuration of policies between Interior:geolocpolicyX and Interior:geolocpolicyY, but such configuration does not get used during logical partitioning checks.

Logical Partitioning Policies Require Adjustment

Symptom

The fields in the logical partitioning policies are not configured correctly.

Corrective Action

Because the hierarchy of geolocation fields is significant, ensure that the hierarchical order of all fields is correct, and ensure that all fields are present. Hierarchical order means that Country entries precede A1 entries, which precede A2 entries, and so on.

Ensure that all fields are present in the logical partitioning policies and all fields are specified in the correct hierarchical order.

See the examples that follows.

Example of Logical Partitioning Policies That Match

In the following geolocation information, search for policy between Border:IN:KA and Interior:IN:KA.

The following possible policies match in order, where ***IN*** represents a Country field entry and KA represents an A1 field entry:

GeolocationPolicyA	GeolocationPolicyB	Policy
Border:IN:KA	Interior:IN:KA	Allow/Deny
Border:IN:KA	Interior:IN	Allow/Deny
Border:IN:KA	Interior	Allow/Deny
Border:IN	Interior:IN:KA	Allow/Deny
Border:IN	Interior:IN	Allow/Deny
Border:IN	Interior	Allow/Deny
Border	Interior:IN:KA	Allow/Deny
Border	Interior:IN	Allow/Deny
Border	Interior	Allow/Deny

Example of Logical Partitioning Policies That Do Not Match

In contrast, if the field of a geolocation is missing in a logical partitioning policy, the necessary match does not occur. The following logical partitioning policies do not include the Country field entry, which specifies ***IN***:

Border:KA
Interior:KA
Border:BLR
Interior:BLR
Border:KA:BLR
Interior:KA:BLR

Note Country=IN is missing.

Troubleshooting SIP with DNS Caching Enabled

Logging

Symptom

Set debug level for logging.

Recommended Action

Set network name-service debug-level 3(default 0)

- level 0 - no logging
- level 1 – errors, some cache removals
- level 2 – cache population
- level 3 and greater – entries considered for cache hits, pruning cache

Log file

Log file: activelog syslog/nscd.log

Consider the following example for Sample log file content:

Wed Dec 17 18:26:01 2014 - 21908: Have not found "clock.cisco.com" in hosts cache!

Wed Dec 17 18:26:01 2014 - 21908: add new entry "clock.cisco.com" of type GETHOSTBYNAME for hosts to cache (first)

Wed Dec 17 18:26:01 2014 - 21908: handle_request: request received (Version = 2) from PID 22151

Packet Capture

utils network capture port 53

Example:

admin: utils network capture port 53

Executing command with options:

```
size=128                count=1000              interface=eth0
 src=                    dest=                   port=53
 ip=  17:54:55.397539 IP b7k-vma150.cisco.com.45921 > dns-sj.cisco.com.domain: 38531+ A?
b7k-vma154.cisco.com.(38)
17:54:55.398952 IP b7k-vma150.cisco.com.44296 > dns-sj.cisco.com.domain: 63056+ PTR?
183.168.70.171.in-addr.arpa.(45)
17:54:55.430709 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.45921: 38531* 1/3/6 A
10.94.12.154.(240)
17:54:55.431802 IP b7k-vma150.cisco.com.47404 > dns-sj.cisco.com.domain: 40244+ PTR?
154.12.94.10.in-addr.arpa.(43)
17:54:55.432016 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.44296: 63056* 1/3/6 PTR
dns-sj.cisco.com.(261)
17:54:55.465242 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.47404: 40244* 1/3/6 PTR
b7k-vma154.cisco.com.(263)
```

A/AAAA record caching is not working

Symptom

A/AAAA record caching is not working. An A/AAAA record query is sent every time SIP call needs host name resolution.

Corrective Action

Check the status of Name Service Cache service. The status should be“Started” as given below:

```
admin:utils service list
Requesting service status, please wait…
System SSH [STARTED]
Cluster Manager [STARTED]
Password Reset [STOPPED] Service Activated
Name Service Cache [STARTED]…
```

If the Name Service Cache service status is not STARTED, use the following CLI command to activate :

admin:utils service activateName Service Cache

admin:utils service start Name Service Cache

If the Name Service Cache service status is already STARTED, use the following CLI command to restart:

admin:utils service restart Name Service Cache

Set debug level to 3 or higher. Ping a valid host name. Check the nscd.log and verify that the A/AAAA record is being added to the cache or the system is utilizing an existing cache entry.

Events appear in system log (/var/log/active/syslog/messages).

Dec 17 10:41:31 localhost user 6 ilog_impl: Received request for platform-event (platform-system-startup)

Dec 17 10:41:31 localhost user 6 ilog_impl: emitting platform-event (platform-system-startup)

Dec 17 10:41:31 localhost user 6 ilog_impl: emitted platform-event (platform-system-startup)

Note If caching works for "ping", ensure that the caching works for the Unified Communications Manager Service (such as Cisco CallManager Service). There can be a delay for the application to detect and interact with nscd.

Hostname resolution returning wrong IP address

Symptom

Hostname resolution returns a wrong IP address.

Possible Cause

The cache is obsolete. This is usually due to A/AAAA record changes in DNS server.

Corrective Action

- Flush the current cache using the following CLI command:

admin:utils network name-service hosts cache invalidate

- If problem persists, restart nscd using the following CLI command:

admin:utils service restart Name Service Cache

- If problem still persists, disable nscd using the following CLI command:

admin: utils service stop Name Service Cache

- If problem still persists check the A/AAAA record configuration in the DNS server.

Cannot find log

Symptom

Cannot find log /var/log/active/syslog/nscd.log

Corrective Action

Check that the debug level is above 0 (default is 0). After updating debug level, restart nscd using the following CLI command:

admin:utils service restart Name Service Cache

Set nscd attributes through CLI

Symptom

I set nscd attributes via CLI, but the new attribute values are not taking effect.

Corrective Action

Restart nscd after any attribute change, using the following CLI command:

utils service restart Name Service Cache

CLI command to set TTL

Symptom

I used CLI command to set TTL for the nscd cache entries, but the value I set is not taking effect for A/AAAA record cache.

Corrective Action

The TTL configured for the A/AAAA record on the DNS server will override the configuration set for nscd.

The TTL configured for nscd will take effect only if TTL is not configured for the A/AAAA record on DNS server.

A/AAAA Record Queries before TTL expires

Symptom

Name Service Cache is enabled, I still see multiple A/AAAA record Queries sent to DNS Server before TTL expires.

Corrective Action

These queries are most likely triggered by nscd reloading the existing cache entries. Nscd reloading behavior is related to the reload-count in the nscd configuration file.

Clearing the cache

Symptom

Will restarting nscd clear the A/AAAA record cache?

Corrective Action

Restarting nscd does not always clear/flush the cache. It depends on the persistent attribute configuration.

- If the persistent attribute is set to Yes, the cache remains the same when nscd restarts.
- If the persistent attribute is set to No(default), the cache will be cleared/flushed when nscd restarts.

To clear/flush the cache, use the following CLI command:

admin:utils network name-service hosts cache invalidate

Content of AAAA record cache

Symptom

Can I see the content of A/AAAA record cache?

Corrective Action

No. NSCD activities can only be observed in nscd.log (with desired debugging level setting). A/AAAA record caching statistics can also be queried using the CLI command:

admin:show network name-service hosts cache-stats

Troubleshooting SAML Single Sign On

This section provides information on symptoms and corrective actions when SAML Single Sign On does not work as expected.

Redirection to IdP fails

Symptom

When the end users attempt to log into a SAML-enabled web application using a Unified Communications Manager supported web browser, they are not redirected to their configured Identity Provider (IdP) to enter the authentication details.

Corrective Action

Check if the following conditions are met:

- The IdP is up and running.
- The correct IdP metadata file is uploaded to Unified Communications Manager.
- Verify if the server and the IdP are part of the same circle of trust.

IdP Authentication Fails

Symptom

The end user is not getting authenticated by the IdP.

Corrective Action

Check if the following conditions are met:

- The LDAP directory is mapped to the IdP.
- The user is added to the LDAP directory.
- The LDAP account is active.
- The User Id and password are correct.

Redirection to Unified Communications Manager fails

Symptom

Even after getting authenticated by the IdP, the user is not redirected to SAML SSO enabled web applications.

Corrective Action

Check if the following conditions are met:

- The clocks of all the Unified Communications Manager nodes and the IdP are synchronized. See the NTP Settings section in System Configuration Guide for Cisco Unified Communications Manager for information on synchronizing clocks.
- The mandatory attribute uid is configured on the IdP.
- The correct Cisco Unified Communication server metadata file is uploaded to the IdP.
- The user has the required privileges.

Run Test Fails

Symptom

The Run test fails.

Corrective Action

Refer the corrective actions that are outlined in Redirection to IdP fails, on page 41, IdP Authentication Fails, on page 41, and Redirection to Unified Communications Manager fails, on page 42.

SAML Single Sign On Page Shows Incorrect Status on Cluster

Symptom

The SAML SSO is enabled on the cluster. If you disable SAML SSO on a subscriber while the publisher is down, and also disable SAML SSO on the publisher after the publisher is up, the clusterwide SAML SSO status is incorrectly displayed as 'SAML SSO enabled'.

Corrective Action

View the 'Unified CM Cluster Overview' report in Cisco Unified Reporting. See the 'Unified CM SAML SSO Status Summary' section. This section indicates that the database value for SAML SSO status for a server is

out of sync on the subscriber. Since the server reports that SAML SSO is enabled, the system assumes that the entire cluster is SAML SSO enabled. Restart that subscriber node to resolve this setting.

For more information about viewing reports in Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

General Tips

- Be sure to set the SAML trace level to DEBUG. For more information on setting the SAML trace level, see *Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)*
- Collect the 'Cisco SSO' service logs (path: /tomcat/logs/ssosp/log4j/* and /platform/logs/ssoApp*) by using TLC in Unified RTMT or by executing the **CLI** command:**file get activelog**.