MGCP 1.0 and Additional MGCP Packages

Document Release History

<table>
<thead>
<tr>
<th>Publication Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 17, 2004</td>
<td>Initial release of the document</td>
</tr>
<tr>
<td>October 26, 2005</td>
<td>Added bulk audit information</td>
</tr>
</tbody>
</table>

Feature History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5(2)</td>
<td>This feature was introduced on the PGW 2200 (MGC) in software Release 9.5(2)</td>
</tr>
</tbody>
</table>

The MGCP 1.0 and Additional MGCP Packages Feature is described in the following sections:

- Feature Overview, page 2
- Supported Platforms, page 5
- Supported Standards, MIBs, and RFCs, page 5
- Configuration Tasks, page 6
- Provisioning Tasks, page 7
- Command Reference, page 14
- Reference Information, page 24
- Obtaining Documentation, page 41
- Documentation Feedback, page 42
- Cisco Product Security Overview, page 42
- Obtaining Technical Assistance, page 43
- Obtaining Additional Publications and Information, page 45
- Glossary, page 46
Feature Overview

The PGW 2200 Softswitch, also known as the Media Gateway Controller (MGC), has been enhanced to support MGCP 1.0 (IETF RFC 2705 bis 5) and additional MGCP packages, including the Announcement package, ATM package, and Bulk Audit package.

The MGCP 1.0 protocol provides better management of endpoints, especially where adverse network conditions exist. Some other enhancements supported in MGCP 1.0 are more return codes, additional restart methods and procedures, and additional capabilities, such as bulk audit support.

The PGW 2200 using MGC 1.0 can operate with the AS5300, AS5350, AS5400, AS5850s (using IOS Release 12.2(11)T, or higher), and the MGX 8000 Voice Gateway.

Benefits

Enhancement of the MGC from MGCP 0.1 to MGCP 1.0 is mainly targeted at increasing the robustness of the PGW 2200 MGC communication. It does not change the fundamental services offered within the supported solutions or applications. However, adding some of the MGCP packages makes possible more efficient service operations.

Endpoint Management

The primary driver for the MGCP 1.0 and Additional MGCP Packages feature is the additional features and functionality that is associated with the better management of endpoints during adverse network conditions.

Additional Feature Support

The secondary driver for the MGCP 1.0 and Additional MGCP Packages feature is support for new features and enhancements, including the announcement package, Bulk Call Audit, and ATM Package. For example, the added features support:

- Additional ReStart In Progress (RSIP) methods—disconnected and cancel-graceful
- Additional return and error codes, listed in Table 1
- Receiving and separating piggyback messages
- Coexistence of both MGCP 0.1 and MGCP 1.0 protocols
- The MGCP Bulk Audit Package
- Local MGCP-controlled announcement and tone capabilities
- ATM profile negotiation between gateways

MGCP 1.0 Error and Return Codes

Table 1 contains the error and return codes that are added to support the MGCP 1.0 and Additional MGCP Packages feature. Table 10 lists the return codes and the corresponding internal cause code.
### Table 1  
**MGCP Return Codes and Descriptions**

<table>
<thead>
<tr>
<th>1.0 Return Code</th>
<th>0.1 Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>NA</td>
<td>Response acknowledgement.</td>
</tr>
<tr>
<td>100</td>
<td>NA</td>
<td>Transaction is being executed. Completion response will follow.</td>
</tr>
<tr>
<td>101</td>
<td>NA</td>
<td>Transaction has been queued.</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
<td>Transaction was executed normally.</td>
</tr>
<tr>
<td>250</td>
<td>250</td>
<td>Connection was already deleted.</td>
</tr>
<tr>
<td>400</td>
<td>400</td>
<td>Transaction not executed, transient error.</td>
</tr>
<tr>
<td>401</td>
<td>401</td>
<td>Phone is already off hook.</td>
</tr>
<tr>
<td>402</td>
<td>402</td>
<td>Phone is already on-hook.</td>
</tr>
<tr>
<td>403</td>
<td>400</td>
<td>Endpoint does not have sufficient resources.</td>
</tr>
<tr>
<td>404</td>
<td>400</td>
<td>Insufficient Bandwidth.</td>
</tr>
<tr>
<td>405</td>
<td>400</td>
<td>Endpoint is restarting.</td>
</tr>
<tr>
<td>406</td>
<td>400</td>
<td>Transaction timeout.</td>
</tr>
<tr>
<td>407</td>
<td>400</td>
<td>Transaction aborted.</td>
</tr>
<tr>
<td>409</td>
<td>400</td>
<td>Internal overload.</td>
</tr>
<tr>
<td>410</td>
<td>400</td>
<td>Endpoint not available.</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
<td>Endpoint unknown.</td>
</tr>
<tr>
<td>501</td>
<td>501</td>
<td>Endpoint is not ready.</td>
</tr>
<tr>
<td>502</td>
<td>502</td>
<td>Endpoint does not have sufficient resources.</td>
</tr>
<tr>
<td>503</td>
<td>502</td>
<td>All of wildcard is too complicated.</td>
</tr>
<tr>
<td>504</td>
<td>510</td>
<td>Unknown or unsupported command.</td>
</tr>
<tr>
<td>505</td>
<td>510</td>
<td>Unknown remote connection descriptor.</td>
</tr>
<tr>
<td>506</td>
<td>510</td>
<td>Unable to satisfy both local connection option and remote connection descriptor.</td>
</tr>
<tr>
<td>507</td>
<td>510</td>
<td>Unsupported functionality.</td>
</tr>
<tr>
<td>508</td>
<td>510</td>
<td>Unknown quarantine handling.</td>
</tr>
<tr>
<td>509</td>
<td>510</td>
<td>SDP Error.</td>
</tr>
<tr>
<td>510</td>
<td>510</td>
<td>Protocol error.</td>
</tr>
<tr>
<td>511</td>
<td>511</td>
<td>Unrecognized extension.</td>
</tr>
<tr>
<td>512</td>
<td>512</td>
<td>Gateway not equipped to detect events.</td>
</tr>
<tr>
<td>513</td>
<td>513</td>
<td>Gateway not equipped to generate signal.</td>
</tr>
<tr>
<td>514</td>
<td>514</td>
<td>Transaction could not be executed because the gateway cannot send the specified announcement.</td>
</tr>
<tr>
<td>515</td>
<td>515</td>
<td>Invalid connection ID.</td>
</tr>
<tr>
<td>516</td>
<td>516</td>
<td>Unknown Call ID.</td>
</tr>
<tr>
<td>517</td>
<td>517</td>
<td>Unsupported/Invalid mode.</td>
</tr>
</tbody>
</table>
Table 1  MGCP Return Codes and Descriptions (continued)

<table>
<thead>
<tr>
<th>1.0 Return Code</th>
<th>0.1 Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>518</td>
<td>518</td>
<td>Unsupported/Invalid package.</td>
</tr>
<tr>
<td>519</td>
<td>519</td>
<td>Endpoint does not have a digit map.</td>
</tr>
<tr>
<td>520</td>
<td>520</td>
<td>Endpoint restarting.</td>
</tr>
<tr>
<td>521</td>
<td>NA</td>
<td>Endpoint redirected to another call agent.</td>
</tr>
<tr>
<td>522</td>
<td>510</td>
<td>No such signal or event.</td>
</tr>
<tr>
<td>523</td>
<td>510</td>
<td>Unknown action or illegal combination of actions.</td>
</tr>
<tr>
<td>524</td>
<td>510</td>
<td>Internal inconsistency in LocalConnectionOptions (LCO).</td>
</tr>
<tr>
<td>525</td>
<td>510</td>
<td>Unknown extension in LCO.</td>
</tr>
<tr>
<td>526</td>
<td>502</td>
<td>Insufficient bandwidth.</td>
</tr>
<tr>
<td>527</td>
<td>510</td>
<td>Missing RemoteConnectionDescriptor.</td>
</tr>
<tr>
<td>528</td>
<td>510</td>
<td>Incompatible protocol version.</td>
</tr>
<tr>
<td>529</td>
<td>501</td>
<td>Hardware failure.</td>
</tr>
<tr>
<td>530</td>
<td>501</td>
<td>CAS signaling protocol error.</td>
</tr>
<tr>
<td>531</td>
<td>501</td>
<td>Failure of a grouping of trunks (facility error).</td>
</tr>
<tr>
<td>532</td>
<td>510</td>
<td>Unsupported values in LCO.</td>
</tr>
<tr>
<td>533</td>
<td>502</td>
<td>Insufficient bandwidth. Response too large.</td>
</tr>
<tr>
<td>534</td>
<td>502</td>
<td>Codec negotiation failure.</td>
</tr>
<tr>
<td>535</td>
<td>510</td>
<td>Packetization period not supported.</td>
</tr>
<tr>
<td>536</td>
<td>510</td>
<td>Unsupported RestartMethod.</td>
</tr>
<tr>
<td>537</td>
<td>510</td>
<td>Unknown or unsupported digit map extension, since the gateway does not have the digit map.</td>
</tr>
<tr>
<td>538</td>
<td>512 or 513</td>
<td>Event/Signal parameter error.</td>
</tr>
<tr>
<td>540</td>
<td>515</td>
<td>Per endpoint connection limit was exceeded.</td>
</tr>
<tr>
<td>596</td>
<td>596</td>
<td>VISIM-specific return code indicating VCC failure or VCC could not be set up.</td>
</tr>
<tr>
<td>598</td>
<td>598</td>
<td>Media connection failure.</td>
</tr>
<tr>
<td>599</td>
<td>599</td>
<td>VISIM-specific return code indicating media connection loss.</td>
</tr>
</tbody>
</table>

Restrictions

The PGW 2200 using MGC 1.0 operates with the AS5300, AS5350, AS5400, and AS5850 (using IOS Release 12.2(11)T or higher), and the MGX 8000 Voice Gateway.

You can run both MGCP 0.1 and MGCP 1.0 on the same MGC.
Related Documents

This document contains information that is related strictly to the MGCP 1.0 and Additional MGCP Packages feature. The documents that contain additional information related to the Cisco MGC are listed below:

- Release Notes for Cisco Media Gateway Controller Software Release 9.5(2)
- Cisco Media Gateway Controller Hardware Installation Guide
- Regulatory Compliance and Safety Information for the Cisco Media Gateway Controller
- Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide
- Cisco Media Gateway Controller Software Release 9 Provisioning Guide
- Cisco Media Gateway Controller Software Release 9 Dial Plan Guide
- Cisco Media Gateway Controller Software Release 9 MML Command Reference
- Cisco Media Gateway Controller Software Release 9 Messages Reference Guide
- Cisco Media Gateway Controller Software Release 9 Billing Interface Guide
- Cisco Media Gateway Controller Software Release 9 Management Information Base Guide
- Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide

Supported Platforms

The hardware platforms supported for the Cisco MGC software Release 9.5(2) are described in the Release Notes for Cisco Media Gateway Controller Software Release 9.5(2); and include the AS5300, AS5350, AS5400, AS5850s (using IOS Release 12.2(11)T, or higher), and the MGX 8000 Voice Gateway.

Supported Standards, MIBs, and RFCs

Standards
No new or modified standards are supported by this feature.

MIBs
No new or modified MIBs are supported by this feature.

For more information on the MIBs used in the Cisco MGC software, refer to the Cisco Media Gateway Controller Release 9 MIB Guide.

RFCs
The MGCP 1.0 and Additional MGCP Packages feature supports the following RFC:
MGCP 1.0 and Additional MGCP Packages

Configuration Tasks

This section contains the steps necessary for configuration of the Cisco MGC software to support the MGCP 1.0 and Additional MGCP Packages feature. If you are installing and configuring the Cisco MGC software on your system for the first time, refer to the Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide, and return to this section once you encounter the FaultRecoveryAuditTimer parameter in the XECfgParm.dat file.

Note

You configure the FaultRecoveryAuditTimer parameter only for the time interval between background audit procedures.

Caution

Configuration of the Cisco MGC software requires that the system software be shut down. In a simplex system, calls cannot be processed during system shutdown. In a continuous service system, your system loses the ability to maintain calls during a critical event while the system software on one of the MGC hosts is shut down.

Configure the FaultRecoveryAuditTimer by performing the following steps:

Step 1
If you have not already done so, open the /opt/CiscoMGC/etc/XECfgParm.dat file on the active and standby Cisco MGC hosts using a text editor, such as vi.

Step 2
If you have not already done so, set the pom.dataSync parameter to false on the active and standby Cisco MGC hosts.

Step 3
Search for the FaultRecoveryAuditTimer parameter and enter the desired time interval on the active and standby Cisco MGC hosts.

Step 4
Save your changes and close the text editor.

Troubleshooting Tips

There are two alarms (AnnTableReadingFail and AnnRespTimeout) specific to this feature. If you find that you are having trouble with your system and you suspect the MGCP 1.0 and Additional MGCP Packages feature is causing an error, verify the provisioning data for the system. If your system is incorrectly configured, fix the faulty data. If that does not solve the problem, or if your system is correctly configured, contact the Cisco TAC for assistance.

- When migrating from an earlier version of software to MGC software Release 9.5(2), the GWProtocolVersion value is MGCP0.1.
- If provisioning from “new” using MGC software Release 9.5(2), be aware that the default value for GWProtocolVersion is MGCP1.0.
- When connecting to gateways, be sure the MGCP version on all the platforms is the same. Set the GWProtocolVersion property value at the SigPath level by performing the following procedure.

To change the MGCP version property to MGCP 1.0, complete the following steps:
Provisioning Tasks

The following sections describe the provisioning tasks related to this feature:

- Planning for Provisioning, page 7
- Provisioning Procedures, page 7

Planning for Provisioning

It is recommended that you gather the following information:

- Gateway ATM profiles
- Announcement identification numbers
- Gateway location string

For more information on planning the provisioning for the rest of the Cisco MGC software, refer to the Cisco Media Gateway Controller Software Release 9 Provisioning Guide.

Provisioning Procedures

This section covers the following provisioning topics:

- Provisioning Basics, page 7

Provisioning Basics

Use the procedures in this section to start a provisioning session and save and activate the changes you have made.

- Starting a Provisioning Session, page 8
Starting a Provisioning Session

You may need to start a provisioning session as part of your system operations. Start a provisioning session by logging on to the active Cisco MGC and starting an MML session using the following MML syntax:

```mml>
prov-sta::srcver="curr_ver",dstver="mod_ver"
```

Where:
- **curr_ver**—The name of the current configuration version. In place of the name of the current configuration version, you can also enter:
  - new—A new default session configuration; no existing source configuration is available.
  - active—Selects the active configuration as the source for configuration changes.

**Note**
You can use “new” as the source configuration only when there is no existing, active set of provisioning data in the configuration library. Therefore, “new” cannot be used as the source configuration once a provisioning session has been saved and activated by using `prov-cpy` or `prov-dply`. Once you have saved and activated a set of data, you must use either “active” or the name of the set of provisioning data as the source configuration.

**Note**
If you do not know the name of your current configuration session, you can use the procedure described in the “Retrieving Data on the Current Provisioning Session” section on page 11.

- **mod_ver**—A new configuration version name that contains your provisioning changes.

For example, to use a configuration version called ver1 as the basis for a version to be called ver2, you would enter the following command:

```mml>
prov-sta::srcver="ver1",dstver="ver2"
```

Once a provisioning session is underway, use the `prov-add`, `prov-ed`, or `prov-dlt` MML commands to add, modify, or delete components on your system. This following sections describe how to add, modify, and delete system components. For more information on provisioning other components on your Cisco PGW 2200, refer to the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

There are two ways to close your provisioning session: saving and activating your provisioning changes, as described in the “Saving and Activating Your Provisioning Changes” section on page 8 or ending your provisioning session without saving and activating your changes, as described in the “Ending a Provisioning Session Without Activating the Changes” section on page 9.

Saving and Activating Your Provisioning Changes

When you have completed making provisioning changes in your session, you must enter an MML command to save and activate your changes. The `prov-cpy` and `prov-dply` MML provisioning commands do this.
Caution Depending on the extent of your provisioning changes, using the `prov-cpy` and `prov-dply` MML commands can severely impact your system call processing performance. We recommend that these commands be issued during a maintenance window when traffic is minimal.

Use the `prov-cpy` MML command to save and activate your changes on the active Cisco MGC. This command is typically used to save and activate changes on a Cisco MGC in a simplex configuration. However, you can use the `prov-cpy` MML command on Cisco MGCs in high-availability or continuous-service configurations, to save and activate your changes on the active Cisco MGC. If you choose to do this, you should enter the `prov-sync` MML command immediately afterwards, to have your changes saved and activated on the standby Cisco MGC.

Note When you enter the `prov-cpy` command, your provisioning session is also automatically ended. If you want to make additional provisioning changes, you must start a new provisioning session, as described in the “Starting a Provisioning Session” section on page 8.

Caution Using the `prov-sync` MML command can severely impact your system call processing performance. We recommend that this command be issued during a maintenance window when traffic is minimal.

Note When the `prov-sync` MML command is used to synchronize the provisioning settings on the standby MGC host with current settings on the active MGC host, the system does not indicate when the synchronization process has failed.

Use the `prov-dply` MML command to save and activate your changes on the active and standby Cisco MGCs. This command is typically used to save and activate changes on Cisco MGCs in high-availability or continuous-service configurations. This command should not be used on a Cisco MGC in a simplex configuration.

Note When you enter the `prov-dply` command, your provisioning session is also automatically ended, unless an error occurs during execution. If you want to make additional provisioning changes, you must start a new provisioning session, as described in the “Starting a Provisioning Session” section on page 8.

**Ending a Provisioning Session Without Activating the Changes**

If you want to end a provisioning session without saving and activating the changes you have entered, enter the `prov-stp` MML command. This command ends your current provisioning session and your changes are not entered.

**Retrieving Provisioning Data**

You can use the `prov-rtrv` MML command to retrieve information about your current provisioning settings. The ways you can use this command to retrieve provisioning data are described in the following sections:

- Retrieving Data for an Individual Component, page 10
- Retrieving Data for Select Components, page 10
- Retrieving Data for All Components of a Particular Type, page 10
Retrieving Data for an Individual Component
You can retrieve provisioning data on any individual component on your system. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:component:name=MML_name
```

Where:
- `component`—The MML component type associated with the desired component. You can find a complete list of MML component types in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.
- `MML_name`—The MML name for the desired component. You can determine the MML names for the various components using the `prov-rtrv:all` MML command.

For example, to view the provisioning data for a SS7 signaling service called `ss7svc1`, you would enter the following command:

```
prov-rtrv:ss7path:name="ss7svc1"
```

The response to the command is dependent upon the component type associated with the desired component. For example, to view the properties for an SUA routing key called `suakey1`, you would enter the following command:

```
prov-rtrv:suakey:name="suakey1"
```

Retrieving Data for Select Components
You can retrieve data on select components provisioned on your system by logging on to the active Cisco MGC, starting an MML session, and entering the following command:

```
mml> prov-rtrv:all
```

Note
This command returns data on all signaling components, except for signaling service and linkset properties.

Retrieving Data for All Components of a Particular Type
You can retrieve provisioning data on all components of a particular type on your system. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:component:*all*
```

Where: `component` is the MML component type associated with the desired component group. You can find a complete list of MML component types in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

Note
You cannot use this command with components that are used to retrieve signaling or routing properties (that is `sigsvcprop`, `lnksetprop`, and `trnkgrpprop`). The properties for only one signaling or routing component can be listed per command instance. Please use the following MML format:

```
mml> prov-rtrv:propComp:name="compName" | name="ss7famName"
```

Where:
**MGCP 1.0 and Additional MGCP Packages**

**Provisioning Tasks**

**propComp**—MML component name appropriate to the property type you want to retrieve:

- `sigsvcprop`—Provides maintenance access to the properties of signaling services
- `trnkgrpprop`—Provides maintenance access to the properties of trunk groups
- `lnksetprop`—Provides maintenance access to the properties of linksets

**compName**—MML name of a previously provisioned signaling service or trunk group.

**ss7famName**—MML name of the SS7 family associated with the desired linkset.

For example, to view the provisioning data for all signaling services, enter the following MML command:

```
provsrvr:ss7path:"all"
```

**Retrieving Data on the Current Provisioning Session**
You can retrieve provisioning data on the current provisioning session by logging on to the active Cisco MGC, starting an MML session, and entering the following command:

```
provsrvr:session
```

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2003-01-13 13:39:19
M RTRV
 "session=jtest:session"
 /*
 Session ID = mml
 SRCVER = active
 DSTVER = jtest
 */
```

**Retrieving Data on Supported Signaling Protocols**
You can retrieve protocol data for the current provisioning session by logging on to the active Cisco MGC, starting an MML session, and entering the following command:

```
provsrvr:variants
```

**Provisioning the ANNOUNCEMENT Result Type**

Perform the following steps to provision the ANNOUNCEMENT result type as part of the MGCP 1.0 and Additional MGCP Packages feature:

**Step 1**
Open a provisioning session on the active MGC by using the following MML command:

```
prov-sta::srcver="amm_rslt",dstver="mml_01"
```

**Note**
You can use “new” as the source configuration only when there is no existing, active set of provisioning data in the configuration library. Therefore, “new” cannot be used as the source configuration once a provisioning session has been saved and activated by using `prov-cpy` or `prov-dply`. Once you have saved and activated a set of data, you must use either “active” or the name of the set of provisioning data as the source configuration.
Provisioning the ToneAndAnnouncement Database Table

To provision the ToneAndAnnouncement database table, use the following MML commands to add, edit, delete, retrieve, or export an announcement.

**Adding an Announcement**

The following MML command is an example of adding an announcement:

```
mml> numan-add:announcement:annid=123,gwtype="AS5400",duration=60,repeat=2,interval=3,locationstring="xyz.aud"
```

**Editing an Announcement**

The following MML command is an example of editing an announcement.

```
mml> numan-ed:announcement:annid=123,gwtype="AS5400",locationstring="welcome.aud"
```

**Deleting an Announcement**

The following MML command is an example of deleting an announcement:

```
mml> numan-dlt:announcement:annid=123,gwtype="AS5400"
```

**Retrieving an Announcement**

The following MML command is an example of retrieving an announcement:

```
mml> numan-rtrv:announcement:annid=123,gwtype="AS5400"
```

**Exporting an Announcement File**

You can generate a data file called announcement.dat along with the file import command by using the following MML command:
MGCP 1.0 and Additional MGCP Packages

Provisioning Tasks

Cisco MGC Software Release 9.5(2)

**Importing an Announcement File**

After you edit this file, you can import it into the database by using the following MML command:

```
mml> prov-add:files:name="announcementfile",file="exp1/announcement.dat",action="import"
```

**Provisioning the ANNOUNCEMENT Result Type**

The following MML command is an example for importing an announcement file:

```
mml> prov-add:files:name="announcementfile",file="exp1/announcement.dat",action="import"
```

To add a remote announcement result: announceId=123, remote, RoutelistId=dulles, use the following MML command:

```
mml> numan-add:resulttable:custgrpId="T002",name="result59",resulttype="ANNOUNCEMENT",dw1="123",dw2="1",dw3="dulles",setname="set1"
```

To add a local announcement result: announceId=123, local, Final_on for playing announcement, use the following MML command:

```
mml> numan-add:resulttable:custgrpId="T002",name="result60",resulttype="ANNOUNCEMENT",dw1="123",dw2="0",dw4="1",setname="set1"
```

To associate a B-digit tree number to the result set, use the following MML command:

```
mml> numan-add:bdigtree:custgrpId="T002",digitstring="7034643375",callsid="originating",setname="set1"
```

**Provisioning ATM Profiles**

Profiles are used on the MGC to change the network Service Level Agreement. You can provision ATM profiles in routeAnalysis.dat by using the following MML commands to add, edit, delete, or retrieve an ATM profile:

```
mml> prov-add:atmprofiles:name="atmprof1",atmprofiles="ITU1;custom100"
mml> prov-ed:atmprofiles:name="atmprof1",atmprofiles="ITU1;custom200"
mml> prov-dlt:atmprofiles:name="atmprof1"
mml> prov-rtrv:atmprofiles:name="atmprof1"
mml> prov-rtrv:atmprofiles:"all"
```

**Provisioning ATM Profiles Result Types**

Provision ATM profiles result types by using the following MML commands:

```
mml> numan-add:resulttable:custgrpId="T002",name="result59",resulttype="ATM_ORIG_PROFILE",dw1="atmprof1",dw2="1",setname="set1"
```

```
mml> numan-add:resulttable:custgrpId="T002",name="result60",resulttype="ATM_TERM_PROFILE",dw1="atmprof1",dw2="1",setname="set1"
```

**Provisioning Trunk Group Properties**

Provision trunk group properties by using the following MML commands:

```
mml> prov-add:trnkgrp:name="1000",svc="ss7svc1",type="ATH"
```
**Provisioning SigPath Properties**

Provision the SigPath properties by using the following MML commands:

```mml
mml> prov-add:mgcppath:name="mgcpsvc1",extnode="AS5400",desc="MGCP service"
mml> prov-add:sigsvcprop:name="mgcpsvc1",GWProtocolVersion="MGCP 1.0"
mml> prov-add:sigsvcprop:name="mgcpsvc1",mgcpBulkAudit="1"
```

For more information on provisioning for the rest of the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

**XECfgParm.dat Changes**

This feature adds the FaultRecoveryAuditTimer parameter to the XECfgParm.dat file. The following table describes the FaultRecoveryAuditTimer parameter.

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>FaultRecoveryAuditTimer</td>
<td>The FaultRecoveryAuditTimer parameter configures the time interval between consecutive background audit procedures. The FaultRecoveryAuditTimer parameter contains an integer, representing the number of milliseconds between consecutive background audit procedures. Valid values: any integer value Default value: 15000</td>
</tr>
</tbody>
</table>

Additional examples of configuration for the Cisco MGC software can be found in the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*.

**Command Reference**

This section documents new, modified, or deleted Man-Machine Language (MML) commands. All other MML commands are documented in the *Cisco Media Gateway Controller Software Release 9 MML Command Reference Guide*.

**New MML Commands**

This section contains the MML commands that are new for the MGCP 1.0 and Additional MGCP Packages feature.

The MGC PlayAnnouncement trunk group property enables per trunk group playing of an early announcement. If the gateway associated with this trunk group can support announcements, then it is appropriate to configure this property to initiate that action.
The PlayAnnouncement property contains a value providing an announcement ID. Alternatively, if it is set to empty, Null, or 0, then the announcement function is considered to be disabled at the trunk group level.

Adding an ATM Profile to routeAnalysis.dat

ATM profile support is provided by using the following MML command:

```mml>
prov-add:atmprofiles:name="atmprof1",atmprofile="ITU1;custom100"
```

The following example represents the result of the previous MML command in routeAnalysis.dat:

```$ATMProfiles
# CiscoMGC:   01
$name             ATMProfiles
atmprof1          ITU1;cust100
```

Adding ATM Profiles to the Result Table

Add result types ATM_ORIG_PROFILE and ATM_TERM_PROFILE to the T002 dial plan. tResultTree includes these two result types and handling their respective datawords.

MML command examples:

```mml>
numan-add:resulttable:custgrpId="T002",name="result59",resulttype="ATM_ORIG_PROFILE",
dw1="atmprof1",dw2="1"
```

```mml>
numan-add:resulttable:custgrpId="T002",name="result60",resulttype="ATM_TERM_PROFILE",
dw1="atmprof1",dw2="1",setname="set1"
```

The result in T002.dialplan

```$resultTable
# Customer: T002
# type           dw1         dw2          dw3             dw4              nextResult
# result1      result59 59  1  1
```

NUMAN-ADD—announcement
NUMAN-ED—announcement
NUMAN-DLT—announcement
NUMAN-RTV—announcement

Purpose: The following MML commands are used to add, edit, delete, and retrieve an announcement or tone to or from the ToneAndAnnouncement database table.

Syntax: Example:

```numan-[verb]:announcement:annid=<announcement ID>,gwtype="<up to 10-character string>",playDuration=<0-120>,
repeat=<0-5>,interval=<0-5000>,locationstring="<up to 128-character string>"
```
Cisco MGC Software Release 9.5(2)

Modified MML Commands

This section contains the MML commands that were modified for the MGCP 1.0 and Additional MGCP Packages feature.

The existing MML command, \texttt{sta-aud-gw}, now allows the MGCP AUEP audit endpoint command to be used for synchronization on a specified gateway or on a specified endpoint. The endpoint is provided as a string parameter.

The MML command syntax allows the user to add an endpoint name to indicate that an MGCP AUEP is required.
The MML command **sta-aud**, which starts an MGC-level audit for all the configured gateways, now accepts parameters to allow gateway-level and line-level audits.

The MML command to retrieve the audit results, **rtrv-aud-gw**, is not changed, and no endpoint name is expected.

**Note**

Only one audit of any kind (AUEP) can be outstanding at any one time per gateway.

An example of the MML output for a successful MGCP AUEP query appears as follows.

```plaintext
mml> rtrv-aud-gw:sp1-mgcp1
 M GC-02 - Media Gateway Controller 2003-01-20 09:28:40.842 PST
 M COMPLD
 "sp1-mgcp1:Audit ep received at 2003-01-20 09:28:36
 Audit Endpoint PASSED for s0/ds-1/1
 response code = 200 connection id = 32F345E2
 request id = FE9FEA44 notified id = 128.96.41.12
 requested evts = D/[0-9] detected evts =
 observed evts = signal requests =
 digit map = quarantine hd1 = process
 reason code = bearer info = A
 max datagram = package list = res,atm
 capabilities
 a:PCMU, p:10-100, e:on, s:off, v:L;S,
    m:sendonly;recvonly;sendrecv;inactive;netwloop;netwtest
 ;
 mml>
```

**sta-aud**

This MML command starts an audit for all endpoints on the MGC. The audit is flow-controlled, based on the configurable timer and the number of endpoints. The **stp-aud** command stops the audit.

**sta-aud:<mgcp sigPath>**

This MML command starts an audit for endpoints on gateways associated with the specified MGCP signal path. This audit is flow-controlled and is stopped by the **stp-aud** command.

**sta-aud:<mgcp sigPath>:ENDPOINT="a/b/c"**

This MML command starts an audit for the specified endpoints (“a/b/c”). The `<mgcp sigPath>` specifies the gateway and “a/b/c” specifies the endpoints. A wildcard is allowed only for parameter “c” so endpoints on E1 or T1 can be audited. MML validates the wildcard limitation on the endpoint parameter.

The **sta-aud-gw** MML command now allows MGCP audits of the endpoints.

The syntax for the MML audit commands is listed in Table 2.
Note

It is not possible to use the sta-aud-gw command on all gateways for an MGCP AUEP.

The endpoint name cannot contain any * characters (wild cards). The format of the endpoint name is a/b/c.

For example:
sta-aud-gw:sp1-mgcp1:*s0/ds1-1/4*

The MML command to retrieve the audit results, rtrv-aud-gw, does not change and no endpoint name is expected.

Modified Properties

The following property has been modified.

GWProtocolVersion

The GWProtocolVersion property is expanded to support the following two values:

*GWProtocolVersion = MGCP0.1
*GWProtocolVersion = MGCP1.0

MML Commands to Provision the Tone and Announcement Database Table

To provision the ToneAndAnnouncement database table, use the following MML commands.

To add an announcement, use the following MML command:

mml> numan-add:announcement:annid=123,gwtype="AS5400",duration="60",repeat="2",interval="3",locationstring="xyz.aud"

To edit an announcement, use the following MML command:

mml> numan-ed:announcement:annid=123,gwtype="AS5400",locationstring="welcome.aud"

To delete an announcement, use the following MML command:

mml> numan-dlt:announcement:annid=123,gwtype="AS5400"

To retrieve an announcement, use the following MML command:

mml> numan-rtrv:announcement:annid=123,gwtype="AS5400"
Use the following MML command to generate a data file called announcement.dat along with the file import command in numan.MML by the following MML command:

```
mml> prov-exp:numan:dirname="exp1"
```

After editing, use the following MML command to import this file back into the database:

```
mml> prov-add:files:name="announcementfile",file="exp1/announcement.dat",action="import"
```

**MML Commands to Provision the ANNOUNCEMENT Result Type**

To add a remote announcement result: announceId=123, remote, RoutelistId=dulles, use the following MML command:

```
mml> numan-add:resulttable:custgrpId="T002",name="result59",resulttype="ANNOUNCEMENT", dw1="123",dw2="1",dw3="dulles",setname="set1"
```

To add a local announcement result: announceId=123, local, Final_on for playing announcement, use the following MML command:

```
mml> numan-add:resulttable:custgrpId="T002",name="result60",resulttype="ANNOUNCEMENT", dw1="123",dw2="0",dw4="1",setname="set1"
```

To associate a B-digit number to the result set, use the following MML command:

```
mml> numan-add:bdigtree:custgrpid="T002",digitstring="7034843375",callside="originating", setname="set1"
```

**MML Commands to Provision ATM Profiles in routeAnalysis.dat**

The following MML command examples show how you can add, edit, delete, and retrieve ATM profile support:

```
mml> prov-add:atmprofiles:name="atmprof1",atmprofiles="ITU1;custom100"
mml> prov-ed:atmprofiles:name="atmprof1",atmprofiles="ITU1;custom200"
mml> prov-dlt:atmprofiles:name="atmprof1"
mml> prov-rtrv:atmprofiles:name="atmprof1"
mml> prov-rtrv:atmprofiles:"all"
```

**MML Commands to Provision ATM Profiles Result Types**

The following MML command examples show how you can add ATM_ORIG_PROFILE and ATM_TERM_PROFILE:

```
mml> numan-add:resulttable:custgrpId="T002",name="result59",resulttype="ATM_ORIG_PROFILE", dw1="atmprof1",dw2="1",setname="set1"
mml> numan-add:resulttable:custgrpId="T002",name="result60",resulttype="ATM_TERM_PROFILE", dw1="atmprof1",dw2="1",setname="set1"
```

**MML Commands to Provision Trunk Group Properties**

The following MML command examples show how you can add or edit trunk group properties:

```
mml> prov-add:trnkgrp:name="1000",svc="ss7svc1",type="ATH"
mml> prov-ed:trnkgrpprop:name="1000",playannouncement="0"
mml> prov-ed:trnkgrpprop:name="1000",GWDefaultATMProfile="profile1;profile2"
mml> prov-ed:trnkgrpprop:name="1000",NetworkType="1"
mml> prov-ed:trnkgrpprop:name="1000",AtmConnectionType="4"
```
MML Commands to Provision SigPath Properties

The following MML command examples show how you can add sigpath properties:

```
mml> prov-add:mgcppath:name="mgcpsvc1",extnode="AS5400",desc="MGCP service"
mml> prov-add:sigsvcprop:name="mgcpsvc1",GWProtocolVersion="MGCP1.0"
mml> prov-add:sigsvcprop:name="mgcpsvc1",mgcpBulkAudit="1"
```

MML Provisioning of ANNOUNCEMENT(8) Result Type

The following is an example of provisioning the ANNOUNCEMENT result from B-number analysis as follows. First, configure the result in the result table, by using the following MML command:

```
mml> numan-add:resulttable:custgrpId="T002",name="result10",resulttype="ANNOUNCEMENT",dw1="1234",dw2="0",dw4="1",setname="setname1"
```

Next, assign the result from a position in the B-digit tree, by using the following MML command:

```
mml> numan-add:bdigtree:custgrpId="T002",digitstring="7034843355",callside="originating",setname="setname1"
```

Added Gateway Announcement Capability

The ANNOUNCEMENT result, described in Table 3, enables playing an early announcement to the MGC originating side before completing call routing. An application example might involve providing a “Welcome to the Network” message before setting up the call. This requires the associated gateway to have the capability to play announcements.

**Note**

Due to the nature of the connection, calls arriving by EISUP (H.323) or SIP protocols are not supported.

Applying an announcement is provisioned on the MGC at three levels: as an incoming trunk group property, as an A-number analysis result, or as a B-number analysis result. The trunk group property (PlayAnnouncement) provides the initial announcement identity and can be optionally over-written during A-number or B-number analysis.

Upon receiving a new call, the MGC analysis function carries out Pre-analysis, A-number analysis, B-number analysis, and routing. Early in the analysis function, the incoming trunk group property PlayAnnouncement is read and any provisioned announcement identity (integer value) is retrieved. If the PlayAnnouncement trunk group property is not configured, the property has a null or zero value indicating that no announcement action is required. If an announcement identity is retrieved, this indicates that an early or welcome announcement is to be played and that this data is stored locally before starting analysis, which is where the selection of announcement can be overridden.

If an ANNOUNCEMENT result is collected at Pre-analysis, A-number analysis, or B-number analysis, it is in addition to any announcement identity collected from the trunk group property. If only the PlayAnnouncement trunk group property is present, it is applied. However, if one of the analysis areas also has provided an ANNOUNCEMENT result, then the result either overrides the trunk group property or negates the trunk group property by not applying the announcement for the incoming number. The basic rule is that the last analysis area determines the final result.

**Note**

If in overlap numbering mode, all digits must be received and analyzed before any announcement is played. This means that any overlap announcement call effectively goes from overlap to enbloc.
If the final ANNOUNCEMENT result has dataword4 set to indicate OFF, then no announcement is played. In this case, generic analysis completely removes the ANNOUNCEMENT result and the call status is determined by the other collected results.

Once generic analysis determines which announcement Id to use, this information is passed back to number analysis to perform the necessary action. The announcement data accompanies any other results being returned. The result from analysis varies according to the announcement type and according to both the final result and the delivered announcement data.

When the RSLT_ANNOUNCEMENT analysis result arrives, the accompanying data is examined. The first check is to determine if it is a remote or local (gateway) announcement. If the announcement is remote, then the previous functionality and handling are invoked. If the indicator is set to local, then a gateway announcement is required, the Times-Ten Announcement table is read, and the data is stored in readiness.

A check is made to determine the course of action. That is, the check determines if the announcement is the final action (play announcement and clear down) or an intermediate action (play announcement and continue processing), as indicated by dataword4.

With the course of action determined, the required call processing is initiated. The MGC sends a CRCX[M: recvonly] over MGCP to the originating side gateway to prepare the channel for announcement playing. Then the MGC sends an ACM signal back to the preceding switch. This is necessary to allow time for playing the announcement, without exceeding the ACM timers, and to prepare the speech path on the previous switches.

At this point, the announcement playing is started and an Notification Request (RQNT) is sent to the gateway. Upon receiving RQNT, the gateway plays the announcement and also positively responds to the command. The MGC times the announcement playing activity and awaits a Notify (NTFY) message from the gateway. Once announcement playing is complete, the gateway responds with the NTFY message, and the completion indication is passed back to the MGC.

The action the MGC takes at this point depends on the indication given by analysis in dataword4. If the indication is ANN_final, then the call is cleared down. However, if the indication is Ann_Interim, then processing continues with the remaining results and the ANNOUNCEMENT result is discarded. If the remaining results include a trunk group, then circuit selection takes place.

### Table 3 Result Type Definitions

<table>
<thead>
<tr>
<th>Result Number</th>
<th>Result Type</th>
<th>Dataword1</th>
<th>Dataword2</th>
<th>Dataword3</th>
<th>Dataword4</th>
<th>Analysis Points</th>
<th>Result Type Valid For</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ANNOUNCEMENT</td>
<td>AnnouncementId</td>
<td>Local/Remote</td>
<td>RouteListId</td>
<td>AnnData</td>
<td>X</td>
<td>X X X X X</td>
</tr>
</tbody>
</table>

The ANNOUNCEMENT result type datawords and their corresponding definitions are as follows:

- **AnnouncementId**—Indicates the identity value corresponding to the announcement identity (or tone identity) that is played to the caller. This is one of the two access keys for which the table is searched. It is a 4-digit integer value.

- **Local/Remote**—Indicates if the Announcement is to be played on a local gateway or routed to a remote announcement server elsewhere in the network. Values 0-Local (gateway), 1-Remote (gateway).

- **RouteListId**—Indicates the RouteListId that is used to route to a remote announcement server. This dataword is applicable only when dataword2 is set to remote (1).
AnnData—Enables the switching off of a trunk group property Announcement for certain A-numbers or B-numbers. It also enables the applying an announcement for certain A-numbers or B-numbers if no trunk group property has been configured. Values are 0-Off, 1-Interim announcement on, or 2-Final announcement on. This dataword is applicable only when dataword2 is set to local (0).

Action If Announcement Is Disabled

You can allow an analysis ANNOUNCEMENT result to disable (switch off) an Announcement according to the A-number or the B-number. For example, the trunk group property PlayAnnouncement can be provisioned with an Announcement identity to play on all calls delivered to a specific trunk group. Then, later in A-number analysis, an ANNOUNCEMENT result is collected that switches this requirement off (dataword4 = 0). Effectively now there is no Announcement requirement, so Generic Analysis must discard the ANNOUNCEMENT result. When this occurs, there is no ANNOUNCEMENT result or Announcement data returned for further processing.

Action When Announcement Is Enabled by Trunk Group and/or Analysis Result

If an ANNOUNCEMENT result type is received with dataword2 set to 1 (indicating a remote announcement), a Route is forwarded to the remote announcement server. Announcement information is also returned containing all the dataword information that has been collected.

If an ANNOUNCEMENT result type is received with dataword2 set to 0 (indicating a local announcement), then local gateway announcement handling is required. If in the accompanying Announcement data, dataword4 (AnnData) is set to 2 (Final announcement on), this indicates that the Announcement is required and the announcement is treated as a final action (that is, play the announcement and then clear down the call).

If an ANNOUNCEMENT result type is received with dataword2 set to 0 (indicating a local announcement), then gateway announcement handling is required. If in the accompanying announcement data, dataword4 (AnnData) is set to 1 (Interim announcement on), the announcement is required and is treated as an intermediate action (meaning that other results determine the final call processing action). For example, an early announcement case could occur if the MGC initiates the playing of an announcement and then routes the call forward. In this scenario, the announcement data is returned as optional data. However, the main result is set to reflect the end of analysis result retrieved (for example, TRUNK_GROUP, ANALYSIS_PERFORMED (nailed call), or ROUTE (Cause analysis result).

Note

When dealing with these results, first determine if there is announcement data and take the appropriate action.

Times-Ten Database Announcement Table

Once it has been established that Tone or Announcement playing is required, the data must be retrieved to support the MGCP message request to the gateway. Within the MGC, the Times-Ten database holds this data in the Announcement table, which is represented in Table 4.
The Announcement table contains the following fields of data relevant to the Announcement package:

**AnnId**—Indicates the announcement identity (or tone identity), which matches the announcement identity defined by the ANNOUNCEMENT result type. This is one of the two access keys for which the Announcement table is searched for a match. (4-digit integer).

**gwType**—A string containing a value that is part of an enumerated set identifying the gateway type for this side of the call. This is the second access key used to read the Announcement table. (10 characters maximum).

**playDuration**—Indicates the intended duration, in seconds, for which the announcement or tone is played. The default value is 60. Value range: 0 through 120 (4-digit integer).

**repeat**—Indicates the number of times the announcement or tone is repeated; or indicates if it must be played continuously for the specified duration. A value of 0 indicates continuous playing. The default value is 1. Value range: 0 through 5 (4-digit integer).

**interval**—Indicates the silence interval duration, in milliseconds, between re-playing an announcement or tone. Default value: 3000. Value range: 0 through 5000 (4-digit integer).

**locationString**—A string indicating to the gateway the audio file to load to enable announcement or tone playing. The string format varies according to the gateway type and its configuration. The string information is part of a URL string that the MGC sends by MGCP to the gateway. (Maximum length of string: 128-characters).

Note: The gateway is expected to support standard URL schemes for this notation (that is, file, http, or ftp), as described in RFC 1738.

For file or ftp versions, the data provisioned in this field is the required filename, because the gateway is expected to already know the directory location or ftp address.

For example:

- Audiofile1.txt           (file or ftp version, gateway knows where to find the file)
- MyName@host.dom/etc/Audiofile1.txt     (http version, gateway will retrieve the file from this location).

Note: Gateways do not support playDuration, repeat, and interval parameters at this time.

### Obsolete Parameters

The following property is no longer used.
NotifySetupComplete

The NotifySetupComplete property is obsolete and no longer used. Since the Setup complete parameter is required in the terminating CreateConnection (CRCX), NotifySetupComplete is no longer necessary.

Reference Information

The following sections contain reference material related:
- XECfgParm.dat Parameters, page 24
- Alarms, page 24
- Logs, page 25
- Billing Interface, page 25
- Properties, page 27
- Result Type Definitions, page 31

XECfgParm.dat Parameters

For information on the other XECfgParm.dat parameters, refer to the Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide.

Alarms

This section contains the alarms that are added to support this feature.

AnnTableReadingFail

Description: This alarm is raised when reading the Times-Ten database ToneAndAnnouncement table fails.
Severity: Minor
Cause: This alarm can be caused by a provisioning error (for example, provisioning an invalid announcement ID), the use of the wrong database version, or any database (Times-Ten) related problem.
Type: 1 (Communication error)
Action: Check Provisioning. Check Times-Ten database. Verify that all components (Times-Ten database) have the right version for this package. Refer to the “Alarm Troubleshooting Procedures” section of the Troubleshooting chapter of the Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide.

AnnRespTimeout

Description: This alarm is raised when the gateway does not respond to the announcement playing and a timeout occurs.
Severity: Minor
Cause: This alarm can be caused by a provisioning error, the use of the wrong database version, or any database (Times-Ten) related problem.
Type: 1 (Communication error)
MGCP 1.0 and Additional MGCP Packages

Reference Information

Cisco MGC Software Release 9.5(2)

Action

Check why the gateway did not play this announcement. Check the gateway configuration for the announcement. Check that the gateway has that announcement. Verify that the gateway received the announcement request correctly from the MGC. Refer to the “Alarm Troubleshooting Procedures” section of the Troubleshooting chapter of the Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide.

For information on the other alarms for the Cisco MGC software, refer to the Cisco Media Gateway Controller Software Release 9 Messages Reference Guide.

Logs

MGC logs the return codes, except 100, 200, and 250 codes, and their associated commentary. Refer to Table 1 for a list of error and return codes.

Billing Interface

This feature uses the existing Tag 4044 (Announcement Id) for both local and remote announcements. The following billing interface data is added to the MGC software.

ATM Ingress Configured Profile (Tag: 4092)

<table>
<thead>
<tr>
<th>Name: ATM Ingress Configured Profile</th>
<th>Tag: 4092</th>
<th>Source: MDL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description/Purpose: Indicates if an ATM profile was configured, based on the Service Level Agreement (SLA) for the ingress call leg.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Format: IA5</td>
<td>Length in Octets: 1–16</td>
<td></td>
</tr>
<tr>
<td>Data Value:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANSI/ITU Variations: None.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Data Value: No extended value.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Information:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGC Release: Release 9.5 and later.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answered (1010)</th>
<th>Deselected (1020)</th>
<th>Aborted (1030)</th>
<th>Release (1040)</th>
<th>Interrupted (1050)</th>
<th>Ongoing (1060)</th>
<th>Maintenance (1070)</th>
<th>External DB (1080)</th>
<th>End of Call (1110)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
ATM Egress Configured Profile (Tag: 4093)

Table 6  ATM Egress Configured Profile Description Form

<table>
<thead>
<tr>
<th>Name: ATM Egress Configured Profile</th>
<th>Tag: 4093</th>
<th>Source: MDL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description/Purpose: Indicates if an ATM profile was configured, based on the Service Level Agreement (SLA) for the egress call leg.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Format: IA5</td>
<td>Length in Octets: 1–16</td>
<td></td>
</tr>
<tr>
<td>Data Value:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANSI/ITU Variations: None.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Data Value: No extended value.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

General Information:

MGC Release: Release 9.5 and later.

<table>
<thead>
<tr>
<th>Answered (1010)</th>
<th>Deselected (1020)</th>
<th>Aborted (1030)</th>
<th>Release (1040)</th>
<th>Interrupted (1050)</th>
<th>Ongoing (1060)</th>
<th>Maintenance (1070)</th>
<th>External DB (1080)</th>
<th>End of Call (1110)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

ATM Negotiated Profile (Tag: 4094)

Table 7  ATM Negotiated Profile Description Form

<table>
<thead>
<tr>
<th>Name: ATM Negotiated Profile</th>
<th>Tag: 4094</th>
<th>Source: MDL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description/Purpose: Indicates if an ATM profile was negotiated, based on the Service Level Agreement (SLA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Format: IA5</td>
<td>Length in Octets: 1–16</td>
<td></td>
</tr>
<tr>
<td>Data Value:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANSI/ITU Variations: None.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The collection of the profile list information data must be carried out in two places. The level 1 trunk group property information is collected by the MGC and is stored in call context. This is for the situation where analysis does not deliver any results.

Generic analysis typically deals with the level 2 analysis results and adjusts the profile list stored in call context accordingly. However, there is a difference in handling between the originating and terminating sides with regard to the property information.

On the originating side, if the trunk group property has a profile list, the list is collected first. Subsequently, if the analysis result is mandatory, the profile list is overwritten. If the analysis result is preferred, then the result profile list is appended with the trunk group profile list to form a new list.

On the terminating side, the analysis results (if present) are written to call context first. Subsequently, once the Terminating Call Control (TCC) side is determined, the trunk group property is read. Because the analysis results have a higher priority than the trunk group property, however, if the call context variable is written to, then the trunk group profile is not read. This means there is no list-appending on the terminating side.

For correct handling of the data and Call Detail Record (CDR) collection of profile information, the following call context variables are required:

- Ingress Configured Profile
- Egress Configured Profile
- Negotiated Profile

For billing interface information for the rest of the Cisco MGC software, refer to the Cisco Media Gateway Controller Software Release 9 Billing Interface Guide.

### Properties

This section indicates the properties this feature adds, modifies, or deletes in the MGC software. Refer to the Cisco MGC Software Release 9 Provisioning Guide for section setup examples for properties.

The properties in this section are used for this feature. For information on other properties for the Cisco MGC software, refer to the Cisco Media Gateway Controller Software Release 9 Provisioning Guide.

The parent objects for the properties involved in this feature are found in Table 8.
The trunk group property `AtmConnectionType` populates the connection type parameter (ct:) in local connection option parameters. This property is read for both originating and terminating legs of all ATM-switched calls.

Applying MGC influence, that is, bias, in the profile negotiation process is hierarchical and is applied through using the `GWDefaultATMProfile` property at the trunk group level, and then by analysis results in A-number or B-number analysis.

### AtmConnectionType

The trunk group property `AtmConnectionType` populates the connection type parameter (ct:) in local connection option parameters. This property is read for both originating and terminating legs of all ATM-switched calls.

Applying MGC influence, that is, bias, in the profile negotiation process is hierarchical and is applied through using the `GWDefaultATMProfile` property at the trunk group level, and then by analysis results in A-number or B-number analysis.

#### Note

ATM profile negotiation can work over Extended ISUP (EISUP) too.

Valid values: 1 (AAL1), 2 (AAL1_SDT), 3 (AAL1_UDT), 4 (AAL2), 5 (AAL 3/4), 6 (AAL5)

Default value: 4 (AAL2)

### Profile Negotiation Levels

This implementation provides the following structure with regard to ATM profile negotiation when the MGC is involved.

#### Level 0

At level 0, nothing is defined on the MGC. That is, no trunk group properties and no analysis results are defined. This means that the decision for the profile used for the call is made at the gateway level. However, the MGC, using MGCP messages, negotiates between ingress and egress gateway. This is the only role of the MGC at this level.

#### Level 1

At level 1, the MGC can influence the profile negotiation by the trunk group property `GWDefaultATMProfile` configuration on the originating side and even on the terminating side.
With GWDefaultATMProfile configured on the originating side, the MGC offers to the originating gateway the profile list extracted from this property within the CreateConnection (CRCX) request. The originating gateway then matches this received list with its own ActiveProfileList to produce a new list composed of the matched profiles. This list is returned by the gateway to the MGC in the SDP information returned in the CRCX Acknowledgement.

If the terminating side trunk group has this property configured, the retrieved profile list is sent along with the SDP profile list (received previously from the originating side) to the terminating-side gateway.

If no terminating trunk group property is configured, then only the originating-side SDP information is sent.

**Note**
With regard to the terminating side, the trunk group property profile list is read only in the absence of any level 2 results from A-number or B-number analysis.

The MGC passes the originating SDP and any retrieved terminating profile list to the terminating-side gateway in another CRCX message. The egress gateway then matches the received list with its own ActiveProfileList to develop a final list. The egress gateway then chooses from this resultant final profile list, which is transported back to the MGC in the CRCX Acknowledgement message.

Finally, the MGC passes this profile choice to the originating gateway in an MDCX message. Once this exchange has been carried out, only one profile exists for both the ingress and egress gateways, which is the result of profile negotiation (influenced by the MGC applying a bias for the SLA between those gateways).

**Level 2**
At level 2, the MGC can apply another layer of SLA bias to profile negotiation. This additional layer provides the capability of provisioning ATM_ORIG_PROFILE and ATM_TERM_PROFILE results within the MGC A-number and B-number analysis functions. These results contain the same data words and both results deliver a profile list to bias negotiation on either the ingress or egress gateway.

Dataword2 in the result type provides a mandatory or preferred indication for the profile list, which determines the actions that must take place. If dataword2 is set to mandatory, then the profile list from the previous stages is ignored and the egress gateway supports a profile from the list identified by dataword1. If dataword2 is set to preferred, then the profile list identified by dataword1 is retrieved and the existing list (from previous stages, if collected) is appended to the profile list, thus forming a new list to forward to the gateway.

**Note**
If results are collected from A-number analysis and then from B-number analysis, B-number analysis can further adjust or overwrite the existing profile list created by the A-number analysis. This provides the possibility for there being two sublevels within the level 2 capability.

**GWDefaultATMProfile**
When the MGC is acting as a Call Agent making ATM voice connections between two gateways, it must provide the capability to influence the profile negotiation between the two sides to the gateway.

To accomplish this profile negotiation, a list of profiles supported by the code image on the gateway, but is refined by configuration according to the prevailing network Service Level Agreement (SLA). The MGC applies the SLA changes or refinements to the profile list rather than apply them as configuration changes on the gateways. Thus, the gateways contain a list of profiles that their respective code images can support. The MGC retrieves a provisioned profile list from the GWDefaultATMProfile trunk group.
property or as the ATM_ORIG_PROFILE or ATM_TERM_PROFILE result delivered from A-number (Calling number) or B-number (Called number) analysis. This list is then passed over MGCP to the gateway to bias profile negotiation.

While establishing the connection between two gateways, the originating gateway profile list is refined by ANDing with a new profile sent from the MGC in the originating side CRCX message. The resultant profile list is passed in the Session Description Protocol (SDP) to the terminating gateway. Also, the MGC can optionally produce another profile choice to bias the profile on the terminating gateway according to the SLA. This profile accompanies other data sent in the CRCX message to the terminating gateway. Upon receiving this profile, the terminating gateway ANDs the SDP profile with any existing received profiles and then ANDs the profile list with the existing gateway ActiveProfileList to produce a resultant profile list. From the resultant profile list, the gateway chooses a profile entry and passes back the profile list to the originating side.

The MGC produces a profile choice list (ProfileList1) that is sent to the originating gateway in the first CRCX command. The originating gateway forms a new list by ANDing the received profile with its own ActiveProfileList and generates ProfileList2, which consists only of the profile choices that were present in both lists. This profile information is embedded in the SDP that is sent back to the MGC in the CRCX Acknowledgement.

If the MGC also has an SLA profile for the terminating gateway (ProfileList3), it is added to the profile list in the SDP and both profiles are sent to the terminating gateway in another CRCX message. Upon receiving this profile, the terminating gateway ANDs all three lists to produce a single profile list that is refined by the SLA conditions from both sides. The terminating gateway makes a choice from the final profile list that is then sent to the MGC in the CRCX Acknowledgement message and the profile is then sent to the originating gateway in an MDCX message.

Once this process has been carried out, a single profile exists for both the originating and terminating gateway, which is the result of profile negotiation between the two gateways by the MGC and application of the prevailing SLAs.

The trunk group property GWDefaultATMPProfile provides, on a per trunk group basis, an initial list of profiles for use in ATM gateway profile negotiation. This property contains a list of profile choices separated by semi-colons, that influences ATM gateway profile negotiation. If GWDefaultATMPProfile is set to NULL (default), then there is no profile list negotiation bias applied from the trunk group level.

Valid values: NULL, <Profile1>;<Profile2>;<ProfileN>
Default value: NULL

Note

This property is added in propSet.xml.dat for provisioning, added in properties.mod for migration, and added in tpTrunkgroup for importing and exporting.

mgcpBulkAudit

The mgcpBulkAudit SigPath property determines if bulk audit is supported. The mgcpBulkAudit SigPath property contains either an integer (1) indicating that bulk audit is supported on that gateway, or contains a Null (0) indicating that bulk audit is not supported on that gateway.

Valid values: 1 or 0
Default value: 0
**NetworkType**

The trunk group property NetworkType populates the network type parameter (nt:) in local connection parameters. This property is read for both originating and terminating legs of all calls. Based on this property, the MGC software determines if the underlying network is ATM or IP. Based on the network type retrieved, various network-specific parameters (for example, for ATM networks, profiles are sent down) are sent down to gateways.

**Valid values:** 0 (IP), 1 (ATM), 2 (IN)

**Default value:** 0 (IP)

**PlayAnnouncement**

The trunk group property PlayAnnouncement enables, on a per trunk group basis, playing an early announcement. This property can either contain an Integer Announcement Identity, or, if it is set to 0 (default), the announcement function is considered disabled at the trunk group level.

**Valid values:** any integer value greater than 0.

**Default value:** 0

For information on other properties for the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

**Result Type Definitions**

Result analysis provides the capability to group actions into result sets that can be attached at different points of analysis. The main attachment points are: Pre-analysis, A-number analysis, B-number analysis, and Cause analysis.

The following result type definitions are added, modified, or deleted for this feature.

Analysis result types ATM_ORIG_PROFILE (59) and ATM_TERM_PROFILE (60) have been added to deliver an ATM AAL2 profile choice for either A-number or B-number analysis. The profile information is passed from the MGC to the gateway for use in profile negotiations. Additionally, the ANNOUNCEMENT (8) result type has been modified by the addition of dword4 and has become an intermediate analysis point.

**Table 9  Result Type Definitions**

<table>
<thead>
<tr>
<th>Result Number</th>
<th>Result Type</th>
<th>Dataword1</th>
<th>Dataword2</th>
<th>Dataword3</th>
<th>Dataword4</th>
<th>Analysis Points</th>
<th>Result Type Valid For</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Intermediate</td>
<td>End Point</td>
</tr>
<tr>
<td>59</td>
<td>ATM_ORIG_PROFILE</td>
<td>AtmProfIdx</td>
<td>Action</td>
<td>0 (not used)</td>
<td>0 (not used)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>60</td>
<td>ATM_TERM_PROFILE</td>
<td>AtmProfIdx</td>
<td>Action</td>
<td>0 (not used)</td>
<td>0 (not used)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>ANNOUNCEMENT</td>
<td>Announcement  ID</td>
<td>Local/Remote</td>
<td>RouteListId</td>
<td>AnnData</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
**ATM_ORIG_PROFILE/ATM_TERM_PROFILE**

Dataword1—AtmProfIdx provides an index value that is used to read the ATM Profiles table from the routeAnalysis.dat file. This enables retrieving a list of ATM profiles for use in the profile negotiation process.

Dataword2—Action provides an indication as to whether this profile list is to be considered preferred or mandatory. Values are: 0 (mandatory) or 1 (preferred).

Possible profile entries are:
- ITU1
- ITU2
- ITU3
- ITU7
- ITU8
- ITU12
- Custom100
- Custom101
- Custom110
- Custom200

MML provisioning for analysis results ATM_ORIG_PROFILE and ATM_TERM_PROFILE can be performed for either the A-numbers or the B-numbers.

Supporting routeAnalysis.dat table ATMProfiles

To support the ATM result types, ATM_ORIG_PROFILE and ATM_TERM_PROFILE, a table is used to provide the list of ATM profiles. The profile list is assigned a name during provisioning, and a semicolon-separated list of profile choices is entered against this name.

The format of the routeAnalysis table is as follows:

```
$ATMProfiles
# CiscoMGC: 01
#name                ATMProfiles
atmprof1            ITU1;cust100
```

Data words

Dataword1—AnnouncementId. This integer represents the announcement identity. This value interrogates the tone and announcement table and retrieves the data for the MGCP message.

Dataword2—Local/Remote. Indicates if the announcement is locally supported (that is, on an MGC-controlled gateway) or remotely supported (that is, routed forward to an announcement server).

Dataword3—RouteListId. This integer is required only for routing to a remote announcement server and is not applicable when gateway announcements are used.

Dataword4—AnnData. This integer indicates if the announcement is applied or not and indicates if the announcement signals the end of a call or continued processing. Valid values: 0 or NULL=OFF, 1=INTERIM_ON, or 2=FINAL_ON.

---

**Note**

Dataword4 (AnnData) indicates if the requirement is to play an announcement and then clear down (FINAL_ON) or play an announcement and then continue processing (INTERIM_ON).
For information on other result type definitions for the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

The ANNOUNCEMENT result type has been modified to become an Intermediate result type. This result type is now available to the Pre-analysis and A-number analysis areas, in addition to Cause and B-number analysis.

**ANNOUNCEMENT**

The ANNOUNCEMENT result type within generic analysis has been modified by introduction of the processing of Dataword4, which indicates if an announcement is to be applied. This modification provides the ability to override a trunk group property setting according to this analysis result.

**AnnouncementId**—Identification value corresponding to the announcement that is played to the caller (INTEGER value).

**Local/Remote**—Indicates if the announcement is to be played on a local gateway or routed out to a remote announcement server elsewhere in the network. Values: 0 = Local (gateway) or 1 = Remote (gateway).

**RouteListId**—Indicates the RouteListId that is used to start routing analysis to route to a remote announcement server (INTEGER value).

**AnnData**—Enables or disables the announcement trunk group property for certain A-numbers and B-numbers or applies an announcement for certain A-numbers and B-numbers where no trunk group property has been configured. Values: 0 = Off, 1 = Interim Announcement On, or 2 = Final Announcement On.

**Cause and Location Codes**

The MGCP 1.0 and Additional MGCP Packages feature supports the cause codes listed in Table 10 in the MGC software. RETURN codes listed in the first column of Table 10 are mapped to internal cause values. The values listed in Table 10 are for reference purposes only.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause Value</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Transaction being executed. Completion response to follow.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>Trans_Executed_Normally</td>
<td></td>
<td></td>
</tr>
<tr>
<td>250</td>
<td>Connection_Deleted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>Trans_Not_Executed_Transient_Error_400</td>
<td>32</td>
<td>IC_NORMAL_UNSPECIFIED</td>
</tr>
</tbody>
</table>

**Transient Error**—It is used to respond to commands when the requested command cannot be processed at the current time; however, the expectation is that if the same command is requested in the very near future, it may succeed.
Table 10  Return Codes with Descriptions and Internal Cause Value Mapping (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause Value</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>401</td>
<td>PhoneAlready_Off_Hook_401</td>
<td>52</td>
<td>IC_USER_BUSY</td>
</tr>
<tr>
<td></td>
<td>The Phone is already off hook—It is returned to respond to an off-hook transition request while the phone is already off-hook. It is also returned when a request is made to generate a signal that is inappropriate for a phone that is off-hook. For example, S: l/rg, which is a request to ring the phone.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>402</td>
<td>Phone is already on-hook—It is returned to respond to an on-hook (or hook-flash) transition request (RQNT) while the phone is already on-hook. It is also returned when a request is made to generate a signal that is inappropriate for a phone that is on-hook. For example, S: l/dl, which is a request to play a tone, such as dial-tone.</td>
<td>52</td>
<td>IC_USER_BUSY</td>
</tr>
<tr>
<td>403</td>
<td>Trans_Not_Executed_End_Pt_Insuff_Res_403</td>
<td>44</td>
<td>IC_RESOURCES_UNAVAIL_UNSPEC</td>
</tr>
<tr>
<td></td>
<td>Endpoint does not have sufficient resources — It is returned if the request cannot be processed due to unavailability of pooled resources, such as CPU utilization, lack of DSP resources, lack of memory, and so on. However, the command may succeed at a later time when resources free up.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>404</td>
<td>Trans_Not_Executed_End_Pt_Insuff_Bandwidth_404</td>
<td>44</td>
<td>IC_RESOURCES_UNAVAIL_UNSPEC</td>
</tr>
<tr>
<td></td>
<td>Insufficient Bandwidth—It is returned to requests when the gateway does not have enough bandwidth to establish the connection. As an example, the gateway shall use this error code to indicate the presence of RSVP failures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>405</td>
<td>Trans_Not_Executed_Endpoint_Restarting_405</td>
<td>77</td>
<td>IC_SERVICE_TEMPORARILY_UNAVAILABLE</td>
</tr>
<tr>
<td></td>
<td>Endpoint is restarting—It is returned to requests when the gateway has initiated the Restart Procedures (RSIP) on an endpoint.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>Trans_timed_out_406</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td></td>
<td>Transaction Timeout — It is returned following a 100 code, if the request did not complete in a reasonable period of time and has been aborted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 10  Return Codes with Descriptions and Internal Cause Value Mapping (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>407</td>
<td>Trans_aborted_407</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td></td>
<td><strong>Transaction Aborted</strong>—It is returned to cancel a pending request. For example, DLCX is received during the processing of a CRCX or MDCX, or the same command is received with another transaction ID.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>Trans_Not_Executed_End_Pt_Uknown_500</td>
<td>33</td>
<td>IC_NO_ROUTE_TO_DEST</td>
</tr>
<tr>
<td></td>
<td><strong>Endpoint is unknown</strong>—It is returned if the endpoint ID supplied in the request is unknown.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>501</td>
<td>Trans_Not_Executed_End_Pt_Not_Ready_501</td>
<td>59</td>
<td>IC_DTE_CONTROLLED_NOT_READY</td>
</tr>
<tr>
<td></td>
<td><strong>Endpoint is not ready</strong>—It is returned if the endpoint is in a permanent not ready state. This includes maintenance states, such as out of service and auto out of service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>502</td>
<td>Trans_Not_Executed_End_Pt_Insuff_Res_502</td>
<td>44</td>
<td>IC_RESOURCES_UNAVAIL_UNSPEC</td>
</tr>
<tr>
<td></td>
<td><strong>Endpoint does not have sufficient resources</strong>—It is returned when the endpoint does not have sufficient resources and future requests on this endpoint are guaranteed to fail. It indicates that the resources dedicated to the endpoint are broken.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>503</td>
<td>WildCardsTooComplicated_503</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>All of wildcard too complicated</strong>—It is returned when the wildcard convention used in the request is understood, but the requested command cannot be processed with wildcarding. An example of this would be an RQNT with a request such that a failure would make it too difficult to roll back the state of all the endpoints to what they were prior to the request.</td>
<td></td>
<td>MDL does not map this return code to an internal cause value. The MGC internally handles this return code.</td>
</tr>
<tr>
<td>509</td>
<td>SdpError_509</td>
<td>23</td>
<td>IC_MSG_IN_WRONG_STATE</td>
</tr>
<tr>
<td></td>
<td><strong>SDP error</strong>—It is returned if the SDP has parameters or attributes that are not recognized or parameters that are recognized but not consistent with the state of the connection. The gateway should ignore attributes that it does not recognize. Also as indicated in the MGCP specification, gateways should generate o, t, and s lines but be lenient if they do not receive them.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 10  Return Codes with Descriptions and Internal Cause Value Mapping (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause Value</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>510</td>
<td>Trans_Not_Executed_Protocol_Error_510</td>
<td>38</td>
<td>IC_PROTOCOL_ERROR_UNSPEC</td>
</tr>
<tr>
<td></td>
<td>Protocol Error—It is returned if the requested command is not in compliance with the MGCP specification. Because this is a least specific error code, it is especially important that gateways provide supporting commentary text to reflect the nature of the error.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>511</td>
<td>Trans_Not_Executed_Unrecognised_Ext_511</td>
<td>38</td>
<td>IC_PROTOCOL_ERROR_UNSPEC</td>
</tr>
<tr>
<td></td>
<td>Unrecognized extension—It is returned if the requested command contains an unrecognized X+ extension. In MGCP 1.0, this specifically refers to unrecognized parameters, because other error codes are available for unrecognized connection modes (517), unrecognized packages (518), unrecognized LCO(541), and so on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>Gateway_Unequipped_To_Detect_Request_512</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td></td>
<td>GW not equipped to detect event—It is returned if the gateway is not equipped to detect one or more of the requested events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>Gateway_Unequipped_To_Generate_Signal_513</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td></td>
<td>GW not equipped to generate signal—It is returned if the gateway is not equipped to generate one or more of the requested signals.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>Gateway_Cannot_Send_Announcement_514</td>
<td>8</td>
<td>IC_CALL_REJECTED</td>
</tr>
<tr>
<td></td>
<td>The gateway is not able to send an announcement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>515</td>
<td>Incorrect_Connection_ID_515</td>
<td>17</td>
<td>IC_INVALID_CALL_REFERENCE_VALUE</td>
</tr>
<tr>
<td></td>
<td>Invalid Connection ID—It is returned if the connection ID supplied in the request refers to an unknown Connection ID. The connection ID can also supplied with events and signals (for example, S: L/rt@connId) or in the SDP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>516</td>
<td>Unknown_Call_ID_516</td>
<td>17</td>
<td>IC_INVALID_CALL_REFERENCE_VALUE</td>
</tr>
<tr>
<td></td>
<td>Unknown/Invalid Call ID—It is returned if the call ID supplied in the request refers to an unknown Call ID.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 10  Return Codes with Descriptions and Internal Cause Value Mapping (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause Value</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>517</td>
<td>Unsupported_Mode_517</td>
<td></td>
<td>IC_SERVICE_UNAVAILABLE</td>
</tr>
<tr>
<td></td>
<td><strong>Unsupported/Invalid mode</strong>—It is returned if the command</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>specifies a connection mode that the endpoint does not support.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>518</td>
<td>Unsupported_Package_518</td>
<td></td>
<td>IC_CALL_TYPE_INCOMPATIBLE</td>
</tr>
<tr>
<td></td>
<td><strong>Unsupported/Invalid package</strong>—It is returned if the command</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>specifies an unsupported or invalid package.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>519</td>
<td>Gateway_Does_Not_Have_Digit_Map_519</td>
<td></td>
<td>IC_REQ_FACILITY_NOT_IMP</td>
</tr>
<tr>
<td></td>
<td><strong>Endpoint does not have a digit map</strong>—It is returned if the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>request is to accumulate digits according to the digit map and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the endpoint does not have a digit map.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>520</td>
<td>Trans_Not_Executed_End_Pt_Restarting_520</td>
<td></td>
<td>IC_SERVICE_TEMPORARILY_UNAVAILABLE</td>
</tr>
<tr>
<td></td>
<td><strong>Endpoint restarting</strong>—This code may be deprecated. Future</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>implementation should use 405, instead.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>521</td>
<td>Endpoint is redirected to another call agent.</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The gateway does not send this return code to the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGC. Also the MGC will not generate this return code at this</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>522</td>
<td>NoSuch_Signal_Event_522</td>
<td></td>
<td>IC_SERVICE_OR_OPTION_NOT_IMP_UNSPEC</td>
</tr>
<tr>
<td></td>
<td><strong>No such signal or event</strong>—It is returned if the requested</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>event or signal name is not registered with this package.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>523</td>
<td>IllegalCombination_Of_Actions_523</td>
<td></td>
<td>IC_SERVICE_OR_OPTION_NOT_AVAIL</td>
</tr>
<tr>
<td></td>
<td><strong>Unknown action or illegal combination of actions</strong>—It is</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>returned if the request contains an invalid or an unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>action or an illegal combination of actions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>524</td>
<td>InConsistency_LCO_524</td>
<td></td>
<td>IC_PROTOCOL_ERROR_UNSPEC</td>
</tr>
<tr>
<td></td>
<td><strong>Internal inconsistency in LocalConnectionOptions (LCO)</strong>—It</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is returned if one or more of LCO parameters are coded with</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>values that are not consistent with each other or with the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>network type.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco MGC Software Release 9.5(2)
### Table 10  Return Codes with Descriptions and Internal Cause Value Mapping (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause Value</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>525</td>
<td>UnknownExt_LCO_525</td>
<td>47</td>
<td>IC_SERVICE_OR_OPTION_NOT_AVAIL</td>
</tr>
<tr>
<td></td>
<td><strong>Unknown extension in LCO</strong>—It is returned if the request contains one or more unrecognized X+ extensions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>526</td>
<td>Insufficient_BandWidth_526</td>
<td>44</td>
<td>IC_RESOURCES_UNAVAIL_UNSPEC</td>
</tr>
<tr>
<td></td>
<td><strong>Insufficient Bandwidth</strong>—Refer to code 404. Future implementation should use 404, instead.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>527</td>
<td>Missing_RemoteConn_Descriptor_527</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td></td>
<td><strong>Missing RemoteConnectionDescriptor</strong>—It is returned if the requests do not contain the RemoteConnectionDescriptor when one is required to support the requested connection mode or a signal to be applied on the connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>528</td>
<td>InCompatible_Protocol_Version_528</td>
<td>105</td>
<td>IC_REMOTE_PROC_ERROR</td>
</tr>
<tr>
<td></td>
<td><strong>Incompatible protocol version</strong>—It is returned if the protocol version does not match the protocol version(s) it was configured to support.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>529</td>
<td>HardWare_Failure_529</td>
<td>26</td>
<td>IC_NETWORK_OUT_OF_ORDER</td>
</tr>
<tr>
<td></td>
<td><strong>Hardware Failure</strong>—It is returned if an endpoint experiences a hardware fault during the execution of a command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the hardware fault forces an endpoint to go out of service, an Restart In Progress (RSIP) is sent. Any command rejected due to an endpoint being out-of-service generates error code 501.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>530</td>
<td>Cas_Signaling_Protocol_Error_530</td>
<td>105</td>
<td>IC_REMOTE_PROC_ERROR</td>
</tr>
<tr>
<td></td>
<td>CAS signaling protocol error.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>531</td>
<td>FailureOf_Grouping_Trunks_531</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td></td>
<td><strong>Failure of a grouping of trunks (facility failure)</strong>—It is returned if an endpoint being grouped becomes unavailable during the execution of a command due to a facility (for example, T1) failure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the facility failure forces an endpoint to go out of service, an RSIP is sent. Any command rejected due to an endpoint being out-of-service generates error code 501.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 10  Return Codes with Descriptions and Internal Cause Value Mapping (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Internal Cause Value</th>
<th>Internal Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>532</td>
<td>Unsupported values in LocalConnectionOptions—It is returned if one or more of the LCO parameters is coded with an unsupported value and the gateway does not have the authority to override the parameter value that is in error.</td>
<td>38</td>
<td>IC_PROTOCOL_ERROR_UNSPEC</td>
</tr>
<tr>
<td>533</td>
<td>Response Too Large—This is likely to occur only in the case of an audit where the maximum response packet size is too large.</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td>534</td>
<td>Codec Negotiation Failure—It is returned if the negotiated list of codecs is empty.</td>
<td>14</td>
<td>IC_FACILITY_REJECTED</td>
</tr>
<tr>
<td>535</td>
<td>Packetization Period not supported—It is returned if the LCO contains an unsupported packetization period with no codec specified.</td>
<td>47</td>
<td>IC_SERVICE_OR_OPTION_NOT_AVAIL</td>
</tr>
<tr>
<td>537</td>
<td>Unsupported DigitMapExt—Unknown or unsupported digit map extension.</td>
<td>47</td>
<td>IC_SERVICE_OR_OPTION_NOT_AVAIL</td>
</tr>
<tr>
<td>538</td>
<td>Event/Signal parameter error—It is returned if the event or signal parameter is in error or not supported.</td>
<td>47</td>
<td>IC_SERVICE_OR_OPTION_NOT_AVAIL</td>
</tr>
<tr>
<td>539</td>
<td>Invalid Unsupported CommandParam—It is returned if the command contains an invalid or unsupported parameter, which is neither a package nor a vendor-specific extension.</td>
<td>47</td>
<td>IC_SERVICE_OR_OPTION_NOT_AVAIL</td>
</tr>
<tr>
<td>540</td>
<td>Per endpoint connection limit exceeded.</td>
<td>50</td>
<td>IC_TEMPORARY_FAILURE</td>
</tr>
</tbody>
</table>
Bulk Audit

The Cisco MGC supports the MGCP Bulk Audit Package, as defined in the IETF RFC 3624 (which is a subset of the specification implemented to support basic bulk audit). The MGCP Bulk Audit Package is used by the Call Agent to determine the connection and endpoint state for a group of endpoints on the gateway.

Bulk audit is more resource efficient than a regular audit on a single endpoint. For a single endpoint audit, the Call Agent has to send an audit message for each endpoint. However, for bulk audit, the Call agent has to send only one bulk audit message for a group of endpoints. Bulk audit significantly reduces the number of messages exchanged between the Call Agent and the gateway during the audit.

The bulk audit support is implemented in the MGC. The MGC uses the following parameters to determine the connection and endpoint state: BA/C, BA/S(I), BA/SE and BA/NU.

Bulk audit messages are used to exchange information between the MGC and the gateway. The bulk audit (BA) message parameters are:

- BA/C: connection count list
- BA/EL: endpoint list
- BA/F: request info
- BA/M: connection mode list
- BA/NE: next endpoint ID
- BA/NU: maximum number of endpoints

For information on other cause and location codes for the Cisco MGC software, refer to the Cisco Media Gateway Controller Software Release 9 Dial Plan Guide.
The gateway property mgcpBulkAudit is defined to enable the bulk audit for a specified gateway. The property can be set 0 (disabled bulk audit for single endpoint audits to take place) or 1 (enable bulk audit). The default value is set to 0.

### Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

#### Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:


#### Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/
Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:


From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- **Emergencies** — security-alert@cisco.com
  
  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- **Nonemergencies** — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:


The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.
Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- **Cisco Marketplace** provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
  

- **Cisco Press** publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  [http://www.ciscopress.com](http://www.ciscopress.com)

- **Packet magazine** is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:


- **iQ Magazine** is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:


  or view the digital edition at this URL:


- **Internet Protocol Journal** is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  [http://www.cisco.com/ipj](http://www.cisco.com/ipj)

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:


- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  [http://www.cisco.com/discuss/networking](http://www.cisco.com/discuss/networking)

- World-class networking training is available from Cisco. You can view current offerings at this URL:

Table 11 contains definitions of acronyms and technical terms used in this document.

**Table 11 Acronym Definitions**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL</td>
<td>ATM Adaptation Layer</td>
</tr>
<tr>
<td>ACM</td>
<td>Address Complete Message</td>
</tr>
<tr>
<td>AUEP</td>
<td>Audit Endpoint</td>
</tr>
<tr>
<td>AUGW</td>
<td>Audit Gateway</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Detail Record</td>
</tr>
<tr>
<td>CPC</td>
<td>ISUP Calling Party Category</td>
</tr>
<tr>
<td>CPM</td>
<td>Connection Plane Manager</td>
</tr>
<tr>
<td>CRCX</td>
<td>Create Connection</td>
</tr>
<tr>
<td>EISUP</td>
<td>Extended ISUP</td>
</tr>
<tr>
<td>LCO</td>
<td>Local Connection Option</td>
</tr>
<tr>
<td>MDCX</td>
<td>Modify Connection</td>
</tr>
<tr>
<td>MGC</td>
<td>(Cisco) Media Gateway Controller</td>
</tr>
<tr>
<td>MGCP</td>
<td>Media Gateway Control Protocol</td>
</tr>
<tr>
<td>MML</td>
<td>Man-Machine Language</td>
</tr>
<tr>
<td>NOA</td>
<td>Nature of Address</td>
</tr>
<tr>
<td>NTFY</td>
<td>Notify</td>
</tr>
<tr>
<td>PGW</td>
<td>PSTN Gateway, also called the MGC</td>
</tr>
<tr>
<td>PTCC</td>
<td>Packet Telephony Call Control</td>
</tr>
<tr>
<td>RQNT</td>
<td>Notification Request</td>
</tr>
<tr>
<td>RSIP</td>
<td>Restart In Progress</td>
</tr>
<tr>
<td>SC</td>
<td>Signaling Controller</td>
</tr>
<tr>
<td>SDP</td>
<td>Session Definition Protocol</td>
</tr>
<tr>
<td>SDT</td>
<td>Structured Data Transfer</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SRCP</td>
<td>Simple Resource Control Protocol</td>
</tr>
<tr>
<td>TCC</td>
<td>Terminating Call Control</td>
</tr>
<tr>
<td>TMR</td>
<td>Transmission Medium Requirement</td>
</tr>
<tr>
<td>UDT</td>
<td>Unstructured Data Transfer</td>
</tr>
<tr>
<td>VSC</td>
<td>Virtual Switch Controller</td>
</tr>
</tbody>
</table>