DPNSS Supplementary Services Interworking with Cisco CallManager

Document Release History

Publication Date	Comments
January 20, 2006	Initial version of the document.

Feature History

Release	Modification
9.4(1)	The DPNSS Transparency feature was introduced on the Cisco MGC software.
9.6(1)	The DPNSS Supplementary Services feature was introduced on the Cisco MGC software.

This document describes DPNSS Supplementary Services Interworking with Cisco CallManager Feature. This feature is described in the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Feature Overview

This feature enables end users to interwork their legacy DPNSS PBXs with Cisco CallManager, and extends the set of features that interwork to:

Note When DPNSS features are inter-worked between a legacy DPNSS PBX network and Cisco CallManager (and vice-versa), the given features mimic the implementation as they function in a DPNSS network.

Add-on Conference

The Add-On Conference Supplementary Service permits the controller of a three-party service conference to extend it to four or more parties.

This Supplementary Service allows a three-party service conference to grow to four or more parties, depending on the capacity of the conference bridge in use at the conference PBX. The number of parties in a conference can vary.

When the conference involves three parties, both Three-Party Service and Add-On Conference services are available; but when the conference has four or more parties, only Add-On Conference Service is available. If the number of parties goes down to two, the conference reverts to a simple call.

This feature allows all the parties involved in a call to do the following:

- Place the conference on hold and make an add-on enquiry call, using Single-Channel Working as far as the conference PBX to facilitate subsequent add-on. Following establishment, shuttle between the enquiry call and the conference, and release of the enquiry call are possible. The Hold supplementary service may be used to place the conference on hold.

- Add the called party of an Add-On Enquiry Call on to the conference.
- Clear down the complete conference.
- Split a selected party away from the conference to talk in private to or release that party (not supported from Cisco CallManager to PBX).
- Obtain details of parties currently participating in the conference (not supported from Cisco CallManager to PBX).
- Clear from the conference.

Call Diversion

Call Diversion (also known as Call Forward) offers users who are absent or busy the capability of having their calls forwarded to a third party.

The following variations are supported for a DPNSS extension to a Cisco CallManager (IP) extension:

- Call Diversion—No Reply (Call Forward No Answer)

  Limitation: This feature does not work with a call from an IP Phone user to a DPNSS phone with the default Media Gateway "Trigger for SDP Transmit to H.323" setting of Address Complete.

  For this feature to work, set the trigger to Answer.

  If you set the trigger to Answer and you are also using either of the following methods for PSTN access to Cisco CallManager:

  – a connected PBX

  – the Cisco PGW 2200

  then forwarded calls to busy or unanswered PSTN numbers will get a ring tone instead of the inband busy tone or announcement.

  In the first case, you can avoid the problem by setting the PBX to not allow in-band Q.931 information to pass through to the DPNSS network. If you cannot do this, change the point of PSTN access to the Cisco CallManager. There is no workaround for the second case; we do not recommend using PSTN Interconnect if you want full CFNA interworking.
- Call Diversion—Busy
- Call Diversion—Immediate

The following variations are supported for a Cisco CallManager (IP) extension to a DPNSS extension:

- Call Diversion—No Reply
- Call Diversion—Busy
- Call Diversion—Immediate

Call Diversion Validation

Call Diversion Validation (Also known as Call Forwarding Validation) ensures that when a PBX user attempts to forward a call, the PBX generates a virtual call to that phone number containing a specified string.

If the Cisco PGW 2200 receives a virtual call containing this string that has the routing number and finds an available outgoing route, then the PGW acknowledges the request. Otherwise, the PGW rejects the call with appropriate cause.

For on-net diversions, the PGW provides transparency only.

Call Offer

The Call Offer service enables the Calling party to indicate to the called party on an already established call that another call is being offered. The Call Offer service is a calling party service.

A user on an existing call is given an indication (Call Waiting Indication) that another call is incoming to his line. At the same time, the calling party is given an in-channel indication that the called extension is receiving a Call Waiting signal. The called party can choose to do one of the following:

- Terminate the existing call and be automatically re-rung.
- Hold the existing call and answer the new call.
- Reject the Call Waiting Indication.
- Ignore the Call Waiting indication.

Note As an option, the calling party may convert from offering the call to Executive Intrusion on the call but this is not supported.

Cisco PGW 2200 will interrogate, on behalf of the DPNSS PBX, the appropriate extension on Cisco CallManager. If the Cisco CallManager extension is busy, because of one of the following scenarios:

- All the available multiple line appearances on the phone are busy
- There is only a single line appearance on the phone
- There is no Call Waiting service provisioned against the extension

the end user will be presented with the option to accept the call offer.

For XML-enabled phones connected to CallManager, the PGW 2200 will provide a tone and a XML-based visual indication (to a soft key) giving the end-user the option to accept the call. If the call is not accepted within a pre-determined time (configurable on a global basis), the timer will expire and the offer withdrawn.

Call Offer is not supported for:

- Non XML-enabled phones connected to Cisco CallManager,
- Analog (non-Cisco IP phones) connected to Cisco CallManager
- Converting to executive intrusion.

Call Transfer

The Call Transfer service supports call transfers between DPNSS PBXs and the Cisco CallManager. It supports transfers between an IP Phone connected to a Cisco CallManager and a phone connected to a DPNSS PBX.

The connected number display will be updated on the phone of the other connected parties which could be either on Cisco CallManager or the DPNSS PBX. It also supports transfer from PBX to Cisco CallManager with the final connected number display updated on the phone of the calling party which could be on either the Cisco CallManager or the DPNSS PBX.

For example, a caller A on Cisco CallManager is talking to caller B on a DPNSS PBX. When caller B transfers the original call to caller C on Cisco CallManager, the connected number display on both ends is updated to show the numbers of caller A and caller C.

Call Waiting

The Call Waiting Supplementary Service (CW) enables an extension user to request that an indication be given if there is an incoming call when the extension is busy on another call. The Call Waiting service is a called-party service.

A user on an existing call is given an indication (Call Waiting Indication) that there is another incoming call to his line, while the calling party is given an audible indication that Call Waiting Indication is being given to the called extension. The called party can choose to do one of the following:

- Terminate the existing call and be automatically re-rung.
- Hold the existing call and answer the new call.
- Reject the Call Waiting Indication. (Cisco CallManager can not reject the Call Waiting Indication.)
- Ignore the Call Waiting indication.

Calling Name Display

This feature allows DPNSS Calling Name Display to be interworked in both directions with CCM. When Cisco IP phone users receive a call from a user on the PBX, the name and number of the caller are displayed on the receiving phone. Also, when a user on the PBX receives a call from a user on the Cisco IP phone, the name and number of the person calling is again displayed on the receiving phone.

Centralized Operator

The Centralized Operator Service allows operators to assist with the connection of calls, without the need to provide and staff operator positions at every PBX in the DPNSS network.

Note The Centralized Operator feature is not supported from Cisco CallManager to DPNSS PBX.

Where operators are centralized, with operators on one PBX providing a service for a number of PBXs, the following DPNSS Supplementary Services must be supported:

- Three Party Service—The PBXs in the network must support Three-Party Service and use the procedures of that service when extensions or operators make enquiry calls and perform subsequent actions such as transfer.
- Call Offer—An operator must have the facility to offer an incoming call to a busy extension (Camp On). This is achieved by using the call offer service in conjunction with the three-party service. When the operator requests Camp On, the operator establish a call offer call to the called extension. If this is successful, the calling party "on offer"is transferred to the called extension. All PBXs for which the operator PBX provides service must be capable of accepting a Call Offer request.
- Redirection—All PBXs in the DPNSS network must support the Redirection Service to redirect a call back to the operator which has been transferred by an operator to an extension which has not answered and fails to answer within a certain time. This includes calls which have been transferred on offer to a busy extension and fail to progress within a certain time.

- Night Service—Night Service is essential where sophisticated night service arrangements are required. for example, local night-answering points. If a night service point is provided on the Operator PBX for use by all types of caller, there may not be a need for the DPNSS Night Service feature.
- Extension Status—The Extension Status feature allows operators the capability of determining the status of an extension without causing a ring.
- Controlled Diversion Service—When the Call Diversion Service is used, Controlled Diversion Service can allows operators to exercise control over any diversions encountered when establishing calls.
- Series Call—The Series Call Service allows operators to give series call capability to callers from other PBXs.
- Three-Party Takeover—The Three-Party Takeover Service allows operators to take control of a three-party situation after answering an enquiry call from an extension on another PBX (the extension that has a third party on hold)
- Hold Service—When Hold Service is used, the Operator PBX should reject any end-to-end message (EEM) containing HOLD-REQ from any party connected to an operator. A PBX should avoid sending an EEM containing HOLD-REQ when the distant party is an operator. Hold requests from extensions should be rejected locally. It is not necessary to use the procedures of the Hold Service when an operator places a party on hold in order to make an enquiry call. Transfer will normally occur within a few seconds and there is little point in supplying a holding indication to the held party for such a short duration. If the operator places a party on hold for another reason (e.g. to attend to another call or await a response to paging), the procedures of the Hold Service should be used.

Note The Centralized Operator feature is not supported from Cisco CallManager to DPNSS PBX.

Extension Status

The Extension-Status Call Supplementary Service offers the capability of determining, on request, the status of an extension. This service permits the establishment of a virtual call to an extension in order to determine its state that is, free, busy, out of service, diverted, etc., without calling the extension.

It might be used by an operator, before the establishment of a call on behalf of an extension, to improve the chances of the extension being free when the call is ready. It might also be used to investigate complaints.

Note Extension Status is not supported from CallManager to DPNSS PBX.

Loop Avoidance

Loop Avoidance prevents certain loops from occurring when calls are set up between DPNSS PBXs and CCM.

Message Waiting Indicator

The MWI feature enables a DPNSS-based voicemail system the ability to light the MWI lamp on a Cisco IP Phone connected to a Cisco CallManager (CCM). The Cisco PGW 2200 interworks the signal from DPNSS to a specific call to CCM to set or clear the MWI lamp.

Night Service

The Night Service Supplementary Service provides alternative answering arrangements for calls to operators at times when normal operator positions are unattended.

An operator group or specific position can be put into Night Mode when unattended. You can activate or deactivate the Night Mode in several ways. For example, each operator position may be switched into or out of Night Mode; an operator group is in Night Mode when all the positions in the group are in Night Mode. Alternatively, Night Mode may be activated and deactivated at particular times of day.

Note Cisco CallManager cannot be the night service answering point.

Redirection

The Redirection Supplementary Service offers callers awaiting connection or reconnection the option of being redirected to an alternative destination after a certain time. Redirection is initiated by the waiting party's PBX if the call does not progress within a certain time. A call redirection can also be requested from the terminating switch. Additionally, a failed call may be redirected to an alternative destination immediately.

Three Party Service

This Supplementary Service permits a user who has placed an existing call into a suspended or on-hold state to make an enquiry call to a third party. The controlling party may then make use of any of the following service options:

- Shuttle—The connection is switched so that the controlling party is connected to the party who was on hold, and the party to whom the controlling party was connected is placed on hold. By repeated use of this option the controlling party may speak to each of the other two parties alternately. The party to whom the controlling party is currently connected is known as the connected party. Before the first Shuttle, the enquired-to party is the connected party.
- Transfer—A connection is established between the two non-controlling parties and the controlling extension is released.
- Add-On—The three parties are connected together to form a three-party conference.

Restrictions

- For the Message Waiting Indication service, only MWI messages originating from DPNSS-based voicemail systems are supported.

- If a call is being transferred from PBX to Cisco CallManager to PBX, loop avoidance is not supported.
- The following Cisco access gateways support DPNSS signaling backhaul:
  - Cisco 2600 Multiservice Router
  - Cisco 3600 and 3660 Multiservice Router
- There are some limitations with the interworking of the Call Diversion feature with CCM, explained in the following two scenarios:
  - **Scenario 1**: There is a PBX phone A which registered a Call Diversion on-busy service and the forwarded-to party is PBX phone B in another PBX. A CCM IP phone calls PBX phone A, but phone A busy, so this call is forwarded to phone B. But phone B does not answer. The CCM IP phone invokes the Call Back When Next Used (CBWNF) feature. The expected result is that the CBWNU should target the phone A and CBWNU should be converted to Call Back When Free (CBWF). The actual result is that the CBWNU feature is targeted on phone A, not the CBWF.
  - **Scenario 2**: A CCM IP phone calls PBX phone A. Since PBX phone A has call forward immediate, this call is forwarded to phone B in another PBX, but phone B happens to be busy. So the CCM IP phone invokes the Call Back When Free feature. This Call Back When Free should be sent to PBX phone B. But the actual result is that it is sent to PBX phone A.

Related Features and Technologies

The following documentation is available to describe additional features on the PGW 2200 (MGC) and IOS Gateways that enable interworking between DPNSS PBXs and Cisco CallManager.

- DPNSS Route Optimization

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mgcfm/96/FMdp_rop.htm
- DPNSS Call Back And Extension Status Interworking with Cisco CallManager

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mgcfm/96/fmcbk_ex.htm
- DPNSS Feature Transparency

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mgcfm/941fm/fmdpnss.htm

Related Documentation

This document contains information that is related strictly to this feature. The documents that contain additional information related to the Cisco Media Gateway Controller (MGC) are listed below and can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/index.htm

- *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*
- *Release Notes for Cisco Media Gateway Controller Software Release 9.6(1)*
- *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 Operations, Maintenance, and Troubleshooting Guide*
- *Cisco Media Gateway Controller Software Release 9 MML Command Reference Guide*
- *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*

Supported Standards, MIBs, and RFCs

This section identifies the new or modified standards, MIBs, or RFCs that are supported by this feature.

Standards

- Digital Private Network Signaling System DPNSS 189 Issue 4 - Interworking Between DPNSS1 and Other Signaling Protocols

  http://www.nicc.org.uk/nicc-public/Public/interconnectstandards/dpnss/nd1302_2001_12.pdf

MIBs

New MIBs are available for this feature. There is a new MIB for each new measurement. You can find a list of the new measurements in Measurements, page 41. For more information on the MIBs used in the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Management Information Base Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mgc_mib/index.htm

RFCs

- SCTP – RFC-2960
- IUA – RFC-3057

Prerequisites for This Feature

You must have Cisco MGC software Release 9.6(1). Prerequisites for this release can be found in the *Release Notes for the Cisco Media Gateway Controller Software Release 9.6(1)* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/relnote/rn961.htm.

XECfgParm.dat Configuration Tasks

You must configure the XECfgParm.dat file in the Cisco MGC software to enable this feature. The following sections describe the tasks related to configuring the XECfgParm.dat file for this feature:

Configuring The XECfgParm.dat File For This Feature

This section contains the steps necessary for configuration of the next hop IP address in the XECfgParm.dat file to support this feature. If you are installing and configuring the Cisco MGC software on your system for the first time, use the procedures in the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/swinstl/index.htm

Come back to this section once you encounter the **.IP_NextHop1* parameter in the XECfgParm.dat file.

Note You need to configure the *.IP_NextHop parameters when the Cisco MGC hosts are on different subnets. If your hosts are on the same subnet, do not perform the procedure below.

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 PGW hosts is shut down.

Caution Do not modify the other XECfgParm.dat parameters associated with this feature.

To configure the next hop IP addresses, perform 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 PGW hosts using a text editor, such as vi.

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

Step 3 Search for the *.IP_NextHop1 parameter and enter the IP address of your first next hop destination on the active and standby Cisco PGW hosts.

Note The IP address should be expressed in dotted decimal notation (for example, 10.25.81.5).

Step 4 Repeat Step 3 for every next hop destination (*.IP_NextHop2, *.IP_NextHop3, etc.) you want to identify on the active and standby Cisco PGW hosts. Up to eight next hop IP addresses can be specified.

Step 5 Return to the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/swinstl/index.htm

and continue from where you left off. You will need to go to Adding DPNSS Connections, page 12 in this document later if you intend to use an IUA interface for data backhaul between your Cisco PGW 2200 and your associated Cisco access gateway(s).

Verifying the XECfgParm.dat Changes

To verify the XECfgParm.dat settings for this feature, perform the following steps:

Caution Do not modify the other XECfgParm.dat parameters associated with this feature.

Step 1 Log in to the standby Cisco MGC as root and change directories to the etc subdirectory by entering the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 2 Open the XECfgParm.dat using a text editor, such as vi.

Step 3 Search for the *.IP_NextHop1 parameter and enter the IP address of your first next hop destination.

Note The IP address should be expressed in dotted decimal notation (for example, 10.25.81.5).

Step 4 Repeat Step 3 for every next hop destination (*.IP_NextHop2, *.IP_NextHop3, etc.) you want to identify. Up to eight next hop IP addresses can be specified.

Step 5 Save your changes and close the text editor.

Step 6 Manually stop the Cisco MGC software on the standby Cisco MGC by entering the following UNIX command:

```
/etc/init.d/CiscoMGC stop
```

Step 7 Once the software shutdown is complete, manually start the Cisco MGC software on the standby Cisco MGC by entering the following command:

```
/etc/init.d/CiscoMGC start
```

Step 8 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sw-over::confirm
```

Site alarms are automatically set until the Out-of-service (OOS) Cisco PGW host is returned to an IS state.

Step 9 Repeat steps 2 through 8 for the newly standby Cisco PGW host.

Configuration Example

This section provides a configuration example of the associated XECfgParm.dat parameters for this feature. Additional configuration examples for the Cisco MGC software can be found in the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/swinstl/index.htm.

Note Configuration of XECfgParm.dat parameters for this feature is required only when the Cisco MGC hosts are not in the same subnet.

```
*.IP_NextHop1 = 147.21.135.10
*.IP_NextHop2 = 147.15.170.11
*.IP_NextHop3 = 0.0.0.0
*.IP_NextHop4 = 0.0.0.0
*.IP_NextHop5 = 0.0.0.0
*.IP_NextHop6 = 0.0.0.0
*.IP_NextHop7 = 0.0.0.0
*.IP_NextHop8 = 0.0.0.0
```

Provisioning Procedures

You must modify the provisioning data of your system to enable this feature. Before you begin provisioning this feature, we recommend that you plan your provisioning changes as described in Planning for Provisioning, page 33.

Tip You can find information on starting and ending provisioning sessions and retrieving provisioning data in Provisioning Basics, page 35.

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

Provisioning This Feature

Provision the transport path for DPNSS data between the Cisco PGW 2200 and the external Cisco access gateway nodes to provide a reliable communication path between the two platforms.

Perform this provisioning when an external node is modified to use an SCTP-based protocol or when a new external node is added to the Cisco PGW 2200. This section covers the following provisioning topics:

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

Adding DPNSS Connections

This section contains the procedures that you must perform to support DPNSS connections with your Cisco PGW 2200 provisioning data. When provisioning the components that enable the Cisco PGW 2200 to support DPNSS, perform the procedures in the following order.

Adding Cisco Access Gateway External Nodes

To add Cisco access gateway external nodes, perform the following steps:

Step 1 Start a provisioning session as described in Starting a Provisioning Session, page 35.

Step 2 Enter the following command to add a Cisco access gateway external node:

```
prov-add:extnode:name="name", desc="description", type="as", isdnsigtype="iua"
```

Where:

- *name*—The name you want to give to the external node. The name can be as many as 20 characters long and can contain numbers, letters, and the dash (-) symbol. The name should begin with a letter.
- *description*—The long name you assign to the node. It can be as many as 128 alphanumeric characters in length.
- *as*—The MML name for the type of Cisco access gateway. Valid values are in the External Node Types, page 52.

For example, to add a Cisco access gateway external node named va-3600-36, you would enter the following command:

```
prov-add:extnode:name="va-3600-36", desc="3600", type="AS3600", isdnsigtype="iua"
```

Step 3 Repeat Step 2 for each Cisco access gateway external node you want to add to your provisioning data.

Step 4 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Otherwise, proceed to Adding IP Routes (Optional), page 13 if your Cisco PGW 2200 is on a different subnet from the associated access gateway, or proceed to Adding SCTP Associations, page 14 if they are on the same subnet.

Adding IP Routes (Optional)

IP routes are required for your provisioning data if your Cisco PGW hosts are not on the same subnet as the Cisco access gateways. To add IP routes, perform the following steps:

Step 1 If you do not already have an active provisioning session, start one as described in Starting a Provisioning Session, page 35.

Step 2 Enter the following command to add an IP route:

```
prov-add:iproute:name="name", desc="description", netmask="mask", nexthop="nhop",
ipaddr="addr", dest="destination"
```

Where:

- *name*—The name you want to give to the IP route. The name can be as many as 20 characters long and can contain numbers, letters, and the dash (-) symbol. The name should begin with a letter.
- *description*—The long name that you assign to the route. It can be as many as 128 alphanumeric characters in length.
- *mask*—Subnet mask of the destination (optional). The value should be expressed as an IP address in dotted decimal notation (default is 255.255.255.255).

- *nhop*—Next hop router hostname, IP address, or one of the following property names defined in the XECfgParm.dat file:
  - IP_NextHop
  - IP_NextHop2
  - IP_NextHop3
  - IP_NextHop4
  - IP_NextHop5
  - IP_NextHop6
  - IP_NextHop7
  - IP_NextHop8
  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4

  The IP address should be in dotted decimal notation, and the host name must be less than or equal to 32 characters.
- *addr*—Local IP address. IP address should be one of the following property names defined in the XECfgParm.dat file:
  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4
- *destination*—Destination hostname or IP address. IP address should be in dotted decimal notation and the hostname must be less than or equal to 32 characters.

For example, to add an IP route named iprte1, you would enter the following command:

```
prov-add:IPROUTE:NAME="iprte1", DESC="IP Route 1", dest="10.82.80.0", ipaddr="IP_Addr1",
netmask="255.255.255.0", nexthop="10.82.82.1"
```

Step 3 Repeat Step 2 for each IP route you want to add to your provisioning data.

Step 4 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Otherwise, proceed to Adding SCTP Associations, page 14.

Adding SCTP Associations

To add SCTP associations, perform the following steps:

Step 1 If you do not already have an active provisioning session, start one as described in Starting a Provisioning Session, page 35.

Step 2 Enter the following command to add an SCTP association:

```
prov-add:association:name="name", desc="description", type="IUA", ipaddr1="addr1",
ipaddr2="addr2", peeraddr1="paddr1", peeraddr2="paddr2", extnode="gway",
iproute1="iprte1", iproute2="iprte2"
```

Where:

- *name*—The name you want to give to the SCTP association. The name can be as many as 20 characters long and can contain numbers, letters, and the dash (-) symbol. The name should begin with a letter.
- *description*—The long name that you assign to the association. It can be as many as 128 alphanumeric characters in length.
- *addr1*—First local IP address, as defined by the following XECfgParm.dat parameters:
  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4
- *addr2*—Second local IP address, as defined by the following XECfgParm.dat parameters:
  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4
  - N/A (default value)
- *paddr1*—Highest priority destination address, expressed in dotted decimal notation.
- *paddr2*—Lowest priority destination address, expressed in dotted decimal notation. This parameter is optional. The default value for this parameter is *0.0.0.0*.
- *gway*—MML name of a previously entered Cisco access gateway external node.
- *iprte1*—MML name of a previously entered IP route (optional).
- *iprte2*—MML name of a previously entered IP route (optional).

For example, to add an SCTP association named dpnssasassoc1, you would enter the following command:

```
prov-add:ASSOCIATION:NAME="dpnssassoc1",DESC="DPNSS Association 1", TYPE="IUA",
IPADDR1="IP_Addr1", IPADDR2="IP_Addr2", PEERADDR1="10.82.80.187",
PEERADDR2="10.82.81.164", extnode="va-3600-37, IPROUTE1="iprte1", IPROUTE2="iprte2"
```

Note The parameters listed above are those you need in order to create an SCTP association for an IUA interface. For a complete list of parameters for this component, see SCTP Association, page 46.

Step 3 Repeat Step 2 for each SCTP association you want to add to your provisioning data.

Step 4 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Otherwise, proceed to Adding DPNSS Signaling Services, page 16.

Adding DPNSS Signaling Services

To add DPNSS signaling services, perform the following steps:

Step 1 If you do not already have an active provisioning session, start one as described in Starting a Provisioning Session, page 35.

Step 2 Enter the following command to add a DPNSS signaling service:

```
prov-add:dpnsspath:name="name", desc="description", extnode="mgw", abflag="side",
sigport=portnum, sigslot=slotnum
```

Where:

- *name*—The name you want to give to the signaling service. The name can be as many as 20 characters long and can contain numbers, letters, and the dash (-) symbol. The name should begin with a letter.
- *description*—The long name you assign to the service. It can be as many as 128 alphanumeric characters in length.
- *mgw*—MML name of a previously defined external node. Valid types are:
  - C2600
  - AS3600
  - AS3660
- *side*—DPNSS side for this signaling service (optional). Value values are A (for A side), B (for B side), and N (for not applicable) (N).
- *portnum*—Number for physical port on the access gateway (optional). Valid values: 0-167 (0).
- *slotnum*—Number for physical slot on the access gateway (optional). Valid values: 0-63 (0).

For example, to add a DPNSS signaling service named dpnsvc1, you would enter the following command:

```
prov-add:naspath:NAME="dpnsvc1",DESC="IUA DPNSS path", extnode="va-3660-20", abflag="a",
sigport=45, sigslot=10
```

Step 3 Repeat Step 2 for each DPNSS signaling service you want to add to your provisioning data.

Step 4 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Modifying DPNSS Components

Modifying Cisco Access Gateway External Nodes

Desc is the only parameter that can be modified for an existing Cisco access gateway external node. To edit the description of a Cisco access gateway external node, perform the following steps:

Step 1 Start a provisioning session as described in Starting a Provisioning Session, page 35.

Step 2 Enter the following command to edit a Cisco access gateway external node:

```
prov-ed:extnode:name="name", desc="description"
```

Where:

- *name*—MML name of the Cisco access gateway external node to be modified.
- *description*—The long name you assign to the external nodes. It can be as many as 128 alphanumeric characters in length.

For example, to modify an Cisco access gateway external node named va-3600-37, you would enter the following command:

```
prov-ed:extnode:name="va-3600-37", desc="3600 supporting DPNSS"
```

Step 3 Repeat the above steps for each Cisco access gateway external node you want to modify in your provisioning data.

Step 4 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Modifying DPNSS Signaling Services

You can modify the description, DPNSS side identification, signaling port number, and signaling slot number in a DPNSS signaling service. To modify DPNSS signaling services, perform the following steps:

Step 1 Shut down the D-channel(s) on the associated access gateway(s). See the documentation for the access gateway for more information on shutting down D-channels.

Step 2 Set the DPNSS signaling services to be modified to the Out-of-Service (OOS) state by entering the following MML command:

```
set-dest:sig_srv:OOS
```

Where *sig_srv* is the MML name of the DPNSS signaling services to be modified.

Step 3 Repeat Step 2 for each of the DPNSS signaling services to be modified.

Step 4 Start a provisioning session as described in Starting a Provisioning Session, page 35.

Step 5 Enter the following command to modify an DPNSS signaling service:

```
prov-ed:dpnsspath:name="name", desc="description", abflag="side", sigport=portnum,
sigslot=slotnum
```

Where:

- *name*—MML name of the component to be modified.
- *description*—The long name assigned that can be as many as 128 alphanumeric characters in length.
- *mgw*—MML name of a previously defined external node. Valid types are:
  - C2600
  - AS3600
  - AS3660
- *side*—DPNSS side for this signaling service (optional). Value values are A (for A side), B (for B side), and N (for not applicable) (N)
- *portnum*—Number for physical port on the access gateway (optional). Valid values: 0-167 (0).
- *slotnum*—Number for physical slot on the access gateway (optional). Valid values: 0-63 (0).

For example, to modify the DPNSS side identification on a DPNSS signaling service named dpnsvc1, you would enter the following command:

```
prov-ed:dpnsspath:NAME="dpnsvc1", abflag="n"
```

Step 6 Repeat Step 5 for each DPNSS signaling service you want to modify in your provisioning data.

Step 7 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Step 8 Set the modified DPNSS signaling services to the In-Service (IS) state by entering the following MML command for each signaling service:

```
set-dest:sig_srv:IS
```

Where *sig_srv* is the MML name of the modified DPNSS signaling service.

Step 9 Restore the D-channel(s) on the associated access gateway(s). See the documentation for the media gateway for more information on shutting down D-channels.

Modifying IP Routes

The only IP route parameter that cannot be modified is the *name*. To modify IP routes, perform the following steps:

Step 1 Set the IP route to be modified to the OOS state as described in Changing the Service State of an IP Route, page 28.

Step 2 Repeat Step 1 for each IP route to be modified.

Step 3 Start a provisioning session as described in Starting a Provisioning Session, page 35.

Step 4 Enter the following command to modify an IP route:

```
prov-ed:iproute:name="name", desc="description", netmask="mask", nexthop="nhop",
ipaddr="addr", dest="destination"
```

Where:

- *name*—MML name of the IP route to be modified.
- *description*—The long name assigned that can be as many as 128 alphanumeric characters in length.
- *mask*—Subnet mask of the destination (optional). The value should be expressed as an IP address in dotted decimal notation (default is 255.255.255.255).
- *nhop*—Next hop router hostname, IP address, or one of the following property names defined in the XECfgParm.dat file:
  - IP_NextHop
  - IP_NextHop2
  - IP_NextHop3
  - IP_NextHop4
  - IP_NextHop5
  - IP_NextHop6
  - IP_NextHop7
  - IP_NextHop8

  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4

  The IP address should be in dotted decimal notation and the host name must be less than or equal to 32 characters.

- *addr*—Local IP address. The IP address should be one of the following property names defined in the XECfgParm.dat file:
  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4
- *destination*—Destination host name or IP address. The IP address should be in dotted decimal notation and the hostname must be less than or equal to 32 characters.

For example, to modify the destination and local IP address in an IP route named iparte1, you would enter the following command:

```
prov-ed:IPROUTE:NAME="iprte1", dest="10.82.80.1", ipaddr="IP_Addr2"
```

Step 5 Repeat the Step 4 for each IP route you want to modify in your provisioning data.

Step 6 If there are no other components that you need to provision, end your provisioning session, as described in Saving and Activating Your Provisioning Changes, page 36.

Step 7 Set the IP route to be modified to the IS state, as described in Changing the Service State of an IP Route, page 28.

Modifying SCTP Associations

Only the name, type, and extnode parameters cannot be modified for an SCTP association. To modify SCTP associations, perform the following steps:

Step 1 Set the SCTP association to be modified to the OOS state as described in Changing the Service State of an Association, page 28.

Step 2 Repeat Step 1 for each SCTP association to be modified.

Step 3 Start a provisioning session, as described in Starting a Provisioning Session, page 35.

Step 4 Enter the following command to modify an SCTP association:

```
prov-ed:association:name="name", desc="description", ipaddr1="addr1", ipaddr2="addr2",
peeraddr1="paddr1", peeraddr2="paddr2", iproute1="iprte1", iproute2="iprte2"
```

Where:

- *name*—MML name of the SCTP association to be modified.
- *description*—The long name you assign to the association. It can be as many as 128 alphanumeric characters in length.
- *addr1*—First local IP address, as defined by the following XECfgParm.dat parameters:

  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4
- *addr2*—Second local IP address, as defined by the following XECfgParm.dat parameters:
  - IP_Addr1
  - IP_Addr2
  - IP_Addr3
  - IP_Addr4
  - N/A (default value)
- *paddr1*—Highest priority destination address, expressed in dot notation.
- *paddr2*—Lowest priority destination address, expressed in dot notation. This parameter is optional. The default value for this parameter is *0.0.0.0*.
- *iprte1*—MML name of a previously entered IP route (optional).
- *iprte2*—MML name of a previously entered IP route (optional).

For example, to modify the local IP addresses for an SCTP association named dpnssassoc1, you would enter the following command:

```
prov-ed:ASSOCIATION:NAME="dpnssassoc1", IPADDR1="IP_Addr2", IPADDR2="IP_Addr3"
```

Step 5 Repeat Step 4 for each SCTP association you want to modify in your provisioning data.

Step 6 If there are no other components that you need to provision, end your provisioning session as described in Saving and Activating Your Provisioning Changes, page 36.

Step 7 Set the SCTP association to be modified to the IS state as described in Changing the Service State of an Association, page 28.

Deleting DPNSS Components

The following sections contain the procedures for deleting the DPNSS components in your Cisco PGW 2200 provisioning data:

Deleting Cisco Access Gateway External Nodes

To delete Cisco access gateway external nodes, perform the following steps:

Step 1 Set the interface on the external node that is associated with the Cisco MGC software to the OOS state. See the documentation for your media gateway for more information on taking interfaces OOS.

Step 2 Delete the signaling service(s) associated with this external node. To delete a DPNSS signaling service, perform the steps in Deleting DPNSS Signaling Services, page 21.

Step 3 If your system uses IP routes for this external node, delete the IP routes, as described in Deleting IP Routes, page 22.

Step 4 Delete the SCTP associations for this external node, as described in Deleting SCTP Associations, page 22.

Step 5 Enter the following command to delete a Cisco access gateway external node:

```
prov-dlt:extnode:name="name"
```

Where *name* is the MML name of the Cisco access gateway external node to be deleted.

For example, to delete a Cisco access gateway external node named va-3600-37, you would enter the following command:

```
prov-dlt:extnode:name="va-3600-37"
```

Step 6 Repeat the above steps for each Cisco access gateway external node you want to delete from your provisioning data.

Deleting DPNSS Signaling Services

To delete DPNSS signaling services, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-dest:sig_srv:OOS
```

Where *sig_srv* is the MML name of the desired signaling service.

For example, to set the service state of a signaling service called sigsrv1 to OOS, enter the following command:

```
set-dest:sigsrv1:OOS
```

Step 2 Block all of the CICs associated with this signaling service using the following MML command:

```
blk-cic:sig_svc:all
```

Where *sig_svc* is the MML name of the signaling service associated with the CICs to be blocked.

Step 3 Delete the bearer channels associated with this signaling service using the following MML command:

```
prov-dlt:switchtrnk:dstsrv="sig_svc", "all"
```

Where *sig_svc* is the MML name of this signaling service.

Step 4 If trunk groups are provisioned for this signaling service, delete the trunk groups using the following MML command:

```
prov-dlt:trnkgrp:dstsrv="sig_svc", "all"
```

Where *sig_svc* is the MML name of this signaling service.

Step 5 Enter the following command to delete a DPNSS signaling service:

```
prov-dlt:dpnsspath:name="name"
```

Where *name* is the MML name of the DPNSS signaling service to be deleted.

For example, to delete a DPNSS signaling service named dpnsvc1, you would enter the following command:

```
prov-dlt:DPNSSPATH:NAME="dpnsvc1"
```

Step 6 Repeat the above steps for each DPNSS signaling service you want to delete from your provisioning data.

Deleting IP Routes

To delete IP routes, perform the following steps:

Step 1 Set the service state of the IP route to OOS, as described in Changing the Service State of an IP Route, page 28.

Step 2 Delete any components that used this route as a parameter. To delete SCTP associations, perform the steps found in Deleting SCTP Associations, page 22.

Step 3 Enter the following command to delete an IP route:

```
prov-dlt:iproute:name="name"
```

Where *name* is the MML name of the IP route to be deleted.

For example, to delete an IP route named iprte1, you would enter the following command:

```
prov-dlt:IPROUTE:NAME="iprte1"
```

Step 4 Repeat the above steps for each IP route you want to delete from your provisioning data.

Deleting SCTP Associations

To delete SCTP associations, perform the following steps:

Step 1 Set the service state of the SCTP association to OOS, as described in Changing the Service State of an Association, page 28.

Step 2 Enter the following command to delete an SCTP association:

```
prov-dlt:association:name="name"
```

Where *name* is the MML name of the association you want to delete.

For example, to delete an SCTP association named nasassoc1, you would enter the following command:

```
prov-dlt:ASSOCIATION:NAME="nasassoc1"
```

Step 3 Repeat the above steps for each SCTP association you want to delete from your provisioning data.

Provisioning Example

This section provides an examples of provisioning for the DPNSS feature. Additional examples of provisioning for the Cisco MGC software can be found in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

```
_____________________________________
; IP Route
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:IPROUTE:NAME="iprte1",DEST="10.82.80.0",NETMASK=”255.255.255.0”,NEXTHOP=”10.82.82
.1”,IPADDR=”IP_Addr1”,DESC="IP Route 1"
prov-add:IPROUTE:NAME="iprte2",DEST="10.82.81.0",NETMASK=”255.255.255.0”,NEXTHOP=”10.82.82
.1”,IPADDR=”IP_Addr2”,DESC="IP Route 2"


_____________________________________
; SS7 External Node
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:EXTNODE:NAME="va-2600-165",TYPE="SLT",DESC="2611 SLT RUDP E1"
prov-add:EXTNODE:NAME="va-2600-166",TYPE="SLT",DESC="2611 SLT RUDP E1"


_____________________________________
; Point Codes
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:OPC:NAME="opc",DESC="Own pointcode",NETADDR="1.1.3",NETIND=2,TYPE="TRUEOPC"
prov-add:DPC:NAME="dpc1",DESC="Destination pointcode1",NETADDR="1.1.1",NETIND=2
prov-add:DPC:NAME="dpc2",DESC="Destination pointcode2",NETADDR="1.1.2",NETIND=2


_____________________________________
; Signal Services to Inet via SLT
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:SS7PATH:NAME="ss7svc1",DESC="SS7 to dpc1",DPC="dpc1", OPC="opc", MDO="Q761_BASE"
prov-add:SS7PATH:NAME="ss7svc2",DESC="SS7 to dpc2",DPC="dpc2", OPC="opc", MDO="Q761_BASE"


_____________________________________
; SS7 linksets
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:LNKSET:NAME="ls1",DESC="linkset 1 to dpc1",APC="dpc1",PROTO="SS7-ITU",TYPE="IP"
prov-add:LNKSET:NAME="ls2",DESC="linkset 2 to dpc2",APC="dpc2",PROTO="SS7-ITU",TYPE="IP"


_____________________________________
; SS7 route
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:SS7ROUTE:NAME="rte1",DESC="SS7 Rte
1-dpc1",OPC="opc",DPC="dpc1",LNKSET="ls1",PRI=1
prov-add:SS7ROUTE:NAME="rte2",DESC="SS7 Rte
2-dpc2",OPC="opc",DPC="dpc2",LNKSET="ls2",PRI=1


_____________________________________
; Sessionset
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:SESSIONSET:NAME="slt1",ipaddr1="IP_Addr1",ipaddr2="IP_Addr2", PORT=7000,
PEERADDR1="10.82.80.188",PEERADDR2="10.82.81.165",PEERPORT=7000,extnode="va-2600-165",
TYPE=”BSMV0”,IPROUTE1="iprte1”, IPROUTE2="iprte2”

prov-add:SESSIONSET:NAME="slt2",ipaddr1="IP_Addr1",ipaddr2="IP_Addr2",
PORT=7000,PEERADDR1="10.82.80.191",PEERADDR2="10.82.81.166",PEERPORT=7000,
extnode="va-2600-166", TYPE=”BSMV0”,IPROUTE1="iprte1”, IPROUTE2="iprte2”


_____________________________________
; C7IPLinks
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
prov-add:C7IPLNK:NAME="ls1lk1",DESC="SS7ANSI", LNKSET="ls1",
SESSIONSET="slt1",SLC=0,PRI=1,TIMESLOT=0

prov-add:C7IPLNK:NAME="ls2lk1",DESC="SS7ANSI",
LNKSET="ls2",SESSIONSET="slt1",SLC=0,PRI=1,TIMESLOT=2

prov-add:C7IPLNK:NAME="ls1lk2",DESC="SS7ANSI", LNKSET="ls1",
SESSIONSET="slt2",SLC=1,PRI=1,TIMESLOT=0

prov-add:C7IPLNK:NAME="ls2lk2",DESC="SS7ANSI",
LNKSET="ls2",SESSIONSET="slt2",SLC=1,PRI=1,TIMESLOT=2

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; External Node
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:EXTNODE:NAME=”va-3660-20”,TYPE=”AS3660”,DESC=”IUA DPNSS”, ISDNSIGTYPE=”IUA”

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; SCTP Association
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
prov-add:ASSOCIATION:NAME="dpnssassoc2",ipaddr1="IP_Addr3",ipaddr2="IP_Addr4",
PEERADDR1="10.82.80.31",PEERADDR2="10.82.81.31", extnode="va-3660-20",
TYPE="IUA",IPROUTE1="iprte1",IPROUTE2="iprte2"
```

Troubleshooting Provisioning Errors

The following sections contain troubleshooting procedures related to provisioning:

- Alarm Troubleshooting Procedures, page 24
- Signaling Channel Troubleshooting Procedures, page 27

For more information on troubleshooting the rest of the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

Alarm Troubleshooting Procedures

The alarms listed below are the new and modified alarms associated with this feature that require user action. For a complete list of Cisco MGC alarms, see the *Cisco Media Gateway Controller Software Release 9 Messages Reference Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/errmsg/index.htm

Association Degraded

This alarm occurs when one of the destination addresses for an SCTP association has failed, but the association is still up.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in Resolving an Association Alarm, page 27.

Association Fail

This alarm occurs when an SCTP association has failed because an IP connection has failed or because a destination has gone OOS.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in Resolving an Association Alarm, page 27.

IP RTE CONF FAIL

This alarm occurs when an IP route cannot find the local interface defined by its IP address parameter.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the IP address settings for the identified IP route are correct. Use the **prov-rtrv** MML command, as described in Retrieving Provisioning Data, page 37.

If the IP address settings for your IP route are correct, proceed to Step 2.

If the IP address settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in Modifying IP Routes, page 18.

Step 2 Verify that the other provisioned settings for the identified IP route obtained in Step 1 are correct.

If the other provisioned settings for your IP route are correct, proceed to Step 3.

If the provisioned settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in Modifying IP Routes, page 18.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution.

IP RTE FAIL

This alarm occurs when an IP route is in the OOS state with a cause other than off-duty or commanded out-of-service.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the provisioned settings for the identified IP route are correct. Use the **prov-rtrv** MML command, as described in Retrieving Provisioning Data, page 37.

If the provisioned settings for your IP route are correct, proceed to Step 2.

If the provisioned settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in Modifying IP Routes, page 18.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution.

LIF FAIL

This alarm occurs when a local Ethernet interface has failed.

Corrective Action

To correct the problem identified by this alarm, perform the following steps.

Note If the Association Degraded or Association Failed alarm occurs along with this alarm, follow the procedure defined in Resolving an Association Alarm, page 27.

Step 1 Verify that the provisioned settings for the identified line interface are correct, using the **prov-rtrv** MML command, as described in Retrieving Provisioning Data, page 37.

If the provisioned settings for your line interface are correct, proceed to Step 4.

If the provisioned settings for your line interface are incorrect, proceed to Step 2.

Step 2 Place the identified line interface in the OOS administrative state, as described in the "Setting the Administrative State" section of the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

Step 3 Start a dynamic reconfiguration session to change the settings, as described in the "Invoking Dynamic Reconfiguration" section of the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

Step 4 Place the identified line interface in the in-service administrative state, as described in the "Setting the Administrative State" section of the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

If that does not resolve the problem, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution.

Wrong IP Path

This alarm occurs when an IP route or local interface associated with the identified component cannot be used. This can happen when one of the following occurs:

- A route has been overridden by another route in the operating system routing table.
- A route configured on your system has been deleted by using the UNIX command **route delete**.
- An IP link or route has been provisioned incorrectly.

This alarm can also occur if an IP signaling channel has been misconfigured. Use the **netstat -rnv** UNIX command to retrieve the current operating system routing table.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Log in to the active Cisco MGC and retrieve the current operating system routing table using the following UNIX command:

```
netstat -rnv
```

The system returns a response similar to the following:

```
IRE Table: IPv4
  Destination          Mask            Gateway      Device Flags
----------------- ---------------- -------------- ------ -----
10.82.80.0        255.255.255.0    10.82.82.1             UGH
10.82.81.0        255.255.255.0    10.82.83.1             UGH
10.82.82.0        255.255.255.0    10.82.82.112   hme0    U
10.82.83.0        255.255.255.0    10.82.83.112   hme1    U
default           0.0.0.0          10.82.82.1             UG
224.0.0.0         240.0.0.0        10.82.82.112   hme0    U
127.0.0.1         255.255.255.255  127.0.0.1      lo0     UH
```

Step 2 If the response does *not* contain the route identified in the alarm, open the operating system routing table file using a text editor such as vi. Otherwise, proceed to Step 5.

Step 3 Add the route to the routing table using the appropriate text editor command.

Step 4 Save the file and exit the editing session. If this resolves the problem, the procedure is complete. Otherwise, proceed to Step 5.

Step 5 Verify that the provisioned settings for the identified IP link are correct, using the **prov-rtrv** MML command, as described in Retrieving Provisioning Data, page 37.

If the provisioned settings for your IP link are correct, proceed to Step 6.

If the provisioned settings for your IP link are incorrect, start a dynamic reconfiguration session to change the settings, as described in the "Invoking Dynamic Reconfiguration" section of the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution.

Signaling Channel Troubleshooting Procedures

The following signaling channel troubleshooting procedures are new for this feature:

- Resolving an Association Alarm, page 27
- Changing the Service State of an Association, page 28
- Changing the Service State of an IP Route, page 28

Resolving an Association Alarm

When you are referred to this section by an alarm indicating a failure on an association, perform the following steps:

Step 1 If this alarm occurs along with a LIF FAIL alarm on the local IP address (ADDR1 and ADDR2), proceed to Step 2. Otherwise, proceed to Step 4.

Step 2 Check the functioning of the cabling between the Cisco MGC and the LAN switch.

If the cables are functioning properly, proceed to Step 3.

If you find bad cable(s), replace them. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 3.

Step 3 Check the functioning of the associated LAN switch. See the documentation for your LAN switch for the steps necessary to verify its proper functioning.

If the LAN switch is functioning properly, proceed to Step 6.

If the LAN switch is not functioning properly, see documentation for the LAN switch for the appropriate troubleshooting procedures. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 4 Debug the IP connectivity between the Cisco MGC and the associated access gateway.

If the IP connectivity is working correctly, proceed to Step 5.

If the IP connectivity is not working correctly, make the necessary repairs. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 5.

Step 5 Determine the health of the associated access gateway.

If the access gateway is working correctly, proceed to Step 6.

If the access gateway is not healthy, fix it using the procedures in the user documentation for the access gateway. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution.

Changing the Service State of an Association

To change the service state of an association, log in to the active Cisco MGC, start an MML session, and enter the following command:

set-association:*assoc_name*:*serv_state*[**,confirm**]

Where:

- *assoc_name*—MML name of the association you want to modify.
- *serv_state*— The service state to which you want to change. Valid values for IP links are IS, OOS, and FOOS.
- confirm—This parameter is required when you are setting the service state to OOS or FOOS.

Note This command cannot be used on the standby Cisco MGC.

For example, to set the service state of the association, assoc1, to OOS, enter the following command:

```
set-association:assoc1:OOS,confirm
```

You can verify that the selected association is in the proper service state by performing the procedure in Retrieving the Service State of an Association, page 30.

Changing the Service State of an IP Route

To change the service state of an IP route, log in to the active Cisco MGC, start an MML session, and enter the following command:

set-iproute:*iproute_name*:*serv_state*[**,confirm**]

Where:

- *iproute_name*—MML name of the IP route you want to modify.
- *serv_state*—The service state to which you want to change. Valid values for IP links are IS, OOS, and FOOS.
- confirm—This parameter is required when you are setting the service state to OOS or FOOS.

Note This command cannot be used on the standby Cisco MGC.

An IP route in any of the following combinations of primary and secondary service states can be set to OOS or FOOS:

- IS
- OOS, CONF
- OOS, OFF_DUTY
- OOS, STDBY

For an IP route to be set to IS, it must have a primary service state of OOS and a secondary service state of COOS.

For example, you would enter the following command to set the service state of an IP route called iprte1 to OOS:

```
set-iproute:iprte1:OOS,confirm
```

Note You can verify that the selected IP route is in the proper service state by performing the procedure in Retrieving the Service State of an IP Route, page 31.

Monitoring and Maintaining

The following sections contain the procedures required for proper monitoring and maintenance of this feature. For more information on operational tasks for the rest of the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

Regular Operations

Introduction of the DPNSS Feature Transparency feature requires new procedures for managing signaling channels.

Managing Signaling Channels

The following sections are new or modified for Release 9.4:

- Retrieving the Service State of an Association, page 30
- Retrieving the Service State of an IP Route, page 31

Retrieving the Service State of an Association

To retrieve the service state for an individual association, log in to the active Cisco MGC, start an MML session, and enter the following command:

rtrv-association:*assoc_name*

For example, to retrieve the service state of an association called assoc1, enter the following command:

rtrv-association:assoc1

The system returns a message similar to the following:

```
   Media Gateway Controller 2000-03-26 20:26:18
M  RTRV
   "assoc1:IS"
```

To retrieve attributes for all of the associations, log in to the active Cisco MGC, start an MML session, and enter the following command:

rtrv-association:all

The system returns a message similar to the following:

```
   Media Gateway Controller 2000-03-26 19:23:23
M  RTRV
   "assoc1:OOS
   "assoc2:OOS
   "assoc3:OOS
   "assoc4:OOS
```

The valid service states for an association are described in the following sections. If the association is in any state other than IS, attempt to bring it into service, as described in Resolving an Association Alarm, page 27.

Primary Service State of an Association

The PST field shows the current primary service state of the association. Table 1 lists the valid primary service state values.

Table 1 Primary Service State of an Association

Link State ID	Link State	Description
INB	Install busy	When a system is first configured, all associations default to this state.
IS	In-service	Association is IS and fully operational. This is its normal operating state.
OOS	Out-of-service	Association is OOS. The system is actively trying to restore the association.

Secondary Service State of an Association

The SST field shows the current secondary service state of the specified association. Table 2 lists the valid secondary service state values.

Table 2 Association Secondary Service States of an Association

Link State ID	Link State	Description
COOS	Commanded out-of-service	Association has been commanded OOS by the operator.
STBY	Standby	Association is on the standby Cisco MGC.
CONF	Configuration	Association is OOS due to a configuration failure.

Retrieving the Service State of an IP Route

To retrieve the service state for an individual IP route, log in to the active Cisco MGC, start an MML session, and enter the following command:

rtrv-iproute:*iproute_name*

For example, to retrieve the service state of an IP route called iprte1, enter the following command:

```
rtrv-iproute:iprte1
```

The system returns a message similar to the following:

```
   Media Gateway Controller 2000-03-26 20:26:18
M  RTRV
   "iprte1:IS"
```

To retrieve attributes for all of the IP routes, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-iproute:all
```

The system returns a message similar to the following:

```
   Media Gateway Controller 2000-03-26 19:23:23
M  RTRV
   "iprte1:IS
   "iprte2:IS
```

The valid service states for an IP route are described in the following sections. If the route is in any other state than IS, attempt to bring it into service, as described in Changing the Service State of an IP Route, page 28.

Primary Service State of an IP Route

The PST field shows the current primary service state of the IP route. Table 3 lists the valid primary service state values:

Table 3 IP Route Primary Service States

Link State ID	Link State	Description
IS	In-service	Route is IS and fully operational. This is its normal operating state.
OOS	Out-of-service	Route is OOS. The system is actively trying to restore the link.

Secondary Service State of an IP Route

The SST field shows the current secondary service state of the specified IP route. Table 4 lists the valid secondary service state values:

Table 4 IP Route Secondary Service States

Link State ID	Link State	Description
COOS	Commanded out-of-service	Route has been commanded OOS by the operator.
STBY	Standby	Routes are on the standby Cisco MGC.
OFF_DUTY	Off duty	Route is available for use, but not currently being used.
CONF	Configuration	Route is OOS due to a configuration failure.

Reference Information

The following sections contain reference material related to this feature. Information is included on the following areas:

XECfgParm.dat Parameters

The XECfgParm.dat file configuration parameters added for this feature are in the table below.

Configuration Parameter	Definition
***.IUA.maxNasExtNodes**	Specifies the maximum number of external nodes that can be defined with an ISDN signaling type of IUA. This number also represents the maximum number of IUA associations that can be provisioned. Valid value: 256 **Note** Do not change this value.
***.IUA.maxNasPathsPerExtNode**	Defines the maximum number of NAS signaling services that can be assigned to each external node with an ISDN signaling type of IUA. Valid value: 112 **Note** Do not change this value.
***.IUA.maxNasPaths**	Defines the maximum number of IUA signaling services that can be provisioned. Valid value:1500 **Note** Do not change this value.
***.IP_NextHop1** ***.IP_NextHop2** ***.IP_NextHop3** ***.IP_NextHop4** ***.IP_NextHop5** ***.IP_NextHop6** ***.IP_NextHop7** ***.IP_NextHop8**	Defines the IP addresses of up to eight next hop counters. These IP addresses are used when the next hop router IP addresses on the Cisco PGW hosts do not match. Default: 0.0.0.0 Valid values: An IP address expressed in dotted decimal notation.

For information on the other XECfgParm.dat parameters, see the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/swinstl/index.htm

Planning for Provisioning

This section lists the data that you must gather to successfully provision this feature. For more information on planning the provisioning for the rest of the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

Collecting External Node Data

The external node component type represents another node with which the MGC communicates. You must be ready to enter the following data:

- MML name
- Component description
- Type of the external node
- ISDN signaling type

The parameters for EXTNODE are defined in Table 9.

Collecting DPNSS Path Data

The path data represents an DPNSS signaling service to a particular Cisco access gateway. See Restrictions, page 7 for more information on the Cisco access gateways that require the use of a DPNSS signaling service. You must be ready to enter the following data:

- Unique ID of this component and component name used in MML commands
- Component description
- MML name of the associated external node
- Customer group ID
- Identification of the DPNSS path as either A side, B side, or neither
- Signaling port number (physical port on the Cisco access gateway)
- Signaling port slot (physical slot on the Cisco access gateway)

The DPNSS signaling service component structure is shown in Table 12.

Collecting IP Route Data (optional)

The IP route represents a static IP route. IP routes are required for this feature only when the Cisco PGW hosts are not on the same subnet as the Cisco access gateways. If your system requires IP routes, you must be ready to enter the following data:

- IP route name
- Component description
- Destination hostname or IP address
- Subnet mask of Destination (optional)
- Next hop router IP address
- Local IP address
- Priority

The IP route component information can be listed in Table 13.

Collecting SCTP Association Data

The Stream Control Transmission Protocol (SCTP) association represents the connection between the Cisco MGC and a Cisco access gateway. You must be ready to enter the following data:

- MML name of the SCTP association.
- Description of this component.
- Signaling type.
- MML name of the signaling gateway process (SGP).
- First local address.
- Second local address (optional).
- Local SCTP port number (optional).
- The highest priority destination address.
- The lowest priority destination address (optional).
- Destination SCTP port number. (optional).
- MML name of the external node.
- MML name of first IPROUTE (optional).
- MML name of second IPROUTE (optional).
- Number of bytes to advertise for the local receive window (optional).
- Maximum number of times to retransmit SCTP INIT message (optional).
- Maximum initial timer retransmission value (optional).
- Maximum number of retransmissions over all destination addresses before the association is declared failed (optional).
- Maximum time after a datagram is received before a SCPT SACK is sent (optional).
- Maximum time SCTP waits for other outgoing datagrams for bundling (optional).
- Minimum value allowed for the retransmission timer (optional).
- Maximum value allowed for the retransmission timer (optional).
- Time between heartbeats. The heartbeat is this value plus the current retransmission timeout value (optional).
- Internet protocol precedence. This value is placed in the IP PRECEDENCE portion of the Type Of Service field for outgoing SCTP datagrams (optional).
- Differential Service Code Point (DSCP). This value is placed in the DSCP portion of the Type Of Service field for outgoing SCTP datagrams (optional).
- Maximum number of retransmissions to either PEERADDR1 or PEERADDR2 before it is declared failed (optional).

The SCTP association component structure is shown in Table 14.

Provisioning Basics

Starting a Provisioning Session

You may need to start a provisioning session as part of your system operations. To do this, log into the active Cisco MGC, start an MML session, and enter the following command:

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 If you do not know the name of your current configuration session, you can use the procedure in Retrieving Data on the Current Provisioning Session, page 39.

- *mod_ver*—A new configuration version name for a version 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:

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

Once a provisioning session is underway, you may use the **prov-add**, **prov-ed**, or **prov-dlt** MML commands to add, modify, and delete components on your system. This document describes how to add, modify, and delete M3UA and SUA components. For more information on provisioning other components on your Cisco PGW 2200, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

There are two ways to close your provisioning session:

- Saving and activating your provisioning changes, as described in Saving and Activating Your Provisioning Changes, page 36
- Ending your provisioning session without saving and activating your changes, as described in Ending a Provisioning Session Without Activating Your Changes, page 37.

Saving and Activating Your Provisioning Changes

When you have completed making provisioning changes in your session, you must enter a command to save and activate your changes. There are two different provisioning MML commands that do this: **prov-cpy** and **prov-dply**.

Caution Using the **prov-cpy** or **prov-dply** MML commands can severely impact your system's call processing performance, depending on the extent of your provisioning changes. We recommend that you issue these commands 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 automatically ended. If you want to make additional provisioning changes, you must start a new provisioning session as described in Starting a Provisioning Session, page 35.

Caution Using the **prov-sync** MML command can severely impact your system's call processing performance. We recommend that you issue these commands 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 a high-availability or continuous-service configurations. Do not use this command on a Cisco MGC in a simplex configuration.

Note When you enter the **prov-dply** command, your provisioning session is 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 Starting a Provisioning Session, page 35.

Ending a Provisioning Session Without Activating Your Changes

You may want to end a provisioning session without saving and activating the changes you have entered during your session. If this is the case, you can 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 in which you can use this command to retrieve provisioning data are described in the following sections:

- Retrieving Data for an Individual Component, page 37
- Retrieving Data for Select Components, page 38
- Retrieving Data for All Components of a Particular Type, page 38
- Retrieving Data on the Current Provisioning Session, page 39
- Retrieving Data on Supported Signaling Protocols, page 39

Retrieving Data for an Individual Component

You can retrieve provisioning data for 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* at:

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

- *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 an IUA signaling service called iua1, you would enter the following command:

```
prov-rtrv:sigsvcprop:name="iua1"
```

The system returns a response similar to the following:

```
<<get system response>>
```

Retrieving Data for Select Components

You can retrieve data on select the components provisioned on your system. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:all
```

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

The system returns a response similar to the following:

```
<< get system response >>
```

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* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

Note You cannot use this command for 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. Use the following format:

prov-rtrv:*propComp***:name="***compName***" | name="*ss7famName*"**

Where:

propComp—MML component name appropriate to the property type you want to retrieve, as listed below:

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, you would enter the following command:

```
prov-rtrv:naspath:"all"
```

The system returns a response similar to the following:

```
<< get system response >>
```

Retrieving Data on the Current Provisioning Session

You can retrieve provisioning data on the current provisioning session. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv: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 = mml1
SRCVER = active
DSTVER = jtest
   */
```

Retrieving Data on Supported Signaling Protocols

You can retrieve protocol data for the current provisioning session. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:variants
```

The system returns a response similar to the following:

```
<< get system response >>
```

This section lists the data that you must gather to successfully provision this feature. For more information on planning the provisioning for the rest of the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

Alarms

This section contains the alarms that were added and modified to support this feature. For information on the other alarms for the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Messages Reference Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/errmsg/index.htm

New Alarms

The alarms that are added for this feature are listed below.

Association Degraded

Description A destination address of the association has failed, and the association is still in an UP state.

Severity Minor

Cause This alarm is reported when one of the association destination addresses has failed.

Type 1 (communication error)

Action See Association Degraded, page 24.

Association Fail

Description The SCTP association has failed.

Severity Major

Cause This alarm is reported when the destination node is out of service or there is an IP connectivity failure.

Type 1 (communication error)

Action See Association Fail, page 25.

Wrong IP Path

Description The IP route or local interface provisioned for the specified component is not being used.

Severity Minor

Cause This alarm is reported when generic analysis cannot access the conditional route description table.

Type 1 (communication error)

Action See Wrong IP Path, page 26.

Modified Alarms

The alarms that are modified for this feature are described in the following section.

IP RTE CONF FAIL

Description IP route is out of service due to a configuration failure.

Severity Information

Cause This existing alarm is now generated against the IP route components instead of against signal channel components Indicates that an IP route is out of service because of a configuration failure.

Type 1 (no error)

Action See IP RTE CONF FAIL, page 25.

IP RTE FAIL

Description IP route is out of service. This existing alarm is now generated by IP route objects instead of by the signal channel components.

Severity Information

Cause Indicates that an IP route is out of service.

Type 1 (No error)

Action See IP RTE FAIL, page 25.

LIF FAIL

Description Line interface failure.

Severity Major

Cause This existing alarm is now generated against local interface components. The line interface (LIF) has failed. All physical lines to the Cisco MGC and local interface components can raise this alarm.

Type 4 (Equipment error alarm)

Action See LIF FAIL, page 26.

M-OOS

Description Resource has been manually taken OOS.

Severity Minor

Cause A software process not necessary for normal system operation has been manually requested OOS. This existing alarm is now generated against IP route components.

Type 1 (Communication alarm)

Action Restore the process to the in-service state using the user interface. IP routes can be returned to service by using the procedure in Changing the Service State of an IP Route, page 28.

Measurements

Table 5 contains the system measurements that are added to support this feature. For information on the other system measurements, see the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm

Table 5 New Operational Measurements

MML Counter Group: Name	Description	Related Components	Logging Interval
IUA GROUP	IUA message statistics	Association	
IUA: ASPUpTx	Number of application server process (ASP) Up messages sent from the Cisco MGC to the media gateway on this SCTP association, indicating that it is ready to receive traffic or maintenance messages.		15, 60, 24
IUA: ASPUpAckRx	Number of ASP Up Acknowledgement messages received by the Cisco MGC from the media gateway on this SCTP association.		15, 60, 24
IUA: ASPDnTx	Number of ASP Down messages sent from the Cisco MGC to the media gateway on this SCTP association, indicating that it is *not* ready to receive traffic or maintenance messages.		15, 60, 24
IUA: ASPDnAckRx	Number of ASP Up Acknowledgement messages received by the Cisco MGC from the media gateway on this SCTP association.		15, 60, 24
IUA: ASPActTx	Number of ASP Active messages sent from the Cisco MGC to the media gateway on this SCTP association, indicating that it is active.		15, 60, 24
IUA: ASPActAckRx	Number of ASP Active Acknowledgement messages received by the Cisco MGC from the media gateway on this SCTP association.		15, 60, 24
IUA: ASPInactTx	Number of ASP Inactive messages sent from the Cisco MGC to the media gateway on this SCTP association, indicating that it is inactive.		15, 60, 24
IUA: ASPInactAckRx	Number of ASP Inactive Acknowledgement messages received by the Cisco MGC from the media gateway on this SCTP association.		15, 60, 24
IUA: ErrorRx	Number of Error messages received by the Cisco MGC from the media gateway on this SCTP association.		15, 60, 24
IUA: NotifyRx	Number of Notify messages received by the Cisco MGC from the media gateway on this SCTP association. These messages provide autonomous indications of IUA events on the media gateway.		15, 60, 24
IUA: DataRqt	Number of Data messages sent from the Cisco MGC to the media gateway on this SCTP association, which are to be transmitted using the Q.921 acknowledged information transfer service.		15, 60, 24

Table 5 New Operational Measurements

MML Counter Group: Name	Description	Related Components	Logging Interval
IUA GROUP (continued)	IUA message statistics (continued)	Association	
IUA: DataInd	Number of Data messages received by the Cisco MGC from the media gateway on this SCTP association which are to be received using the Q.921 acknowledged information transfer service.		15, 60, 24
IUA: UnitDataRqt	Number of Data messages sent from the Cisco MGC to the media gateway on this SCTP association, which are to be transmitted using the Q.21 unacknowledged information transfer service.		15, 60, 24
IUA: UnitDataInd	Number of Data messages received by the Cisco MGC from the media gateway on this SCTP association, which are to be received using the Q.21 unacknowledged information transfer service.		15, 60, 24
IUA: EstRqt	Number of requests to establish this SCTP association.		15, 60, 24
IUA: EstConf	Number of confirms that IUA has established an SCTP association with the media gateway.		15, 60, 24
IUA: EstInd	Number of times the media gateway has informed Link Management that the Cisco MGC has established an SCTP association.		15, 60, 24
IUA: RelRqt	Number of requests to release an SCTP association with a media gateway.		15, 60, 24
IUA: RelConf	Number of confirms that IUA has released an SCTP association with the media gateway.		15, 60, 24
IUA: RelInd	Number of times the media gateway has informed Link Management that the Cisco MGC has released an SCTP association.		15, 60, 24

Table 5 New Operational Measurements

MML Counter Group: Name	Description	Related Components	Logging Interval
SCTP-GROUP	SCTP traffic statistics	Association	
SCTP: OOTB	Number of out of the blue packets received.		15, 60, 24
SCTP: InvalidChksum	Number of checksum error packets received.		15, 60, 24
SCTP: CtrlTx	Number control chunks sent.		15, 60, 24
SCTP: OrdDataTx	Number of ordered data chunks sent.		15, 60, 24
SCTP: UnordDataTx	Number of unordered data chunks sent.		15, 60, 24
SCTP: CtrlRx	Number control chunks received.		15, 60, 24
SCTP: OrdDataRx	Number of ordered data chunks received.		15, 60, 24
SCTP: UnordDataRx	Number of unordered data chunks received.		15, 60, 24
SCTP: DataSegTx	Number of SCTP data segments sent.		15, 60, 24
SCTP: DataSegRx	Number of SCTP data segments received.		15, 60, 24
SCTP: AssocFailures	Number of association failures.		15, 60, 24
SCTP: DestFailures	Number of destination failures.		15, 60, 24
SCTP: PeerRestarted	Number of peer restarts.		15, 60, 24

Components

The sections below describe the provisioning components that are added and modified for this feature. For information on the rest of the components in the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

New Components

The provisioning components listed in the following sections are added for this feature.

DPNSS Signaling Service

The DPNSS signaling service component type represents a DPNSS signaling path that is back-hauled over IP to/from a NAS (destination). Its MML name is DPNSSPATH.

Table 6 shows the DPNSS signaling service component structure.

Table 6 DPNSS Signaling Service Component Structure

Parameter MML Name	Parameter Description	Parameter Values (Default)
NAME	IP route name	The name can be as many as 20 alphanumeric characters. No special characters other than "-" are allowed. The name should begin with a letter.
DESC	Component description	The description can be up to any 128 characters.

Table 6 DPNSS Signaling Service Component Structure (continued)

EXTNODE	External node MML name	MML name of a previously defined external node.
CUSTGRPID	Customer group ID	Four digit ID; (0000).
ABFLAG	DPNSS Side	Valid values are a (for A side), b (for B side), and n (for not applicable); (n).
SIGSLOT	Physical Slot on the NAS defining the NFAS Group (optional)	An integer, 0 through 63; (0).
SIGPORT	Physical Port on the slot of NAS defining the NFAS Groupl. (optional)	An integer, 0 through 167.

The following parameters cannot be modified:

- NAME
- EXTNODE

The following rules apply when you create or edit DPNSS signaling paths:

- The maximum number of combined DPNSSPATHs and IUA NASPATHs per IUA external node is 112.
- An ASSOCIATION must be defined with the same EXTNODE attribute as the DPNSSPATH. If this ASSOCIATION has not been defined when the DPNSSPATH is added/edited, a warning is issued. If the ASSOCIATION still has not been defined when the provisioning session is copied or deployed, an error message is generated and the copy or deployment is stopped.
- If the ASSOCIATION with the same EXTNODE value as the DPNSSPATH is deleted, a warning message is issued to inform you that the DPNSSPATH must also be deleted. If it has not been deleted when the provisioning session is copied or deployed, an error message is generated and the copy or deployment is stopped.

IP Route

The IP route is static and it's MML name is IPROUTE.

Table 7 shows the IP route component structure.

Table 7 IPROUTE Component Structure

Parameter MML Name	Parameter Description	Parameter Values (Default)
NAME	IP route name	The name can be as many as 20 alphanumeric characters. No special characters other than "-" are allowed. The name should begin with a letter.
DESC	Component description	The description can be up to 128 characters in any combination.
DEST	Destination host name or IP address	IP address in decimal notation or a host name that is less than or equal to 32 characters.
NETMASK	Subnet mask of Destination (optional)	IP address in decimal notation. (255.255.255.255).

Table 7 IPROUTE Component Structure (continued)

NEXTHOP	Next hop router IP address	IP address or host name that is less than or equal to 32 characters, or one of the following property names defined in XECfgParm.dat: IP_NextHop1, IP_NextHop2, IP_NextHop8, IP_Addr1, IP_Addr2, or IP_Addr4.
IPADDR	Local IP address	IP_Addr1, IP_Addr2, IP_Addr3, or IP_Addr4.
PRI	Priority	1 through 65535; (1).

Note NAME is the only parameter for this command that cannot be modified.

To create or edit IP routes, follow these rules:

- The NETMASK attribute is validated by the system. For your provisioning setup to work correctly, its value (when converted to binary) must have at least one leading 1 and cannot have any trailing 1s after the first 0. The values 255.255.0.0 and 255.255.255.128 are valid. The values 0.0.255.255, 255.0.0.255, and 0.0.0.0 are invalid.
- Ensure that the destination resolves to a non-zero address.
- When the resolved destination address is bit ORed with the netmask value, the result is equal to the netmask. For example, a destination of 10.11.12.13 and a netmask of 255.255.0.0 are invalid because the ORed result would be 255.255.12.13, which is not equal to 255.255.0.0.
- The combination of DESTINATION, NETMASK, and IPADDR must be unique for each IP route.
- The combination of DESTINATION, NETMASK, and PRI must be unique for each IP route.
- When an IP route is specified in a link object (for example, IPLNK, SESSIONSET, or ASSOCIATION), the IP address resolved from the PEERADDR attribute must be checked against the DESTINATION and NETMASK attributes to verify that the IPROUTE is valid.
- When an IP route is specified in a link object (for example, IPLNK, SESSIONSET, or ASSOCIATION), the IPADDR must match the IPADDR of the link.
- When an IPROUTE is not specified for a link object (having that option), the IP address resolved from the PEERADDR attribute must be checked against the defined IPROUTES to verify that it should not be assigned an IPROUTE. If the PEERADDR is on the same subnet as the DESTINATION (based on the NETMASK), and if the IPADDR matches the IPADDR of the link object, then use IPROUTE.
- If the NEXTHOP attribute is a host name or symbolic name from XECfgParm.dat, it can resolve to the address 0.0.0.0, which indicates that the IPROUTE is not used. The IPROUTE status shows up in the **rtrv-iproute:all** command output when in the OOS, OFF_DUTY state.
- If the resolved NEXTHOP address is not 0.0.0.0, it must be on the same subnet as the IPADDR.

The commands to retrieve the service state of an IP route are in Retrieving the Service State of an IP Route, page 31. The commands to set the service state of an IP route are in Changing the Service State of an IP Route, page 28.

SCTP Association

The SCTP association represents the connection between the Cisco MGC and a Cisco access gateway, and its MML name is ASSOCIATION.

Table 8 shows the SCTP association component structure.

Table 8 Association Component Structure

Parameter MML Name	Parameter Description	Parameter Values (Default)
NAME	Unique ID of this component and component name used in MML commands.	The name can be up to 20 alphanumeric characters. No special characters other than "-" are allowed. The name should begin with an alphabetic character.
DESC	Unique ID of this component and component name used in MML commands.	The name can be up to 128 alphanumeric characters. No special characters other than "-" are allowed. The name should begin with an alphabetic character.
TYPE	Signaling type.	The type of protocol to be used. Values: M3UA, SUA, and IUA
SGP	SGP's MML name (optional).	MML name of a previously configured SGP. Used for M3UA and SUA interfaces.
IPADDR1	First local address.	IP_Addr1, IP_Addr2, IP_Addr3, or IP_Addr4.
IPADDR2	Second local address (optional).	IP_Addr1, IP_Addr2, IP_Addr3, IP_Addr4, or N/A, (N/A).
PORT	Local SCTP port number (optional).	From 1024 through 65535. Defaults to 9900 for IUA. Defaults to 2905 for M3UA. Defaults to 14001 for SUA.
PEERADDR1	The highest priority destination address.	IP address.
PEERADDR2	The lowest priority destination address (optional).	IP address; (0.0.0.0).
PEERPORT	Destination SCTP port number (optional).	From 1024 through 65535. Defaults to 9900 for IUA. Defaults to 2905 for M3UA. Defaults to 14001 for SUA.
EXTNODE	External Node's MML name (optional).	MML name of a previously configured external node. Used in IUA interfaces.
IPROUTE1	MML Name of first IPROUTE (optional).	MML name of a previously configured IPROUTE.
IPROUTE2	MML Name of second IPROUTE (optional).	MML name of a previously configured IPROUTE.
RCVWIN	Number of bytes to advertise for the local receive window. (optional).	From 1500 through 65535; (18000).
MAXINITRETRANS	Maximum number of times to retransmit SCTP INIT message (optional).	0 through 100; (10) 0 means use SCTP internal default.

Table 8 Association Component Structure (continued)

Parameter MML Name	Parameter Description	Parameter Values (Default)
MAXINITRTO	Maximum initial timer retransmission value (optional).	0, 300 through 3000 (2000). 0 means use SCTP internal default.
MAXRETRANS	Maximum number of retransmissions over all destination addresses before the association is declared failed (optional).	From 1 through 10 (5). **Note** This value is not to exceed MAXRETRANSDEST * the number of destinations.
CUMSACKTO	Maximum time after a datagram is received before a SCPT SACK is sent (optional).	From 100 through 500 ms; (300).
BUNDLETO	Maximum time SCTP waits for other outgoing datagrams for bundling (optional).	From 100 through 600 ms; (100).
MINRTO	Minimum value allowed for the retransmission timer (optional).	From 300 through 3000 ms; (300).
MAXRTO	Maximum value allowed for the retransmission timer (optional).	From 1000 through 3000 ms; (3000).
HBTO	Time between heartbeats. The heartbeat will be this value plus the current retransmission timeout value (optional).	The value can be 0, or from 300 through 10000 ms; (2000). 0 means disabled.
IPPRECEDENCE	Internet Protocol Precedence. This value is placed in the IP PRECEDENCE portion of the Type Service field for outgoing SCTP datagrams (optional).	ROUTINE 000 PRIORITY 001 IMMEDIATE 010 FLASH 011 FLASH-OVERRIDE 100 CRITICAL 101 INTERNET 110 NETWORK; (ROUTINE) 111

Table 8 Association Component Structure (continued)

Parameter MML Name	Parameter Description	Parameter Values (Default)	
DSCP	Differential Service Code Point (DSCP). This value is placed in the DSCP portion of the Type Service field for outgoing SCTP datagrams (optional).	EF	101110—Expedited Forwarding
		AF11	001010—Assured Forwarding Class 1 Low Drop Precedence
		AF12	001100—Assured Forwarding Class 1 Medium Drop Precedence
		AF13	001110—Assured Forwarding Class 1 High Drop Precedence
		AF21	010010—Assured Forwarding Class 2 Low Drop Precedence
		AF22	010100—Assured Forwarding 2 Medium Drop Precedence
		AF23	010110—Assured Forwarding Class 2 High Drop Precedence
		AF31	011010—Assured Forwarding Class 3 Low Drop Precedence
		AF32	011100—Assured Forwarding Class 3 Medium Drop Precedence
		AF33	011110—Assured Forwarding Class 3 High Drop Precedence
		AF41	100010—Assured Forwarding Class 4 Low Drop Precedence
		AF42	100100—Assured Forwarding Class 4 Medium Drop Precedence
		AF43	100110—Assured Forwarding Class 4 High Drop Precedence
		N/A; (N/A)	
MAXRETRANSDEST	Maximum number of retransmissions to either PEERADDR1 or PEERADDR2 before it is declared failed (optional).	From 1 through 10; (3).	

The following parameters cannot be modified:

- NAME
- EXTNODE
- TYPE
- SGP

To create or edit SCTP associations, follow these rules:

- Only one association with a type of IUA can be assigned to an external node.
- If the type of the association is IUA, the associated external node must have its ISDN signaling type set to IUA, and that external node must be able to support IUA signaling.
- If two associations have the same port value, the values of IPADDR1 and IPADDR2 must either be the same or both must be different.
- The values of IPADDR1 and IPADDR2 must be different.
- If the value of IPPRECEDENCE is not ROUTINE, the value of DSCP must be N/A.
- If the value of DSCP is not N/A, the value of IPPRECEDENCE must be ROUTINE.
- The value of MAXRTO must be greater than or equal to the value of MINRTO.
- When a peer IP address (PEERADDR1 or PEERADDR2) is not on the local subnet of IPADDR1 or IPADDR2, that peer IP address cannot be on the subnet of any other local interface, even if it is not defined within the Cisco MGC software.
- When a peer IP address (PEERADDR1 or PEERADDR2) is not on the local subnet of IPADDR1 or IPADDR2, an IP route (IPROUTE1 or IPROUTE2, respectively) must be specified.
- When an IP route is specified, the values set in PEERADDR1 and PEERADDR2 are checked against the DESTINATION and NETMASK values of the IP route(s) to verify that the IP route is valid.
- When an IP route is specified, its value for IPADDR must match the related IP address of the association. In other words, IPROUTE1 should have an IPADDR that matches IPADDR1 on the association, and IPROUTE 2 should have an IPADDR that matches IPADDR2 on the association.
- When an IP route is not specified, the IP address resolved from the PEERADDR1 or PEERADDR2 parameter is checked against the defined IP routes to verify that it should not be assigned to one of those IP routes. If the peer address is on the same subnet as an IP route, the link should use that IP route.
- The value of PEERADDR1 cannot be 0.0.0.0 or 255.255.255.255, and the value of PEERADDR2 cannot be 255.255.255.255.
- When a host name is specified for a peer IP address, the host name must resolve to an IP address.
- PEERADDR1 and PEERADDR2 can resolve to the same IP address. If the external node has only one IP address and two IP addresses (IPADDR1 and IPADDR2) are defined, PEERADDR2 should be set to the same value as PEERADDR1.
- Associations, session sets, IP links, SIP links, and SS7 signaling gateway links that share a peer address (that is, PEERADDR, PEERADDR1, or PEERADDR2) must be assigned directly or indirectly to the same external node.
- When you are deleting an association and a NASPATH uses the same external node, a warning message is issued to inform you that the NASPATH must also be deleted. If it has not been deleted when the provisioning session is copied or deployed, an error message is generated and the copy or deployment stops.

- The value of PORT cannot be set to the same value as the PORT attribute of any IP link, session set, SIP link, or SS7 signaling gateway link.
- If a value for IPADDR2 or PEERADDR2 is specified, values for IPADDR1 and PEERADDR1 must also be specified. In other words, you cannot have one local address and two remote addresses, or two local addresses and one remote address.
- An IP link, session set, SS7 signaling gateway link, or another association with a different external or signaling gateway node cannot use the resolved value set in PEERADDR1 or PEERADDR2.
- Only one association can be defined to an SS7 signaling gateway process (SGP).
- A value for EXTNODE can be defined only when the association type is IUA.
- A value for SGP can be defined only when the association type is M3UA or SUA.
- The maximum number of associations with a type of M3UA is defined in the XECfgParm.dat parameter, M3UA.maxSgp.
- The maximum number of associations with a type of SUA is defined in the XECfgParm.dat parameter, SUA.maxSgp.

The commands to retrieve the service state of an IP route are in Retrieving the Service State of an IP Route, page 31. The commands to set the service state of an IP route are in Changing the Service State of an IP Route, page 28.

Modified Components

The following components are modified for this feature.

External Node

The external node component type represents another node with which the MGC communicates. Its MML name is EXTNODE.

The parameters for EXTNODE are defined in Table 9.

Table 9 External Node Component Structure

Parameter MML Name	Parameter Description	Parameter Values (Default)
NAME	MML name	The name can be as many as 20 alphanumeric characters. No special characters other than "-" are allowed. The name should begin with a letter.
DESC	Component description	The description can be up to 128 characters.
TYPE	The type of the external node	Valid values are in External Node Types, page 52.
ISDNSIGTYPE	ISDN Signaling Type	Valid values are IUA and N/A (default is N/A). This parameter was added in software Release 9.4(1)T.
GROUP	M3UA/SUA Group Number	Value is 1–100 for M3UA or SUA nodes. Value is 0 for nodes that do not support M3UA or SUA. This parameter was added in software Release 9.4(1)T.

Note DESC is the only parameter for this command that can be modified:

The following rules apply when creating/editing external nodes:

- TYPE must be one of the valid external node types.
- The maximum number of external nodes with an ISDNSIGTYPE of IUA is 256.

External Node Types

Table 10 lists the valid external node types for Release 9.6(1)T of the Cisco MGC software.

Table 10 External Node Types for Cisco MGC Software Release 9.6(1)

ExtNode MML Type	SGCP	MGCP	IPFAS	IUA	BRI	NAS	MGCP ANNO	MGCP IVR	SUA	Other
AS5200			IPFAS			NAS				
AS5300	SGCP	MGCP	IPFAS	IUA		NAS	MGCP ANNO	MGCP IVR		
AS5350	SGCP	MGCP	IPFAS	IUA		NAS	MGCP ANNO	MGCP IVR		BSMV0
AS5400	SGCP	MGCP	IPFAS	IUA		NAS	MGCP ANNO	MGCP IVR		BSMV0
AS5800			IPFAS			NAS	MGCP ANNO			
AS5850		MGCP	IPFAS	IUA		NAS	MGCP ANNO	MGCP IVR		
AS7200	SGCP	MGCP	IPFAS			NAS				
C1751		MGCP	IPFAS	IUA	BRI					
C1760		MGCP	IPFAS	IUA	BRI					
C2600	SGCP	MGCP	IPFAS	IUA	BRI					
C2610XM		MGCP	IPFAS	IUA	BRI					
C2611XM		MGCP	IPFAS	IUA	BRI					
C2620XM		MGCP	IPFAS	IUA	BRI					
C2621XM		MGCP	IPFAS	IUA	BRI					
C2650XM		MGCP	IPFAS	IUA	BRI					
C2651XM		MGCP	IPFAS	IUA	BRI					
C2691		MGCP	IPFAS	IUA	BRI					
C3600	SGCP	MGCP	IPFAS							
C3640		MGCP	IPFAS	IUA	BRI					
C3640A		MGCP	IPFAS	IUA	BRI					
C3660	SGCP	MGCP	IPFAS	IUA	BRI	NAS				
C3725		MGCP	IPFAS	IUA	BRI					
C3745		MGCP	IPFAS	IUA	BRI					
CAT8510	SGCP	MGCP								

Table 10 External Node Types for Cisco MGC Software Release 9.6(1) (continued)

ExtNode MML Type	SGCP	MGCP	IPFAS	IUA	BRI	NAS	MGCP ANNO	MGCP IVR	SUA	Other
CAT8540	SGCP	MGCP								
CCMCLUSTER										
H323										EISUP
ITP									SUA	M3UA
LIMD										LI
LS1010	SGCP	MGCP								
MC3810		MGCP	IPFAS							
MGC										EISUP
MGX8260		MGCP	IPFAS			NAS				
MGX8850	SGCP	MGCP								
SCP										TCAPIP
SLT										BSMV0
TALISS7										SS7SG
UNKNOWN										UNKNOWN
VISM	SGCP	MGCP	IPFAS							
VXSM	SGCP	MGCP	IPFAS							

Properties

New properties have been added to the following MML commands to configure loop avoidance, calling name display, call transfer, and message waiting indication:

- **prov-add:sigsvcprop**
- **prov-add:trnkgrpprop**

LoopAvoidanceSupport

Purpose: This property enables the support of the loop avoidance feature in DPNSS protocol.

Valid Values: 0, 1

Default Value: 0

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:
```
mml>prov-add:sigsvcprop:name="dpnsssvc2", LoopAvoidanceSupport = "1"
mml>prov-add:trnkgrpprop:name="3333", LoopAvoidanceSupport = "1"
```

LoopAvoidanceCounter

Purpose: This property enables the support of the loop avoidance feature in DPNSS protocol.

Valid Values: Any integer

Default Value: 0

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:
```
mml>prov-add:sigsvcprop:name="dpnsssvc2", LoopAvoidanceCounter ="3"
mml>prov-add:trnkgrpprop:name="3333", LoopAvoidanceCounter ="3"
```

InhibitIncomingCallingNameDisplay

Purpose: This property enables or disables inhibit incoming calling name display.

Valid Values:
- 0 to enable
- 1 to disable

Default Value: 0, i.e., Enabled

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:
```
mml>prov-add:sigsvcprop:name="dpnsssv1", InhibitIncomingCallingNameDis-
play ="1"
mml>prov-add:trnkgrpprop:name="2222", InhibitIncomingCallingNameDisplay
="1"
```

InhibitOutgoingCallingNameDisplay

Purpose: This property enables or disables inhibit outgoing calling name display.

Valid Values:
- 0 to enable
- 1 to disable

Default Value: 0, i.e., Enabled

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:
```
mml>prov-add:sigsvcprop:name="dpnsssv1", InhibitOutgoingCallingNameDis-
play ="1"
mml>prov-add:trnkgrpprop:name="2222", InhibitOutgoingCallingNameDisplay
="1"
```

InhibitIncomingConnectedNameDisplay

Purpose: This property enables or disables inhibit incoming connected name display.

Valid Values:
- 0 to enable
- 1 to disable

Default Value: 0, i.e., Enabled

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:
```
mml>prov-add:sigsvcprop:name="dpnsssv1", InhibitIncomingConnectedNameDis-
play ="1"
mml>prov-add:trnkgrpprop:name="2222", InhibitIncomingConnectedNameDis-
play ="1"
mml>prov-add:sigsvcprop:name="dpnsssv1", InhibitIncomingConnectedNumberD-
isplay ="1"
mml>prov-add:trnkgrpprop:name="2222", InhibitIncomingConnectedNumberDis-
play ="1"
mml>prov-add:sigsvcprop:name="dpnsssv1",
```

InhibitOutgoingConnectedNameDisplay

Purpose: This property enables or disables inhibit outgoing connected name display.

Valid Values:
- 0 to enable
- 1 to disable

Default Value: 0, i.e., Enabled

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:
```
InhibitOutgoingConnectedNameDisplay ="1"
mml>prov-add:trnkgrpprop:name="2222", InhibitOutgoingConnectedNameDis-
play ="1"
mml>prov-add:sigsvcprop:name="dpnsssv1", InhibitOutgoingConnectedNumberD-
isplay ="1"
mml>prov-add:trnkgrpprop:name="2222", InhibitOutgoingConnectedNumberDis-
play ="1"
```

MwiStringON

Purpose: This property enables the support of MWI to the DPNSS protocol to turn on the MWI lamp on a particular extension when this string is encoded in a message.

Valid Values: Digit string with minimum length=0, maximum length=32

Note The digit string provisioned should be the same MWI string provisioned in Cisco CallManager.

Default Value: NULL

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:

```
mml>prov-add:sigsvcprop:name="dpnsssvc2", MwiStringON = "*58*AN*0#"

mml>numan-add:digmodstring:custgrpid="1111",name="mwion",dig-
string="4085556666"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t49",result-
type="BNBRMODMWI", dw1="mwion",dw2="mwioff", setname="rset1"
```

Comments

Note The MwiStringON and MwiStringOFF strings are typically unique for each vendor. The string needs to be provisioned depending on the vendor for DPNSS PBX used.

MwiStringOFF

Purpose: This property enables the support of MWI to the DPNSS protocol to turn off the MWI lamp on a particular extension when this string is encoded in message.

Valid Values: Digit string with minimum length=0, maximum length=32

Note The digit string provisioned should be the same MWI string provisioned in Cisco CallManager.

Default Value: NULL

Domain: _XE Parameter _X_SigPath _LinkSet X_Trunk Group _MGC (Choose one)

Example:

```
mml>prov-add:sigsvcprop:name="dpnsssvc2", MwiStringOFF = "*58*AN*1#"
mml>numan-add:digmodstring:custgrpid="1111",name="mwioff",dig-
string="4085556667"
```

Comments:

Note The MwiStringON and MwiStringOFF strings are typically unique for each vendor. The string needs to be provisioned depending on the vendor for DPNSS PBX used.

Provisioning Worksheets

This section contains worksheets for the provisioning components required for this feature. For worksheets covering the rest of the provisioning components in the Cisco MGC software, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm

Table 11 External Node Worksheet Example

Name	Type	ISDN Signaling Type	Group	Description
va-3600-37	AS3600	iua		DPNSS conn to va-3600-37

Table 12 DPNSS Signaling Service Worksheet Example

Name	External Node	Customer Group ID	DPNSS Side	Signaling Port	Signaling Slot	Description
dpnsvc2	va-3660-20		A	0	0	IUA DPNSSpath to GW

Table 12 DPNSS Signaling Service Worksheet Example (continued)

Name	External Node	Customer Group ID	DPNSS Side	Signaling Port	Signaling Slot	Description

Table 13 IP Route Worksheet Example (optional)

Name	Destination	Subnet Mask	Next Hop	IP Address	Priority	Description
iproute1	va-3600-37	255.255.255.0	va-3600-36	175.25.211.17	1	IP route to va-3600-37

Table 14 SCTP Association Worksheet Example

Parameter	Parameter Value					
Name	nasassoc1					
Description	DPNSS IUA association 1					
Signaling type	IUA					
SGP name						
First local address	IP_Addr1					
Second local address (optional)	IP_Addr2					
Local SCTP port number (optional)						
Highest priority destination address	10.82.80.30					
Lowest priority destination address (optional)	10.82.81.30					

Table 14 SCTP Association Worksheet Example (continued)

Parameter	Parameter Value					
Destination SCTP port number (optional)						
External node name	va-3600-37					
First IP route name (optional)	iprte1					
Second IP route name (optional)	iprte2					
Number of bytes to advertise for the local receive window (optional)						
Maximum number of times to retransmit SCTP INIT message (optional)						
Maximum initial timer retransmission value (optional)						
Maximum number of retransmissions over all destination addresses before the association is declared failed (optional)						
Maximum time after a datagram is received before a SCPT SACK is sent (optional)						
Maximum time SCTP will wait for other outgoing datagrams for bundling (optional)						
Minimum value allowed for the retransmission timer (optional)						
Maximum value allowed for the retransmission timer (optional)						
Time between heartbeats (optional)						
IP precedence (optional)						

Table 14 SCTP Association Worksheet Example (continued)

Parameter	Parameter Value					
Differential Service Code Point (optional)						
Maximum number of retransmissions to peer address 1 or 2 before it is declared failed (optional)						

Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Glossary

Table 15 contains definitions of acronyms and technical terms used in this feature module.

Table 15 Glossary

Term	Definition
ANSI	American National Standards Institute
CIC	Carrier Identification Code
DPNSS	Digital Private Network Signaling System. A PBX standard developed in the United Kingdom.
EISUP	Extended ISDN User Part. A proprietary protocol used to communicate between Cisco MGC nodes and between a Cisco MGC node and a Cisco H.323 System Interface.
I/O	Input/Output
IOCC	Input/Output channel controller
IOCM	Input/Output Channel Controller Manager
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
IUA	ISDN Q.921 User Adaptation Layer
LNP	Local Number Portability
M3UA	Message Transfer Point Level 3 User Adaptation

Table 15 Glossary (continued)

Term	Definition
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MML	Man-Machine Language
MTP3	Message Transfer Part Level 3
NAS	Network access server
NFAS	Non-Facility Associated Signaling
PSTN	Public switched telephone network
Q.931	ITU document that defines the ISDN connection control protocol.
Q.921	ITU document that defines the data link protocol used on an ISDN D-channel. Also known as Link Access Protocol - D Channel (LAPD).
RFC	Request For Comments. A proposed standards document. There are RFCs for both IUA and SCTP.
RLM	Redundant Link Manager. A proprietary protocol used for the transport of Q.931 data between a Cisco MGC host and an associated media gateway.
SCCP	Service Connection Control Part
SCTP	Stream Controlled Transmission Protocol
SIGTRAN	Signaling Transport—An IETF working group that addresses the transport of packet-based PSTN signaling over IP networks.
SIP	Session Initiation Protocol
SS7	Signaling System 7
SUA	SCCP User Adaptation
TALI	Transport Adapter Layer Interface
TCAP	Transaction Capability Application Part
UDP	User Datagram Protocol