Cisco Virtual PGW 2200 Softswitch SIP Profiles Feature Module
For Cisco Hosted Collaboration Solution 9.0
Provisioning SIP Header Tables ........................................................................................................... 23
Adding an Inbound SIP Header Table Entry .......................................................................................... 23
Adding an Outbound SIP Header Table Entry ....................................................................................... 23
Adding a SIP Header Table to a Profile .................................................................................................. 23
Modifying a SIP Header Table Entry .................................................................................................... 23
Retrieving a SIP Header Table ............................................................................................................. 23
Retrieving a SIP Header Table Entry .................................................................................................... 23
Reordering a SIP Header Table .............................................................................................................. 24
Deleting an Entry from a SIP Header Table ........................................................................................... 24
Deleting a SIP Header Table .................................................................................................................. 24
Provisioning Examples .......................................................................................................................... 24
Software Changes for This Feature ......................................................................................................... 25
MML Command Reference .................................................................................................................... 25
New MML Commands ............................................................................................................................ 25
  PROV-ADD:INSIPHEADER ....................................................................................................................... 25
  PROV-ADD:OUTSIPHEADER ................................................................................................................... 26
  PROV-ADD:DOMAINPROF .................................................................................................................... 28
Modified MML Commands ..................................................................................................................... 28
  PROV-ADD:PROFILE .............................................................................................................................. 28
  Properties ............................................................................................................................................... 30
Provisioning Worksheets ........................................................................................................................ 32
Glossary ................................................................................................................................................... 35
Obtaining Documentation and Submitting a Service Request ............................................................... 35
Feature description

The SIP profile feature introduces new service profiles for SIP, EISUP, and other protocols. Service profiles improve provisioning and security for the Cisco Virtual PGW 2200 (VPGW) Softswitch by allowing you to create a customized set of call properties and assign it to a call trunk group.

Profile enhancements

In Previous releases Cisco VPGW Softswitch supported two profile types: grprofiles (for SS7 and SIP trunk groups) and isuptmrprofiles (for SS7 sigpaths). In current version this feature includes four new profile types:

- SIP profiles—Profiles for SIP trunk groups.
- EISUP profiles—Profiles for EISUP trunk groups.
- Domain profiles—Profiles based upon a domain name. Domain profiles are for SIP interfaces only.
- Common profiles—A general profile type that can handle SIP and EISUP trunk groups as well as properties from other protocols. SIP and EISUP profiles can contain references to a common profile.

Security enhancements

SIP profile introduces improved security features including topology hiding, back-to-back user agent (B2BUA), and customizable SIP header treatment. These features provide improved security by obscuring or removing call topology information. It allows you to customize how the Cisco VPGW Softswitch processes certain SIP headers. You can combine these features with the new profile types to create unique security settings for each service profile.

Property enhancements

This feature replaces all existing SIP and EISUP trunk group properties with equivalent SIP and EISUP profile properties. From Release 9.9(1), trunk group properties are not available. For more information about migrating to Release 9.9(1), see Upgrading to Support this feature.

Note

This feature does not affect sigpath properties.

Benefits

With this feature, you can

- Create service profiles with custom provisioning and security settings
- Apply profiles based on trunk group or domain name
- Create separate profiles for inbound and outbound traffic
- Define a unique level of B2BUA support for each profile
- Hide the topology of core and access networks by erasing Via: and Record-Route: headers from outbound SIP messages
- Create customized SIP header treatment
Prerequisites

The Cisco Virtual_PGW Softswitch must be running Cisco Virtual_PGW Softswitch Software Release 9.9(1). Prerequisites for this release can be found in the "Release Notes for the Cisco Virtual PGW 2200 (VPGW) Softswitch Software Release 9.9(1)"

Restrictions or Limitations

- Limited service for transparent B2BUA mode for call transfers—The Cisco Virtual_PGW Softswitch does not support transparent B2BUA mode for transferred calls.
- Limited trust policy for call transfers—The Cisco Virtual_PGW Softswitch provides limited trust policy support for call transfers. The transferred call is considered trusted only if both legs of the call are trusted.
- B2BUA Mode Limitation—The B2BUA mode implementation in this feature does not provide protocol repair or repair for a capability mismatch between call legs.
- SIP header table size limitation—In the SIP header table only 20 entries are created.
- SIP profiles do not modify SIP messages affected by call treatment—SIP profiles do not modify the URLs of SIP messages that are affected by the existing call treatment in the Cisco Virtual_PGW Softswitch configuration.
- Topology hiding limitations—The following limitations apply to topology hiding:
  - For some messages that involve multiple contacts, such as 300 (Multiple Choices), 301 (Moved Permanently), and 302 (Moved Temporarily), the Cisco Virtual_PGW Softswitch does not support topology hiding for retry requests. This is because the Cisco VPGW Softswitch may obtain an incorrect routing analysis result when using domain-based routing to resolve a hostname that has been rewritten for topology hiding.
  - The sipEgressRoutingControl property modifies the Request-Line and Route headers. In full B2BUA, the default value MODIFY_REQUEST_LINE_NO_ROUTE_USED does not reveal topology information. However, the other available values might reveal topology information.
  - If your privacy policy requires that the hostname be set to "anonymous.invalid", topology hiding does not rewrite this hostname.

To read more about B2BUA modes, see B2BUA modes

Related features and technology

The following features are related to SIP Profiles:

- SIP-I Protocol
- Multiple Inbound IP Trunks

Upgrade to SIP profile feature

For instructions on how to migrate to Release 9.9(1), see Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Migration Guide.

The following caveats apply to the migration procedure:

- If the Cisco Virtual_PGW Softswitch is in B2BUA mode, the migration process sets all existing trunk groups to nontrusted.
- The migration process converts existing trunk group properties to equivalent SIP and EISUP profile properties. If a trunk group property does not have an equivalent profile property, the migration script moves it to a common profile, which is referenced by the SIP or EISUP profile.
- No domain profiles are defined by default.
Implement SIP profiles

The following sections describe how to implement the SIP profiles feature.

Profile creation

The following sections describe how to create SIP, EISUP, common, and domain profiles.

SIP profiles

A SIP profile creates a set of provisioning properties applies to SIP trunk groups. Each SIP profile contains:

- SIP properties (former trunk group properties) - A pointer to a common profile (optional)
- A pointer to a grpprofile (optional)
- A pointer to an ISUP timer profile (optional)
  - A pointer to an inbound SIP header table (optional)
  - A pointer to an outbound SIP header table (optional)

EISUP profiles

An EISUP profile creates a set of provisioning properties applies EISUP trunk groups. Each EISUP profile contains:

- EISUP properties (former trunk group properties) - A pointer to a common profile (optional)
- A pointer to a grpprofile (optional)

Common profiles

A common profile is an extension of SIP and EISUP profiles that creates set of provisioning properties for multiple protocols. Common profile contains properties present in other profile types.

Domain profiles

A domain profile creates a set of provisioning properties applies to one or more domain names. Each domain profile contains:

- SIP provisioning properties
- B2BUA properties of this feature (optional)
  - A pointer to an inbound SIP header table (optional)
  - A pointer to an outbound SIP header table (optional)

Domain table

The domain table defines the domain profile associated with a given domain name. The domain table contains the following information for each domain name:

- A direction (inbound or outbound)
- A pointer to a domain profile

Multiple Profiles

If the Cisco Virtual_PGW Softswitch processes traffic that matches both a SIP profile and a domain profile, the Cisco Virtual_PGW Softswitch uses both profiles to process the SIP message.

Topology hiding

Topology hiding improves network security in a VoIP environment by preventing customers on one side of a call from knowing the details of the network topology on the other side of the call. This feature uses two SIP modes: proxy mode
and partial B2BUA mode. These options provide topology hiding between the incoming and outgoing sides of the call. This feature introduces a full B2BUA SIP mode which completely divides a SIP call into two separate SIP calls, with one call terminating at the Cisco Virtual_PGW Softswitch and the other originating from the Cisco Virtual_PGW Softswitch.

A call in full B2BUA mode with topology hiding enabled, the Cisco Virtual_PGW Softswitch rewrites the FROM, CONTACT, VIA, Call-ID, RECORD-ROUTE, Remote-Party-ID, and P-Asserted-ID headers to remove topology information. The Cisco VPGW Softswitch does not rewrite headers that contain a Telephone Uniform Resource Identifier value.

By default, other headers include topology information, such as Refer-to and Diversion. You can define customized header treatment for some tags using the SIP header table’s capability available in this feature.

The following table shows how the Cisco Virtual_PGW Softswitch performs topology hiding for selected SIP headers.

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
<th>Treatment</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Contains a URI and a display name (optional). The URI can include topology information at the originating side.</td>
<td>The Cisco Virtual_PGW Softswitch reconstructs the URI using the Cisco VPGW Softswitch’s domain name and port number when sending to the terminating side of the connection, and restores the original values when sending to the originating side of the connection. <strong>Note</strong> The Cisco VPGW Softswitch does not rewrite the domain in the From header if it is altered by the IP_SET_SOURCE_DMN result type introduced in the Domain-based Routing feature.</td>
<td>Incoming Cisco VPGW Softswitch OCC: From: &quot;Bob&quot; <a href="">sip:bob@example.com:5511</a>;tag=a48s&lt;br&gt;Outgoing Cisco VPGW Softswitch TCC: From: &quot;Bob&quot; <a href="">sip:bob@cisco.com:5060</a>;tag=b84s</td>
</tr>
<tr>
<td>Contact</td>
<td>The Contact header contains a display name, a URI with URI parameters, and header parameters. The URI can reveal topology information.</td>
<td>Cisco Virtual_PGW Softswitch reconstructs the URI with the Cisco Virtual_PGW Softswitch’s domain and port number. Other parts of the header are unchanged.</td>
<td>Incoming Cisco VPGW Softswitch: Contact: &quot;Mr. Watson&quot; &lt;sip:mr <a href="mailto:watson@example.com">watson@example.com</a>:5061&gt;&lt;br&gt;Outgoing Cisco VPGW Softswitch: Contact: &quot;Mr. Watson&quot; &lt;sip:mr <a href="mailto:watson@cisco.com">watson@cisco.com</a>:5060&gt;</td>
</tr>
</tbody>
</table>
Via
The Via header contains the transport protocol used to send a message and the client’s host name or network address. It contains the requested port number for responses. The Via header also contains parameters including maddr, ttl, received, and branch.

| In full B2BUA mode, the Cisco Virtual_PGW Softswitch replaces the Via header with the Cisco VPGW Softswitch’s Via header. |
| Incoming Cisco VPGW Softswitch: Via: SIP/2.0/UDP example.com:5060 |
| Outgoing Cisco VPGW Softswitch: Via: SIP/2.0/UDP cisco.com:5060 |

Call-ID
Some SIP implementations use a Call-ID header with the localid@host format.

| In full B2BUA mode, the Cisco VPGW Softswitch generates a new Call-ID value using Cisco VPGW Softswitch domain as the hostname. |
| Incoming Cisco VPGW Softswitch: Call-ID: 12345600@example.com |
| Outgoing Cisco VPGW Softswitch: Call-ID: 7624438c-9380b3e-95b3f8d-8@cisco.com |

Record-Route
Some SIP proxy devices insert a Record-Route into a request to force future requests in the dialog to use the proxy.

| In full B2BUA mode, the Cisco VPGW Softswitch does not transmit Record-Route headers from one side of the call to the other and also inserts a non-Record-Route header. |

P-Asserted-ID
The P-Asserted-ID header contains a URI (typically a SIP URI) and an optional display-name. This header is transmitted from the originating side of the call to the terminating side depending on the local configuration.

| When the header is sent to the terminating side, the Cisco VPGW Softswitch reconstructs the URI using the Cisco VPGW Softswitch’s domain name and port number. Other parts of the header are unchanged. |
| Incoming Cisco VPGW Softswitch: P-Asserted-Identity: "Ms. Jennings" <sip:jennings@example.com:5522> |
| Outgoing Cisco VPGW Softswitch: P-Asserted-Identity: "Ms. Jennings" <sip:jennings@cisco.com:5060> |

Remote-Party-ID
The Remote-Party-ID header contains the URI of the remote party.

| The Cisco VPGW Softswitch reconstructs the URI using the Cisco VPGW Softswitch domain name and port number. Other parts of the header are unchanged. |
| Incoming Cisco VPGW Softswitch: Remote-Party-ID: "John Doe" <sip:jdoe@example.com:5522> |
| Outgoing Cisco VPGW Softswitch: Remote-Party-ID: "John Doe" <sip:jdoe@cisco.com:5060> |

**B2BUA modes**

The SIP Profiles feature introduces four B2BUA modes with configurable multiple levels of call security. B2BUA mode provides a distinct level of unknown SIP header treatment and a topology hiding. B2BUA is configured by setting the trustLevel and topologyHidingEnabled properties of each profile, which specify whether the trunk group is on a trusted interface and whether topology hiding is enabled.

**Note** You can modify a profile’s SIP header table to override the default treatment of unknown SIP headers.
The following table shows the trustLevel and topologyHidingEnabled values for configuring the B2BUA mode.

<table>
<thead>
<tr>
<th>B2BUA Mode</th>
<th>Unknown SIP Header Treatment</th>
<th>trustLevel Value</th>
<th>TopologyHidingEnabled Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent</td>
<td>Transparent</td>
<td>0 (trusted)</td>
<td>0 (based on trustLevel value) or 1 (disabled)</td>
</tr>
<tr>
<td>Full</td>
<td>Transparent</td>
<td>0 (trusted)</td>
<td>2 (enabled)</td>
</tr>
<tr>
<td>Full</td>
<td>Discarded</td>
<td>1 (nontrusted)</td>
<td>0 (based on trustLevel value) or 2 (enabled)</td>
</tr>
<tr>
<td>Partial</td>
<td>Discarded</td>
<td>1 (nontrusted)</td>
<td>1 (disabled)</td>
</tr>
</tbody>
</table>

**SIP header tables**

A profile with a SIP header table, defines a set of SIP headers and corresponding actions. SIP header tables allow you to customize how the Cisco Virtual_PGW Softswitch treats calls based on defined SIP header values.

The following table shows the actions that the Cisco Virtual_PGW Softswitch takes based on SIP headers in inbound and outbound traffic.

<table>
<thead>
<tr>
<th>Inbound SIP Traffic</th>
<th>Outbound SIP Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard header</td>
<td>Discard header</td>
</tr>
<tr>
<td>Reject message if header is present</td>
<td>Add header using fixed string</td>
</tr>
<tr>
<td>Reject message if header is not present</td>
<td>Replace the header using fixed string</td>
</tr>
<tr>
<td>Remove tag</td>
<td>Remove tag</td>
</tr>
<tr>
<td>Add tag</td>
<td>Add tag</td>
</tr>
<tr>
<td>Replace tag</td>
<td>Replace tag</td>
</tr>
</tbody>
</table>

Add header using header of another call leg

Replace the header of another call leg

**SIP headers that support customized treatment**

The SIP Profiles feature defines two categories of SIP headers:

- **Known SIP headers**—The first column of the following table lists known SIP headers in Cisco VPGW Softswitch Software Release 9.9(1). The Cisco VPGW Softswitch treats known SIP headers following its rules.
- **Unknown SIP headers**—All of the SIP headers that are not listed in the first column of the following table are unknown SIP headers. The Cisco VPGW Softswitch discards unknown SIP headers by default.
The second column of the following table lists SIP headers that support customized treatment for Cisco VPGW Softswitch Software Release 9.9(1) by default. You can use SIP header tables to customize treatment for these SIP headers. Available treatment is can be found in Table 3 SIP Header Table Actions.

You can find provisioning examples of SIP header tables in the Provisioning SIP Header Tables.

**Note** The second column of the following table lists SIP headers that support customized treatment by default. If you want to customize treatment for more SIP headers, contact Cisco Technical Assistance Center (TAC) personnel.

### Table 4 Known SIP Headers and SIP Headers That Support Customized Treatment

<table>
<thead>
<tr>
<th>Known SIP Headers</th>
<th>SIP Headers That Support Customized Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>Diversion</td>
</tr>
<tr>
<td>also</td>
<td>Organization</td>
</tr>
<tr>
<td>call-ID</td>
<td>Priority</td>
</tr>
<tr>
<td>call-info</td>
<td>Requested-By</td>
</tr>
<tr>
<td>contact</td>
<td>Server</td>
</tr>
<tr>
<td>content-disposition</td>
<td>Subject</td>
</tr>
<tr>
<td>content-encoding</td>
<td>User-Agent</td>
</tr>
<tr>
<td>content-language</td>
<td>Warning</td>
</tr>
<tr>
<td>content-length</td>
<td></td>
</tr>
<tr>
<td>content-type</td>
<td></td>
</tr>
<tr>
<td>cseq</td>
<td></td>
</tr>
<tr>
<td>date</td>
<td></td>
</tr>
<tr>
<td>event</td>
<td></td>
</tr>
<tr>
<td>expires</td>
<td></td>
</tr>
<tr>
<td>from</td>
<td></td>
</tr>
<tr>
<td>max-forwards</td>
<td></td>
</tr>
<tr>
<td>min-se</td>
<td></td>
</tr>
<tr>
<td>p-asserted-identity</td>
<td></td>
</tr>
<tr>
<td>privacy</td>
<td></td>
</tr>
<tr>
<td>proxy-require</td>
<td></td>
</tr>
<tr>
<td>rack</td>
<td></td>
</tr>
<tr>
<td>reason</td>
<td></td>
</tr>
</tbody>
</table>
Inbound SIP header tables implementation

The following table shows the properties of inbound SIP header tables.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Valid values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header Name</td>
<td>The name of a SIP header used by Cisco VPGW Softswitch modifies traffic.</td>
<td>String from 1-255 characters, case insensitive</td>
</tr>
<tr>
<td>Note</td>
<td>You can use the same header name more than once in a SIP header table.</td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>The SIP message that triggering a customized action. The value must be the</td>
<td>String from 1-256 characters, case insensitive</td>
</tr>
<tr>
<td></td>
<td>name of a SIP request or response message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Request message names: ACK, BYE, CANCEL, COMET, INFO, INVITE, NOTIFY,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPTIONS, PRACK, RE_INVITE, REFER, REGISTER, SIGNAL, SUBSCRIBER, UPDATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Response numbers: 100–699</td>
<td></td>
</tr>
<tr>
<td>Keywords</td>
<td>ALL, ALL_REQUEST, ALL_RESPONSE</td>
<td></td>
</tr>
</tbody>
</table>
| Condition | Defines how the Cisco VPGW Softswitch uses the SIP header table entry to analyze traffic. This field requires one or more entries in the Condition DW fields. | Valid values:  
• 0 = Unconditional  
• 1 = Header contains tag  
• 2 = Header doesn't contain tag  
• 3 = Message contains tag  
• 4 = Message doesn't contain tag |
| --- | --- | --- |
| Treatment | The action that the Cisco VPGW Softswitch takes when the SIP header is present.  
**Note** The Cisco VPGW Softswitch applies inbound SIP header table header actions during message validation. | Valid values:  
• 1 = Discard header  
• 2 = Reject message if header exists  
• 3 = Reject message if header does not exist  
• 4 = Remove tag  
• 5 = Add tag  
• 6 = Replace tag |
| Index | Defines the preferred order for applying SIP header table entries. If a SIP header matches more than one entry in the SIP Header table, the Cisco VPGW Softswitch applies the entry with the lowest Index value. | Valid values: 1–20  
Default value: 1 |
| Condition DW1–4 | The tags the Cisco VPGW Softswitch uses to analyze SIP traffic. You can define up to four tags for each row in the SIP header table.  
**Note** SIP table header treatments take effect only if a message matches all of the Condition DW fields. | String from 1–255 characters, optional, case insensitive. |
| Treatment DW1–4 | Data words that describe how the Cisco VPGW Softswitch applies the treatment settings.  
If the Treatment field is set to 2 or 3, Treatment DW1–4 defines the response code that the Cisco VPGW Softswitch uses to reject the SIP request.  
If the Treatment field is set to 4, 5, or 6, DW1–4 define the tag the Cisco VPGW Softswitch removes, adds, or replaces. You can apply up to four tags for each row in the SIP header table. | String from 1–255 characters, optional, case sensitive.  
Permitted response codes are from 400 to 699. If the SIP header table specifies a response code that the Cisco VPGW Softswitch does not support or does not specify a response code, the Cisco VPGW Softswitch uses the 400 Bad Request response.  
For more information about supported response codes, see the *Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Dial Plan Guide*. |

The following table shows an example of an inbound SIP header table.
### Table 6  
**Sample Inbound SIP Header Table**

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Index</th>
<th>Message</th>
<th>Condition</th>
<th>Treatment</th>
<th>DW1 Condition</th>
<th>DW2 Condition</th>
<th>DW3 Condition</th>
<th>DW4 Condition</th>
<th>DW1 Treatment</th>
<th>DW2 Treatment</th>
<th>DW3 Treatment</th>
<th>DW4 Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diversion</td>
<td>1</td>
<td>ALL</td>
<td>1</td>
<td>6</td>
<td>example.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>2</td>
<td>Notify</td>
<td>0</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>3</td>
<td>486</td>
<td>4</td>
<td>1</td>
<td>Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>4</td>
<td>All_Request</td>
<td>3</td>
<td>4</td>
<td>example.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>example.com</td>
</tr>
<tr>
<td>User-Agent</td>
<td>5</td>
<td>ALL_Responder</td>
<td>3</td>
<td>5</td>
<td>example.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Urgent</td>
</tr>
<tr>
<td>Priority</td>
<td>6</td>
<td>Invite</td>
<td>4</td>
<td>2</td>
<td>Urgent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>7</td>
<td>ALL</td>
<td>4</td>
<td>3</td>
<td>example.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested-By</td>
<td>8</td>
<td>ALL</td>
<td>3</td>
<td>6</td>
<td>example.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>example.com</td>
</tr>
</tbody>
</table>
For example, row four of the table removes the Subject header from all SIP requests. The following example demonstrates how this entry alters a SIP request.

Before:
INVITE sip:bob@cisco.com SIP/2.0
Via: SIP/2.0/UDP site3.example.com;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP pc33.example.com;branch=z9hG4bKnashds8;received=192.0.2.1
Max-Forwards: 69
To: Bob <sip:bob@cisco.com>
From: Alice <sip:alice@example.com>;tag=1928301774
Subject: Invite
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.example.com>
Content-Type: application/sdp
Content-Length: 142

After:
INVITE sip:bob@cisco.com SIP/2.0
CC-Diversion:alice@192.0.2.1
Via: SIP/2.0/UDP site3.example.com;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP pc33.example.com;branch=z9hG4bKnashds8;received=192.0.2.1
Max-Forwards: 69
To: Bob <sip:bob@cisco.com>
From: Alice <sip:alice@example.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.example.com>
Content-Type: application/sdp
Content-Length: 142

Implementing outbound SIP header tables
The following table describes the properties of outbound SIP header tables.

<table>
<thead>
<tr>
<th>Table 7</th>
<th>Outbound SIP Header Table Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>Header Name</td>
<td>The name of a SIP header that the Cisco VPGW Softswitch uses to modify traffic.</td>
</tr>
<tr>
<td></td>
<td>Note You can use the same header name more than once in a SIP header table.</td>
</tr>
</tbody>
</table>
| Apply Policy | Defines the B2BUA mode applied to the call/trunk group | • Trusted  
• Nontrusted  
• ALL |
<table>
<thead>
<tr>
<th>Message</th>
<th>The SIP message that triggering a customized action. The value must be the name of a SIP request or response message.</th>
<th>String from 1–256 characters, case insensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request message names: ACK, BYE, CANCEL, COMET, INFO, INVITE, NOTIFY, OPTIONS, PRACK, RE_INVITE, REFER, REGISTER, SIGNAL, SUBSCRIBER, UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response numbers: 100–699</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keywords: ALL, ALL_REQUEST, ALL_RESPONSE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Condition | Defines how the Cisco VPGW Softswitch uses the SIP header table entry to analyze traffic. This field requires one or more entries in the Condition DW fields. | 0 = Unconditional  
1 = Header contains tag  
2 = Header doesn't contain tag  
3 = Message contains tag  
4 = Message doesn't contain tag |
| Treatment | The action that the Cisco VPGW Softswitch takes when the SIP header is present. To apply multiple changes to a single SIP message, define the treatments in the outbound SIP header table. The Cisco VPGW Softswitch applies the treatments in order of index value.  
**Note** The Cisco VPGW Softswitch analyzes headers prior to SIP table header handling. | 1 = Discard header  
2 = Add header using fixed string  
3 = Replace the header using fixed string  
4 = Remove tag  
5 = Add tag  
6 = Replace tag  
7 = Add text from a header in another call leg |
| Index | Defines the order in which the Cisco VPGW Softswitch applies SIP header table entries. If a SIP header matches more than one entry in the SIP Header table, then Cisco VPGW Softswitch applies the entry with the lowest Index value. | Valid values: 1–20  
Default value: 1 |
The tags the Cisco VPGW Softswitch uses to analyze SIP traffic. You can define up to four tags for each row in the SIP header table.

**Note** SIP table header treatments take effect only if a message matches all of the Condition DW fields.

The tag the Cisco VPGW Softswitch uses based on the value in the Treatment field. You can apply up to four tags for each row in the SIP header table.

String from 1–256 characters, optional, case insensitive.

String from 1–256 characters, optional, case sensitive.

The following table shows an example of an outbound SIP header table.

**Table 8** Sample Outbound SIP Header Table

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Index</th>
<th>Message</th>
<th>Apply Policy</th>
<th>Condition Treatment</th>
<th>Condition DW1</th>
<th>Treatment DW1</th>
<th>Treatment DW2</th>
<th>Treatment DW3</th>
<th>Treatment DW4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diversion</td>
<td>1</td>
<td>All</td>
<td>Trusted</td>
<td>1</td>
<td>6 example.com</td>
<td>2405 example.com</td>
<td>cisco.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>2</td>
<td>Notify</td>
<td>Nontrusted</td>
<td>0</td>
<td>5 example.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>3</td>
<td>486</td>
<td>ALL</td>
<td>4</td>
<td>1 cisco.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>4</td>
<td>ALL_Req</td>
<td>ALL</td>
<td>3</td>
<td>4 example.com</td>
<td></td>
<td></td>
<td></td>
<td>example.com</td>
</tr>
<tr>
<td>User-Agent</td>
<td>5</td>
<td>ALL_Res</td>
<td>ALL</td>
<td>2</td>
<td>5 organization</td>
<td></td>
<td></td>
<td></td>
<td>organization: Cisco</td>
</tr>
<tr>
<td>Priority</td>
<td>6</td>
<td>Invite</td>
<td>ALL</td>
<td>2</td>
<td>3 Urgent</td>
<td>Urgent</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>7</td>
<td>ALL</td>
<td>ALL</td>
<td>4</td>
<td>2 cisco.com</td>
<td></td>
<td></td>
<td>Server: VPGW</td>
<td></td>
</tr>
<tr>
<td>Requested-By</td>
<td>8</td>
<td>ALL</td>
<td>ALL</td>
<td>3</td>
<td>6 example.com</td>
<td></td>
<td></td>
<td>example.com</td>
<td>cisco.com</td>
</tr>
<tr>
<td>User-agent</td>
<td>9</td>
<td>ALL</td>
<td>ALL</td>
<td>3</td>
<td>7 User-Agent: cisco.com</td>
<td></td>
<td></td>
<td>User-Agent: example.net</td>
<td></td>
</tr>
<tr>
<td>Requested-By</td>
<td>10</td>
<td>ALL</td>
<td>ALL</td>
<td>3</td>
<td>8 example.com</td>
<td></td>
<td></td>
<td>example.com</td>
<td>cisco.com</td>
</tr>
</tbody>
</table>

For example, row four of the table removes the Subject header from all SIP requests. The following example demonstrates how this entry alters a SIP message.
Multiple SIP headers

If the Cisco VPGW Softswitch applies multiple profiles to a SIP message and both profiles have SIP header tables defined, the Cisco VPGW Softswitch uses both SIP header tables to process the SIP message.

Provisioning tasks

Further information about provisioning is available in the Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Provisioning Guide.

The following tasks describe how to provision the SIP Profile feature.

Provisioning SIP and EISUP profiles

Use the commands presented in the following sections to provision SIP and EISUP profiles.

Add SIP or EISUP profile

The following examples demonstrate how to add a new SIP or EISUP profile:

```
<command>
provisioning
add:profile:name="sp1", type="SIPPROFILE", custgrpid="1111",
mgcdomain="10.0.6.55", trustlevel="1", topologyhidingenabled="1"
<command>
```

```
<command>
provisioning
add:profile:name="spf2", type="EISUPPROFILE", populatedsdpinfoincdr="1"
<command>
```

Clone SIP or EISUP profile

The base parameter allows you to create a new profile based on an existing profile. To use this parameter, create a new profile and set the base parameter to an existing profile name. The new profile has the properties of the original profile, but you can override the settings of the original profile properties by manually specifying new settings in the command. Both profiles must be of the same type.

```
<command>
provisioning
add:profile:name="spf3", type="EISUPPROFILE", base="spf1", responseattempts="2"
<command>
```
Retrieve SIP or EISUP profile

Use the prov-rtrv:profile command to retrieve SIP and EISUP profile properties. This command has the following parameters:

- prop—Displays the provisioning property settings for the profile
- comp—Displays the components associated with the profile
- all—Displays the profile name, type, and property names, and values for all existing profiles

```
mml> prov-rtrv:profile:"prop", name="spf1"
mml> prov-rtrv:profile:"comp", name="spf2"
mml> prov-rtrv:profile:"all"
```

Modify SIP or EISUP profile

Use the prov-ed:profile command to modify a SIP or EISUP profile:

```
mml> prov-ed:profile:name="spf1", noninvitereqattempts="2"
```

Add Common Profile, a Grprofile, or an ISUP Timer Profile Reference to a SIP profile

You can add a common profile or grprofile reference to a SIP or EISUP profile using the commonprofile and grprofile parameters. You can also add an ISUP timer profile reference to a SIP profile using the isuptmrprofile parameter.

```
mml> prov-ed:profile:name="spf1",commonprofile="cpf1"
mml> prov-ed:profile:name="spf1",grprofile="gpf1"
mml> prov-ed:profile:name="spf1",isuptmrprofile="isuptmrpf1"
```

Note: You must create common profiles or grprofiles before referencing them in a SIP or EISUP profile. You must create ISUP timer profiles before referencing them in a SIP profile.

Note: For instructions on how to create a grprofile or an ISUP timer profile, see the Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Provisioning Guide.

Remove property from SIP or EISUP profile

Use the following command to remove a property from a SIP or EISUP profile:

```
mml> prov-dlt:profile:name="spf1","noninvitereqattempts"
```

Caution: Be sure to specify a property value when deleting a property from a SIP or EISUP profile. If you do not, the command deletes the entire profile.

Delete SIP or EISUP profile

Use the prov-dlt command to delete a SIP or EISUP profile:

```
mml> prov-dlt:profile:name="spf1"
```

Note: You cannot delete a SIP or EISUP profile that is referenced by another profile.

Common profiles

Common profiles allow you to apply SIP or EISUP profiles to profile types that use other protocols, such as SS7. Use the following commands to provision common profiles.

Add common profile

Use the prov-add:profile command to add a common profile:
Clone common profile

The base parameter allows you to create a new profile based on an existing profile. To use this parameter, create a new profile and set the base parameter to an existing profile name. The new profile has the properties of the original profile, but you can override the settings of the original profile properties by manually specifying them in the command. Both profiles must be of the same type.

```
mml> prov-add:profile:name="cpf1", type="COMMONPROFILE", glare="0"
mml> prov-add:profile:name="cpf2", type="COMMONPROFILE", base="cpf1", responseattempts="2"
```

Retrieving a common profile

Use the `prov-rtrv:profile` command to retrieve common profile properties. This command has the following parameters:

- `prop`—Displays the provisioning property settings for the profile
- `comp`—Displays the components associated with the profile
- `all`—Displays the profile name, type, and property names, and values for all existing profiles

```
mml> prov-rtrv:profile:"prop", name="cpf1"
mml> prov-rtrv:profile:"comp", name="gpf2"
mml> prov-rtrv:profile:"all"
```

Modify common profile

Use the `prov-ed:profile` command to modify a common profile:

```
mml> prov-ed:profile:name="cpf1", noninvitereqattempts="2"
```

Remove property from a common profile

Use the following command to remove a property from a common profile:

```
mml> prov-dlt:profile:name="cpf1", "noninvitereqattempts"
```

Caution

Be sure to specify a property value when deleting a property from a group or common profile. If you do not, the command deletes the entire profile.

Delete common profile

Use the `prov-dlt` command to delete a common profile:

```
mml> prov-dlt:profile:name="cpf1"
```

Provision domain profiles

The commands to provision domain profiles are similar to the commands for provisioning SIP and EISUP profiles, with the exception that SIP and EISUP provisioning properties are not available. Use the commands in the following sections to provision domain profiles.

Add domain profile

The following example demonstrates how to add a new domain profile:

```
mml> prov-add:profile:name="dpf1", type="DOMAINPROFILE", topologyhidingenabled="2", trustlevel="1"
```
Clone domain profile
The base parameter allows you to create a new profile based on an existing profile. To use this parameter, create a new profile and set the base parameter to an existing profile name. The new profile has the properties of the original profile, but you can override the settings of the original profile properties by manually specifying them in the command. Both profiles must be of the same type.
```
mml> prov-add:profile:name="dpf2", type="DOMAINPROFILE", base="dpf1",trustlevel="1"
```

Retrieve domain profile
Use the `prov-rtrv:profile` command to retrieve domain profile properties. This command has the following parameters:
- `prop`—Displays the provisioning property settings for the profile
- `comp`—Displays the components associated with the profile
- `all`—Displays the profile name, type, and property names, and values for all existing profiles

```
mml> prov-rtrv:profile:"prop", name="dpf1"
mml> prov-rtrv:profile:"comp", name="dpf2"
mml> prov-rtrv:profile:"all"
```

Modify domain profile
Use the `prov-ed:profile` command to modify a domain profile:
```
mml> prov-ed:profile:name="dpf1", topologyhidingenabled="1"
```

Add common profile or Grprofile Reference to a domain profile
You can add a common or grprofile reference within a domain profile using the `commonprofile` and `grprofile` parameters.
```
mml> prov-ed:profile:name="dpf1",commonprofile="cpf1"
mml> prov-ed:profile:name="dpf1",grprofile="gpf1"
```

**Note** You must create Common Profiles or grprofiles before referencing them in a domain profile. For instructions on how to create a grprofile, see the *Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Provisioning Guide*.

Remove property from a domain profile
Use the `prov-dlt:profile` command to remove a property from a domain profile:
```
mml> prov-dlt:profile:name="dpf1", "topologyhidingenabled"
```

**Caution** Be sure to specify a property value when deleting a property from a SIP or EISUP profile. If you do not, the command deletes the entire profile.

Delete domain profile
Use the `prov-dlt` command to delete a domain profile:
```
mml> prov-dlt:profile:name="dpf1"
```

**Note** You cannot delete a domain profile that is referenced by another profile.

Manage The Domain Table
The domain table defines a set of domain names and associates them with a domain profile for both inbound and outbound traffic. Use these commands to manage the domain table.
Add New domain name
Use the `prov-add:domainprof` command to add a new domain name to the domain table. Type (inbound or outbound) and profile are required.

```
mml> prov-add:domainprof:domain="cisco.com", type="OUTBOUND", profile="dpf1"
```

Edit domain properties
Use the `prov-ed:domainprof` command to modify the properties of a domain name:

```
mml> prov-ed:domainprof:domain="cisco.com", type="INBOUND", profile="dpf1"
```

Modify domain profile assigned to a domain
Use the `prov-ed:domainprof` command to change the domain profile assigned to a domain name:

```
mml> prov-ed:domainprof:domain="cisco.com", type="INBOUND", profile="dpf1"
```

Retrieve domain names
Use the `prov-rtrv:domainprof` command to retrieve domain names from the domain table. To retrieve properties for an individual domain, specify the domain name and type (inbound or outbound).

```
mml> prov-rtrv:domainprof:domain="cisco.com", type="INBOUND"
mml> prov-rtrv:domainprof:domain="cisco.com", type="OUTBOUND"
```

To retrieve properties for all domain names in the domain table, enter the following command:

```
prov-rtrv:domainprof:"all"
```

Delete domain name
Use the `prov-dlt:domainprof` command to delete a domain name from the domain table:

```
mml> prov-dlt:domainprof:domain="cisco.com", type="OUTBOUND"
```

---

Note  You cannot delete a domain name that is referenced by a domain profile.

---

Assign profiles to trunk groups
To customize call behavior assigns one profile to each trunk group. Use these commands to assign profiles to trunk groups.

Tip  In many cases, inbound and outbound trunk groups can utilize the same profile.

---

Add profile to a trunk group
The created profiles above are associated with trunk groups. The inbound and outbound trunk groups typically have the same profile. Use the `prov-add:trnkgrpprof` command to add a trunk group to a profile:

```
mml> prov-add:trnkgrpprof:name="1", profile="spf1"
mml> prov-add:trnkgrpprof:name="2", profile="gpf1"
```

Modify profile assigned to a trunk group
Use the `prov-ed:trnkgrpprof` command to modify the profile associated with a trunk group:

```
mml> prov-ed:trnkgrpprof:name="1", profile="spf2"
```
Remove trunk group from a profile
Use the `prov-dlt:trnkgrpprof` command to remove a trunk group from a profile:
```
mml> prov-dlt:trnkgrpprof:name="1",profile="spf1"
```

Provision SIP header tables
Use the commands described in the following sections to provision SIP header tables.

Add Inbound SIP header table entry
Use the `prov-add:insipheader` command to add an inbound SIP header table entry:
```
mml> prov-add:insipheader:name="insipht1",header="p-asserted-identity", message="INVITE",cond=2,treat=1, cdw1="user=phone"
```

**Note** To create a new SIP header table, use a new header table name when adding a table entry. The Cisco VPGW Softswitch creates the new SIP header table automatically.

Add outbound SIP header table entry
Use the `prov-add:outsipheader` command to add an outbound SIP header table entry:
```
mml> prov-add:outsipheader:name="outsipht1",header="user-agent",message="INVITE",co nd=0, treat=5 ,cdwl="pgw Release 9.9",policy="ALL"
```

Add SIP header table to a profile
Use the `prov-ed:profile` command to add a SIP header table to a profile:
```
mml> prov-ed:profile:name="spf1", outsipheadertable="outsipht1"
```

Modify SIP header table entry
Use the `prov-ed:insipheader` command to modify a SIP header table entry:
```
mml> prov-ed:insipheader:name="insipht1",index=1, cdw1="user=phone"
```

**Note** You must provide an index value to edit SIP header table entries.

Retrieve SIP header table
Use the `prov-rtrv:insipheader` or `prov-rtrv:outsipheader` command to retrieve SIP header tables.
```
mml> prov-rtrv:insipheader:name="insipl"
mml> prov-rtrv:insipheader:name="insipl", message="INVITE"
mml> prov-rtrv:insipheader:name="insipl", header="user-agent"
```

Use the following command to retrieve all SIP header tables:
```
mml> prov-rtrv:insipheader:"all"
```

Retrieve SIP header table entry
To retrieve an individual entry in a SIP header table, use the `prov-rtrv:insipheader` or `prov-rtrv:outsipheader` command and specify an index, header, or message value.
```
mml> prov-rtrv:insipheader:name="insipl", index=1
mml> prov-rtrv:outsipheader:name="outsipl", header="user-agent"
mml> prov-rtrv:outsipheader:name="outsipl", message="INVITE"
mml> prov-rtrv:insipheader:name="insipl2",index=1, header="user-agent",message="INVITE"
```
Note: You can retrieve a SIP header table entry using an index, header, or message value.

**Reorder SIP header table**

The following caveats apply when you reorder a SIP header table:

- If you create a new SIP table header entry without specifying an index value, the Cisco VPGW Softswitch assigns a value higher than the largest existing index number. If you attempt to set a larger index value, the Cisco VPGW Softswitch replaces the new value with the default next value.
- If you set a SIP table header table entry to an existing index value, the new entry takes this value, and all affected entries are incremented by one.
- To move an entry backward in index order, use the **prov-add** and **prov-dlt** commands to remove the original entry and insert it earlier in the index order.

**Delete entry from a SIP header table**

Use the **prov-dlt:insipheader** command to delete an entry from a SIP header table:

```
mml> prov-dlt:insipheader:name="insipht1",index=1, header="user-agent", message="INVITE"
```

Note: You must enter an index, header, and message value to delete a SIP header table entry.

**Delete SIP header table**

Use the **prov-dlt:insipheader** command to delete a SIP header table:

```
mml> prov-dlt:insipheader:name="insipht1"
```

Note: You cannot delete a SIP header table that is referenced in a profile.

**Provisioning example**

This section provides a provisioning example for this feature. Additional provisioning examples for the Cisco VPGW Softswitch software can be found in the *Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Provisioning Guide*.

```
; Group Profile
; Group Profile
mml> prov-add:profile:name="gp1",type="GRPROFILE",cgpninclude="1"

; Common Profile
; Common Profile
mml> prov-add:profile:name="cp1",type="COMMONPROFILE",mgcdomain="10.0.6.55"

; ISUP Timer Profile
; ISUP Timer Profile
mml> prov-add:profile:name="isuptmrp1",type="ISUPTMRPROFILE",t6="120000", variant="etsi356",t2="180000",t9="60000",t33="12000",validation="OFF"

; SIP Profile
; SIP Profile
mml> prov-
add:profile:name="sp1",type="SIPPROFILE",custgrpid="1111",mgcdomain="10.0.6.55", trustlevel="1",topologyhidingenabled="1"
mml> prov-
add:profile:name="sp2",type="SIPPROFILE",grprofile="gp1",commonprofile="cp1"
mml> prov-
ed:profile:name="sp2",isuptmrprofile="isuptmrp1"
```
Software Changes

The following document contains software changes related to the SIP Profiles feature.

MML commands

This section documents new, modified, or deleted Man-Machine Language (MML) commands. All other MML commands are documented in the Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 MML Command Reference.

New MML Commands

This section document MML commands that are new for this feature.

PROV-ADD:INSIPHEADER

Purpose: This MML command adds an inbound SIP header table.

Syntax:

```
prov-add:insipheader: name="Header Table Name", header="Header Name", message="Message Name", index="Index", cond="Condition", cdw1="Condition Word 1", cdw2="Condition Word 2", cdw3="Condition Word 3", cdw4="Condition Word 4", treat="treatment", tdw1="treatment word 1", tdw2="treatment word 2", tdw3="treatment word 3", tdw4="treatment word 4"
```
Input Description:

- **name**—The name of the SIP header table.
- **header**—The name of a SIP header that the Cisco VPGW Softswitch uses to modify traffic.
- **message name**—The name of the SIP message that triggers a customized action. The value must be the name of a SIP request or response message.
- **index**—Defines the order in which the Cisco VPGW Softswitch applies SIP header table entries. If a SIP header matches more than one entry in the SIP Header Table, the Cisco Virtual_PGW Softswitch applies the entry with the lowest index value.
- **cond**—Defines how the Cisco Virtual_PGW Softswitch uses the SIP header table entry to analyze traffic. This field requires one or more entries in the Condition DW fields.
- **cdw1–4**—The tags the Cisco Virtual_PGW Softswitch uses to analyze SIP traffic.
- **treat**—The action that the Cisco Virtual_PGW Softswitch takes when the SIP header is present.
- **tdw1–4**—Data words that describe how the Cisco Virtual_PGW Softswitch applies the treatment settings.

**Note** For more information about applying inbound SIP headers, see Inbound SIP Header Tables.

Output Description:

- **COMPLD**—Provision succeeds.
- **DENY**—Provision fails.

Example:

```
prov-add:insipheader:name='insipt1',message='INVITE',cond=2,treat=1,cdw1='user=phone',header='User-Agent'
```

MGC-01 - Media Gateway Controller 2008-03-04 10:47:38.222 EST
M COMPLD
'insipheader'

Comments:

Performance impact category C applies to the commands used to create, delete, and edit inbound SIP header tables.

For more information about performance impact categories, see *Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 MML Command Reference*.

---

**PROV-ADD:OUTSIPHEADER**

**Purpose:**

This MML command adds an outbound SIP header table.
Syntax:

```
prov-add:outsipheader: name="Header Table Name", header="Header Name", message="Message Name", policy="Policy", index="Index", cond="Condition", cdw1="Condition Word 1", cdw2="Condition Word 2", cdw3="Condition Word 3", cdw4="Condition Word 4", treat="treatment", tdw1="treatment word 1", tdw2="treatment word 2", tdw3="treatment word 3", tdw4="treatment word 4"
```

Input Description:

- **name** — The name of the SIP header table.
- **header** — The name of a SIP header that the Cisco Virtual_PGW Softswitch uses to modify traffic.
- **message name** — The name of the SIP message that triggers a customized action. The value must be the name of a SIP request or response message.
- **policy** — Defines the B2BUA mode applied to the call/trunk group.
- **index** — Defines the order in which the Cisco Virtual_PGW Softswitch applies SIP header table entries. If a SIP header matches more than one entry in the SIP Header table, the Cisco Virtual_PGW Softswitch applies the entry with the lowest Index value.
- **cond** — Defines how the Cisco Virtual_PGW Softswitch uses the SIP header table entry to analyze traffic. This field requires one or more entries in the Condition DW fields.
- **cdw1-4** — The tags the Cisco Virtual_PGW Softswitch uses to analyze SIP traffic. You can define up to four tags for each row in the SIP header table. SIP table header treatments take effect only if a message matches all of the Condition DW fields.
- **treat** — The action that the Cisco Virtual_PGW Softswitch takes when the SIP header is present.
- **tdw1-4** — Data words that describe how the Cisco Virtual_PGW Softswitch applies the treatment settings. For values 2–3 in the Treatment field, Treatment DW1 defines the response code used to reject the request. For values 4–6 in the Treatment field, Treatment DW1–4 define the tag the Cisco Softswitch applies. You can apply up to four tags for each row in the SIP header table.

**Note** For more information about applying inbound SIP headers, see [Implementing Inbound SIP Header Tables](#).

Output Description:

- **COMPLD** — Provision succeeds.
- **DENY** — Provision fails.

Example:

```
prov-add:outsipheader:name='outsipht1',header='Diversion',message='INVITE',cond=1,treat=1,cdw1='xyf2',policy=0,index=1
```

MGC-01 - Media Gateway Controller 2008-03-04 10:51:22.260 EST
M COMPLD
'outsipheader'


Comments: Performance impact category C applies to the commands used to create, delete, and edit outbound SIP header tables.

For more information about performance impact categories, see Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 MML Command Reference.

**PROV-ADD:DOMAINPROF**

**Purpose:** This MML command creates an entry in the domain table.

**Syntax:**

`prov-add:domainprof:domain="Domain Name",type="Inbound or Outbound",profile="Domain Profile Name"`

**Input Description:**

- **domain**—The domain name used to analyze traffic
- **type**—The direction of the profile (inbound or outbound)
- **profile**—The name of a domain profile that is used for the domain name

**Output Description:**

- **COMPLD**— Provision succeeds.
- **DENY**— Provision fails.

**Example:**

```
mml> prov-add:domainprof:domain='cisco.com',type='INBOUND',profile='dpf1'
```

MGC-01 - Media Gateway Controller 2008-03-04 10:47:38.222 EST
M COMPLD
''domainprof'' ;

Comments: Performance impact category A applies to the commands used to manage the domain table.

For more information about performance impact categories, see Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 MML Command Reference.

**Modified MML Commands**

This section documents MML commands that are modified for this feature.

**PROV-ADD:PROFILE**

**Purpose:** This MML command creates a SIP, EISUP, Domain, or Common profile.
Syntax: prov-add:profile:name= "profile name",
type="SIPPROFILE",validation="ON", base="existing profile",
cat="Category", topologyhidingenabled="enablevalue",
trustlevel="level"

Input Description:
- **name**—The name of the new profile.
- **type**—The type of profile you wish to create. The available options are
  - SIPPROFILE
  - EISUPPROFILE
  - DOMAINPROFILE
  - COMMONPROFILE
- **validation**—Indicates if profile property validation is enabled or disabled.
  Valid values are ON and OFF.

Note: Validation can be disabled only for ISUP timer profiles.

- **base**—The name of an existing profile used to create the new profile. The properties of the existing profile are copied to the new profile.
- **cat**—A property category name which is used to filter the provisioning properties. This parameter allows you to apply a command to a subset of provisioning properties. Valid values are
  - A&R
  - Billing
  - Media
  - Misc
  - Number
  - SIP
  - Timer
- **topologyhidingenabled**—Indicates if topology hiding is enabled. Valid values are:
  - 0 (based on trustLevel value)
  - 1 (disabled)
  - 2 (enabled)
- **trustlevel**—Defines the trust level assigned to a profile. Valid values are
  - 0 (trusted)
  - (nontrusted)

Output Description:
- **COMPLD**—Provision succeeds.
- **DENY**—Provision fails.
Example: mml> prov-add:profile:name="spf1", type="SIPPROFILE", validation="ON", cat="SIP", topologyhidingenabled="2", trustlevel="1"

MGC-01 - Media Gateway Controller 2008-03-04 10:47:38.222 EST
M COMPLD
'
profile'

Comments: The base property is new in 9.9(1) and allows you to create a new profile based on an existing profile. To use this property, set the base property to the name of an existing profile. You can set additional properties to override the values copied from the original profile.

Performance impact category A applies to this command. For more information about performance impact categories, see Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 MML Command Reference.

Properties
The SIP Profiles feature replaces all existing SIP and EISUP trunk group properties with equivalent SIP and EISUP profile properties. For a full listing of all affected properties, see Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Provisioning Guide.

The following tables describe the trunk group properties used for this feature.

Table 9  Software Properties Related to This Feature

<table>
<thead>
<tr>
<th>Property Name</th>
<th>AVM</th>
<th>DPNSS</th>
<th>EISUP</th>
<th>ISDNPRI</th>
<th>MGCP</th>
<th>QSIG</th>
<th>RLM</th>
<th>SESSION</th>
<th>SGCP</th>
<th>SIP</th>
<th>SS7-ANSI</th>
<th>SS7-China</th>
<th>SS7-ITU</th>
<th>SS7-Japan</th>
<th>SS7-UK</th>
<th>TAI-HOCC</th>
<th>TrunkGroup</th>
<th>VSI</th>
<th>LI</th>
<th>CII-QBE</th>
</tr>
</thead>
<tbody>
<tr>
<td>commonprofile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>grprofile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>isuptmrprofile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>insipheadertable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>outboundDomainProfileSource</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>outsipheadertable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>topologyHidingEnabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trustLevel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>useDomainProfile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>commonprofile</td>
<td>Contains a pointer to a Common Profile.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid values: String. Enter the name of an existing Common Profile.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value: NULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamically reconfigurable: Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>grprofile</td>
<td>Contains a pointer to a GRPROFILE profile.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid values: String. Enter the name of an existing Group Profile.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value: NULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamically reconfigurable: Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>insipheadertable</td>
<td>Contains a pointer to an inbound SIP header table.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid values: String. Enter the name of an existing inbound SIP Header table.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value: NULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamically reconfigurable: Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>isuptmrprofile</td>
<td>Contains a pointer to an ISUP timer profile.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid values: String. Enter the name of an existing ISUP timer profile.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value: NULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamically reconfigurable: Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>outboundDomainProfileSource</td>
<td>Indicates the source that the Cisco VPGW Softswitch uses for the outbound domain name.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 = If available, the Cisco VPGW Softswitch uses the domain used for routing as introduced by the domain-based routing feature. Otherwise, the Cisco VPGW Softswitch uses the domain of the SIP trunk group.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 = The Cisco VPGW Softswitch uses the domain of the SIP trunk group.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamically reconfigurable: Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>outsipheadertable</td>
<td>Contains a pointer to an outbound SIP header table.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid values: String. Enter the name of an existing outbound SIP header table.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value: NULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamically reconfigurable: Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### topologyHidingEnabled

Indicates whether topology hiding is enabled.

Valid values:
- 0 = Trust level configuration
- 1 = Disabled
- 2 = Enabled

Default value: 1
Dynamically reconfigurable: Yes

### trustLevel

Indicates if the trunk group or domain is on a trusted or nontrusted interface.

Valid values:
- 0 = trusted
- 1 = nontrusted

Default value: 0
Dynamically reconfigurable: Yes

### useDomainProfile

Indicates whether domain profiles are enabled for a SIP profile.

Valid values:
- 0 = Disabled
- 1 = Enabled

Default value: 1
Dynamically reconfigurable: Yes

### Worksheets for Provisioning

This section contains worksheets for the provisioning components required for this feature. For worksheets covering the rest of the provisioning components in the Cisco VPGW Softswitch software, see *Cisco Virtual PGW 2200 (VPGW) Softswitch Release 9.9 Provisioning Guide*.

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Type</th>
<th>Trust Level</th>
<th>Topology Hiding</th>
<th>Property</th>
<th>Value</th>
<th>Profile Reference</th>
<th>SIP Header Table Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>spf1</td>
<td>SIP</td>
<td>0</td>
<td>1</td>
<td>ACCRespCntlInhibit</td>
<td>1</td>
<td>outsipht1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ADigitCCPrefix</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>spf2</td>
<td>EISU</td>
<td>1</td>
<td>2</td>
<td>epf1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 11: SIP and EISUP Profiles Worksheet Example
### Table 12  Common Profiles Worksheet Example

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Type</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>epf1</td>
<td>Common</td>
<td>Glare</td>
<td>0</td>
</tr>
<tr>
<td>gpf1</td>
<td>Group</td>
<td>cgpninclude</td>
<td>1</td>
</tr>
</tbody>
</table>

### Table 13  Domain Profile Worksheet Example SIP_Profiles_v2

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Domain</th>
<th>Direction</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dpf1</td>
<td>cisco.com</td>
<td>Inbound</td>
<td>populatesdpinfoincdr</td>
<td>1</td>
</tr>
<tr>
<td>dpf2</td>
<td>bt.com</td>
<td>Outbound</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 14  Trunk Group Profile Assignments Worksheet Example

<table>
<thead>
<tr>
<th>Trunk Group Number</th>
<th>Profile Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>spf1</td>
</tr>
<tr>
<td>2</td>
<td>gpf1</td>
</tr>
</tbody>
</table>
### Table 15  
**SIP Header Tables Worksheet Example**

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>insipht1</td>
<td>Inbound</td>
<td></td>
</tr>
<tr>
<td>outsipht1</td>
<td>Outbound</td>
<td></td>
</tr>
</tbody>
</table>

### Table 16  
**Inbound SIP Header Table Worksheet Example**

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Message</th>
<th>Condition</th>
<th>Treatment</th>
<th>DW1 Condition</th>
<th>DW2 Condition</th>
<th>DW3 Condition</th>
<th>DW4 Condition</th>
<th>DW1 Treatment</th>
<th>DW2 Treatment</th>
<th>DW3 Treatment</th>
<th>DW4 Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote-Party_id</td>
<td>INVITE</td>
<td>2</td>
<td>4</td>
<td>User=</td>
<td>Rpi-</td>
<td></td>
<td></td>
<td>;User=phone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Referred-By</td>
<td>REFER</td>
<td>2</td>
<td>4</td>
<td>Pgw.cisco.co m</td>
<td>Cisco.com</td>
<td></td>
<td></td>
<td>CallerDomain.com</td>
<td></td>
<td>Pgw.cisco.co m</td>
<td></td>
</tr>
</tbody>
</table>

### Table 17  
**Outbound SIP Header Table Worksheet Example**

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Apply Policy</th>
<th>Message</th>
<th>Condition</th>
<th>Treatment</th>
<th>Condition DW1</th>
<th>Condition DW2</th>
<th>Treatment DW1</th>
<th>Treatment DW2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry-After</td>
<td>Trusted</td>
<td>503</td>
<td>2</td>
<td>5</td>
<td>Duration=</td>
<td>;Duration=100</td>
<td>;Reason=overload</td>
<td></td>
</tr>
<tr>
<td>Referred-By</td>
<td>ALL</td>
<td>REFER</td>
<td>2</td>
<td>6</td>
<td>CallerDomainA</td>
<td>CallerDomainA.com</td>
<td>PGWA.cisco.com</td>
<td></td>
</tr>
</tbody>
</table>
### Table 18: Acronym Expansions and Definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B</td>
<td>Back to back. See B2BUA.</td>
</tr>
<tr>
<td>B2BUA</td>
<td>A device that acts as a user agent on both ends of a call. The B2BUA handles all SIP signalling for both ends of the call and maintains state for all dialogues.</td>
</tr>
<tr>
<td>CDR</td>
<td>Call detail record. A record containing call information that is used in billing.</td>
</tr>
<tr>
<td>EISUP</td>
<td>Extended-ISUP. Originally a subset of Q.761 ISUP.</td>
</tr>
<tr>
<td>MGC</td>
<td>Cisco Media Gateway Controller.</td>
</tr>
<tr>
<td>MML</td>
<td>Man-Machine Language. Industry standard command line language used to manage telecommunications network elements, including the Cisco VPGW Softswitch.</td>
</tr>
<tr>
<td>VPGW</td>
<td>Virtual PSTN Gateway</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol. A protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.</td>
</tr>
<tr>
<td>Tel: URI</td>
<td>Telephone Uniform Resource Identifier.</td>
</tr>
</tbody>
</table>

### Obtaining Documentation and Submitting a Service Request

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:


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.