Advanced Screening and Modification

Document Release History

Publication Date	Comments
July 18, 2003	Initial release of this document.

Feature History

Release	Modification
9.4(1)	This feature was introduced for MGC Release 9.4(1).

The Advanced Screening and Modification Feature is described in the following sections:

Feature Overview

The Advanced Screening and Modification feature allows the Cisco PGW 2200 Softswitch to perform additional screening and modification of normal voice dial plans, in addition to SIP and H.323-related dial plans.

Note Before the Advanced Screening and Modification feature, the PGW 2200 Softswitch could not use dial plans along with SIP or H.323.

Selecting Customer Group IDs Based on Source IP Addresses

Advanced Screening and Modification allows customers to select a customer group ID based on the source IP address. For example, if there are four call managers and H.323 is being used, the PGW 2200 Softswitch can read the source IP address in the H.323 message and determine that the H.323 message originated from different PGW 2200 Softswitches.

Determining and Selecting Customer Group ID

The Advanced Screening and Modification feature allows customers to select the customer group ID, based on the following:

- Last hop IP address,
- Source IP address, and/or
- Calling Number Prefix.

Determining the customer group ID, based on these values extends the PGW 2200 multiple dial plan capability beyond groups of normal voice call users to SIP and H.323 users based on the IP address of the last hop SIP Proxy or H.323 Gatekeeper; and also extends this flexibility to groups based on the Enhance Calling Line Identity (CLI) Prefix.

For example, if there are four call managers and H.323 is being used, the PGW 2200 Softswitch can read the source IP address in the H.323 message and determine that the H.323 message originated from different PGW 2200 Softswitches.

Using Last Hop IP Address to Modify Calls

This is used when a call with a Calling Party Number (CgPn) “703-123-4567” ingresses to a PGW 2200. In this example, since the CgPn contains “4567” and the call matches an IP address in the dial plan, the PGW 2200 sets SI to NP and passes the CgPn on unmodified.

See Advanced Screening and Modification Screening Example (NP) for more information.

Using Source IP Address to Screen Calls

This is used when a call with a CgPn “703-123-4567” ingresses to a PGW 2200. In this example, since CgPn contains “703123” and the call matches an IP address in the dial plan, the PGW 2200 sets SI to UPVP and passes the CgPn on unmodified.

See Advanced Screening and Modification Screening Example (UPVP) for more information.

Using Calling Number Prefix to Modify Calls

This can be used in a company in which internal company calls can be routed over an IP network by entering only a few digits of the called telephone extension, as opposed to the full telephone number.

See Advanced Screening and Modification Example (Source-Based Routing) for more information.

Implementing Multiple Dial Plans for Ingress Calls

Advanced Screening and Modification allows customers to implement multiple dial plans. Using multiple dial plans for SIP and H.323 in each PGW 2200 Softswitch allows users to leverage and re-use dial plans in both SIP and H.323 implementations.

Note See the following sections in this document for information about using this feature:
Provisioning CLI IP Address, page 6
Provisioning CLI Prefix, page 7
Provisioning H.323 ID, page 7

Handling Trusted and Untrusted Ingress Calls

Advanced Screening and Modification allows the Cisco PGW 2200 Softswitch to handle trusted and untrusted connections. Trust is important to:

- Protect the privacy of subscribers who wish to remain anonymous for signaling that is sent out.
- Determine the validity of Caller Identification information that is received.

Trusted and Untrusted Call Examples

Examples of identifying trusted and untrusted calls:

- PGW 2200 Softswitch prevents a user of a SIP user agent from masquerading as another device by allowing the SP to overwrite the received Calling Number with a Network Provided calling number using the PGW 2200 Softswitch.
- PGW 2200 Softswitch extends new and existing trunk group properties to allow the users to set trust policies with regard to passing Calling Number or Connected Number over a certain Trunk Group.
- PGW 2200 Softswitch enforces the Network Code of Practice on outgoing trunks. For example, service providers typically provision PGW 2200 trunk groups to enforce the Network Code of Practice if they do not trust the system downstream. When enforced, the PGW 2200 Softswitch removes numbers that have their associated Presentation Indicators set to “Restricted”.

Note See the following sections in this document for information about using this feature:
Verifying Incoming Calls that Do Not Have a Presentation Number, page 10.
Verifying Incoming Calls that Do Not Have an NOA Presentation Number, page 10.
Verifying Incoming Calls that Do Not Have an NPI Presentation Indicator, page 10.
Verifying Incoming Calls that Do Not Have a PN Presentation Indicator, page 11.

Enforcing Network Code of Practice

The PGW 2200 Softswitch uses the existing trunk group properties to enforce the Network Code of Practice. This applies to ISUP, PRI, SIP, and H.323 (E-ISUP) trunk groups. The parameters include numbers with a presentation indicator. Messages in the forward direction containing:

- Calling Party Number (CgPN)
- Generic Number:
  - Additional CLI
  - Redirecting Number
  - Original Called Number
- Redirecting Number
- Original Called Number
- Backward messages:
  - Redirection Number
  - Connected Number
  - Generic Number (Additional Connected Number and Redirection Number).

Additional Features

Screening the Calling Party Number

The PGW 2200 Softswitch screens (based on Customer Group ID) the Calling Party number against the correct white or black list, selecting the appropriate part of the table by “Service Name” if the Bwhite list or Bblack list is used.

This functionality is added for screening success and failure cases. Users can choose to change the dial plan and restart with the pre-analysis in either the success or failure cases.

Note For information on other result type definitions for the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide* for information about using this feature.

Screening COLI

The PGW 2200 Softswitch does not need to screen COLI. For PRI trunks, the PGW 2200 Softswitch sets the SI = 1, which is “UPNV” (user provided, not verified).

Note See the Advanced Screening and Modification Screening Example (UPVP), page 22 for information about using this feature.

New Components, Result Types, and Properties

See Command Reference, page 12 for information regarding added components, result types, and properties.

Related Documents

This document contains information that is related strictly to the Advanced Screening and Modification feature. The documents that contain additional information related to the Cisco Media Gateway Controller (MGC) are:

- *Release Notes for Cisco Media Gateway Controller Software Release 9.4(1)*
- *Cisco Media Gateway Controller Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Media Gateway Controller*
- *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
- *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*
- *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide*
- *Cisco Media Gateway Controller Software Release 9 MML Command Reference 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 MIB Guide*
- *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide*
- *Cisco H.323 Signaling Interface Guide*
- *Cisco Voice Services Provisioning Tool User Guide*
- *Billing and Measurements Server User Guide*

Supported Platforms

The hardware platforms supported for the Cisco MGC software are described in the *Release Notes for Cisco Media Gateway Controller Software Release 9.4(1)*.

Prerequisites

SPs that interconnect the PGW 2200 Softswitch for regular voice networks in addition to H.323 or SIP networks may elect to use Advanced Screening and Modification.

Provisioning Tasks

The following provisioning tasks are explained in this section:

- Provisioning CLI IP Address
  - Adding CLI IP Address to a Customer Group
  - Deleting CLI IP Address with Subnet Mask from a Customer Group
  - Editing CLI IP Address
- Provisioning CLI Prefix

Planning for Provisioning

Before you provision Advanced Screening and Modification-related commands, you must have the following information about your installation:

- H.323 messages coming from different call managers
- Dial plan information (depending on the source IP address of the call manager)

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

Provisioning CLI IP Address

The **cliipaddress** parameter allows you to associate an IP address with a specific customer group.

Adding CLI IP Address to a Customer Group

Use the following steps to add the CLI IP address to a customer group:

Step 1 Add a customer group to the Dial Plan table if one has not already been created:

```
mml> numan-add:dialplan:custgrpid="Cust_1"
```

Step 2 Define cliprefix and group them by clisetname:

```
mml> numan-add:cliprefix:clisetname="x", cliprefix="1844260", custgrpid="Cust_1"
```

Step 3 Define IP address and subnet to customer group:

```
mml> numan-add:cliipaddress:custgrpid="Cust_1",ipaddr="172.22.99.247",
subnetmask="255.255.0.0, clisetname="x"
```

Deleting CLI IP Address with Subnet Mask from a Customer Group

Use the following command to delete CLI IP address with subnet mask from a customer group:

```
mml> numan-dlt:cliipaddress:custgrpid="Cust_1",ipaddr="172.22.99.170",subnet=
"255.255.255.0"
```

Editing CLI IP Address

Use the following command to edit the CLI IP address for a customer group:

```
mml> numan-ed:cliipaddress:custgrpid="Cust_1",ipaddr="172.22.121.247",clisetname="x"
```

Provisioning CLI Prefix

The **cliprefix** parameter allows you to associate a CLI prefix with a specific customer group. If an incoming call matches the CLI prefix parameter, you can apply certain dial plan functions to it.

Adding CLI Prefix to a Customer Group

Use the following steps to add CLI prefix to a customer group:

Step 1 Add a customer group to the Dial Plan table if one has not already been created:

```
mml> numan-add:dialplan:custgrpid="Cust_1"
```

Step 2 Add CLI prefix to customer group.

```
mml> numan-add:cliprefix:clisetname="x",cliprefix="408",custgrpid="Cust_1"
```

Deleting CLI Prefix from a Customer Group

Use the following command to remove CLI prefix from a customer group:

```
mml> numan-dlt:cliprefix:clisetname="x",cliprefix="DEFAULT"
```

Editing CLI Prefix

Use the following command to edit CLI prefix for a customer group:

```
mml> numan-ed:cliprefix:clisetname="x",cliprefix="DEFAULT",custgrpid="Cust_1"
```

Provisioning H.323 ID

The **h323iddivfrom** parameter allows you to associate an H.323 ID with a specific customer group. If an incoming call matches the H.323 ID parameter, you can apply certain dial plan functions to it.

Adding H.323 ID to a Customer Group

Use the following steps to add H.323 ID to a customer group:

Step 1 Add customer group to Dial Plan table if one has not already been created:

```
mml> numan-add:dialplan:custgrpid="Cust_1"
```

Step 2 Add H.323 ID to customer group.

```
mml> numan-add:h323iddivfrom:custgrpid="Cust_1",h323iddivfrom="4eaf005",clisetname="x"
```

Deleting H.323 ID from a Customer Group

Use the following command to remove H.323 ID from customer group:

```
mml> numan-dlt:h323iddivfrom:custgrpid="Cust_1",h323iddivfrom="4eaf005"
```

Editing H.323 ID

Use the following command to edit H.323 ID in a customer group:

```
mml> numan-ed:h323iddivfrom:custgrpid="Cust_1",h323iddivfrom="AFA1974",clisetname="x"
```

Importing Dial Plan Information

Use the following commands to import the following information:

```
mml> prov-add:files:name="cliprefixfile",file="abc1.dat",action="import"
mml> prov-add:files:name="ipaddrfile",file="abc2.dat",action="import"
mml> prov-add:files:name="h323idfile",file="abc3.dat",action="import"
```

Enabling Dial Plan Selection for Incoming Trunk groups

Enabling Dial Plan Selection for Incoming SIP Trunk Group

Use the following steps to configure and verify the **enableipscreening** property for an incoming SIP trunk group:

Step 1 Start and name MML provisioning session:

```
mml> prov-sta::srcver="SIP_EISUP_1001",dstver="sip_0801"
```

Step 2 Dynamically set the **enableipscreening** property to "1" for the SIP trunk group:

```
mml> prov-add:trnkgrpprop:name="550",enableipscreening="1"
```

Step 3 Commit the changes: `mml> prov-cpy`

Enabling Dial Plan Selection for Incoming EISUP Trunk Group

Use the following steps to configure and verify the **enableipscreening** property for an incoming EISUP trunk group:

Step 1 Start and name MML provisioning session:

`mml>` **`prov-sta::srcver="SIP_EISUP_1001",dstver="eisup_0801"`**

Step 2 Dynamically set the **enableipscreening** property to "1" for the EISUP trunk group:

`mml>` **`prov-add:trnkgrpprop:name="2000",enableipscreening="1"`**

Step 3 Commit the changes: `mml>` **`prov-cpy`**

Verifying Your Changes

- Verify that **prov-cpy** is successful.
- Verify the property is added correctly: `mml>` **`prov-rtrv:trnkgrpprop:"all"`**

Determining Which IP Address to Use for Dial Plan Selection

Configuring PGW 2200 Softswitch to Use IP Packet Source Address for Dial Plan Selection

Use the following steps to configure and verify the **sipipsource** property to use IP packet source address for dial plan selection:

1. Start and name MML provisioning session:

mml> **prov-sta::srcver="SIP_EISUP_1001", dstver="sip_0801"**

2. Dynamically set the **sipipsource** property to "0" for the SIP trunk group:

mml> **prov-add:trnkgrpprop:name="550",sipipsource="0"**

3. Commit the changes: mml> **prov-cpy**

Configuring PGW 2200 Softswitch to use IP from SDP INVITE for Dial Plan Selection

Use the following steps to configure and verify the **sipipsource** property to use IP address from SDP in INVITE for dial plan selection.

1. Start and name MML provisioning session:

mml> **prov-sta::srcver="SIP_EISUP_1001",dstver="sip_0801"**

2. Dynamically set the **sipipsource** property to "1" for the SIP trunk group:

mml> **prov-add:trnkgrpprop:name="550",sipipsource="1"**

3. Commit the changes: mml> **prov-cpy**

Verifying Your Changes

- Verify that **prov-cpy** is successful.

- Verify the property is added correctly: mml> **prov-rtrv:trnkgrpprop:“all”**

Verifying Incoming Trunk Group Calls

Verifying Incoming Calls that Do Not Have a Presentation Number

Use the following steps to configure and verify the **defaultpn** property on incoming trunk group for the incoming calls not having presentation number.

Step 1 Start and name MML provisioning session:

```
mml> prov-sta::srcver="SIP_EISUP_1001", dstver="ss7_0801"
```

Step 2 Set the **defaultpn** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000",defaultpn="4EAF005"
```

Step 3 Commit the changes: `mml>` **prov-cpy**

Verifying Incoming Calls that Do Not Have an NOA Presentation Number

Use the following steps to configure and verify the **defaultpnnoa** property on incoming trunk group for the incoming calls not having presentation number Nature of Address.

Step 1 Start and name MML provisioning session:

```
mml> prov-sta::srcver="SIP_EISUP_1001",dstver="ss7_0801"
```

Step 2 Set the **defaultpnnoa** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000", defaultpnnoa="5"
```

Step 3 Commit the changes: mml> **prov-cpy**

Verifying Incoming Calls that Do Not Have an NPI Presentation Indicator

Use the following steps to configure and verify the **defaultpnnpi** property on incoming trunk group for the incoming calls not having presentation number Nature of Presentation Indicator.

Step 1 Start and name MML provisioning session:

```
mml> prov-sta::srcver="SIP_EISUP_1001",dstver="ss7_0801"
```

Step 2 Set the **defaultpnnpi** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000",defaultpnnpi="6"
```

Step 3 Commit the changes: `mml>` **prov-cpy**

Verifying Incoming Calls that Do Not Have a PN Presentation Indicator

Use the following steps to configure and verify the **defaultpnpres** property on incoming trunk group for the incoming calls not having presentation number Presentation Indicator.

Step 1 Start and name MML provisioning session:

```
mml> prov-sta::srcver="SIP_EISUP_1001",dstver="ss7_0801"
```

Step 2 Set the **defaultpnpres** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000",defaultpnpres="6"
```

Step 3 Commit the changes: `mml> prov-cpy`

Verifying Your Changes

- Verify that **prov-cpy** is successful.
- Verify the property is added correctly: `mml> prov-rtrv:trnkgrp:name="1000"`

Result Types

```
mml> numan-add:dialplan:custgrpid="A001"
mml> numan-add:dialplan:custgrpid="A002"
mml> numan-add:service:custgrpid="1111",name="TollFree"
mml> numan-add:dpsel:custgrpid="1111",newdp="A001"
mml> numan-add:dpsel:custgrpid="1111",newdp="A002"
mml> numan-add:digmodstring:custgrpid="1111",name="mod1",digstring="12345"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1",resulttype="ROUTE", dw1="rlst1",setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t23",resulttype="SCREENING",
dw1="1",dw2="TollFree",dw3="A001",dw4="A002",setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t49",resulttype="PNMODDIG",dw1="3",dw2="5",dw3="mod1",
setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t50",resulttype="PN_NUMBER_TYPE",dw1="43",
setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t51",resulttype="PN_PRES_IND",dw1="3",setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t52",resulttype="CG_SCREEN_IND",dw1="5",
setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t53",resulttype="PN_SCREEN_IND",dw1="5",
setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t54",resulttype="A_NUM_NPI_TYPE",dw1="10",
setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t55",resulttype="CG_PN_COPY",
dw1="mod1",setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t56",resulttype="PN_NPI_TYPE",
dw1="10",setname="rset1"
mml> numan-add:resulttable:custgrpid="1111",name="rtab1t37",resulttype="CG_PRES_IND",dw1="3",setname="rset1"
```

Troubleshooting Tips

See SIP Call Traces for SIP call traces that may assist with call troubleshooting.

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

Command Reference

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

Components

The following components are added for this feature:

- cliprefix
- cliipaddress
- h323iddivfrom

Note The following validation rules apply to these components.
Provision cliprefix (since clisetname has to be defined first) before provisioning cliipaddress or h323iddivfrom.
The IP address format is validated.
The minimum and maximum string length are also validated.

cliprefix

This MML component adds **cliprefix** component to a dial plan table. Its MML name is as follows:

- numan-add:cliprefix
- numan-ed:cliprefix
- numan-dlt:cliprefix

The structure of this component is shown in the table below.

Parameter MML Name	Parameter Description	Parameter Values (Default)
CUSTGRPID	Trunk group Customer Group ID.	4 alphanumeric characters.
CLIPREFIX	CLI prefix.	1 to 20 overdecadic digits (0-9;A-F) or default
clisetname	A unique name that serves as a pointer to the cliPrefix table.	4 alphanumeric characters.

cliipaddress

This MML component adds **cliipaddress** component to a dial plan table. Its MML name is as follows:

- numan—add:cliipaddress
- numan—ed:cliipaddress
- numan—dlt:cliipaddress

The structure of this component is shown in the table below.

Parameter MML Name	Parameter Description	Parameter Values (Default)
CUSTGRPID	Trunk group Customer Group ID.	4 alphanumeric characters..
IPADDR	IP address.	N/A.
SUBNETMASK	Subnet mask.	N/A.
clisetname	A unique name that points to the cliPrefix table.	4 alphanumeric characters..

h323iddivfrom

This MML component adds **h323iddivfrom** component to a dial plan table. Its MML name is as follows:

- numan—add:h323iddivfrom
- numan—ed:h323iddivfrom
- numan—dlt:h323iddivfrom

The structure of this component is shown in the table below.

Parameter MML Name	Parameter Description	Parameter Values (Default)
CUSTGRPID	Trunk group Customer Group ID.	4 alphanumeric characters.
H323IDDIVFROM	The originating H.323 ID or the originating SIP from header or diversion header based on the MDLAnumberScreening parameter in XECfgParm.dat file for SIP calls.	1 to 32 alphanumeric characters..
clisetname	A unique name that points to the cliPrefix table.	4 alphanumeric characters..

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

Properties

New Properties

The following trunkgroup properties are added for this feature.

- DefaultPN Property
- DefaultPNNOA Property
- DefaultPNNPI Property
- DefaultPNPres Property
- EnableipScreening Property
- SIPipSource Property

DefaultPN Property

This property enables the incoming trunk group to have default PN if the incoming call does not have one, overdecadic digits are supported.

Valid Values: overdecadic digit string with minimum length 1 and maximum length 20.

Default Value: NULL

The following example shows the **DefaultPN** property for the TDM_ISUP trunk group:

```
mml> prov-add: grpprop:name="1000",defaultpn="4EAF005"
```

DefaultPNNOA Property

This property enables the default Presentation Number NOA value and Table 1 lists valid values.

Default: 0

The following example shows the **defaultpnnoa** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000",defaultpnnoa="5"
```

Table 1 Valid Values for defaultpnnoa Property

Value	Description
1	NOA_NONE
2	NOA_UNKNOWN
3	NOA_SUBSCRIBER
4	NOA_NATIONAL
5	NOA_INTERNATIONAL
6	NOA_NETWORK
7	NOA_MERIDIAN
8	NOA_ABBR
9	NOA_UNIQUE_3DIG_NAT_NUM
10	NOA_ANI
11	NOA_NO_ANI_RECD
12	NOA_NON_UNIQUE_SUBSCRIBER
13	NOA_NON_UNIQUE_NATIONAL
14	NOA_NON_UNIQUE_INTERNATIONAL
15	NOA_OPRREQ_TREATED
16	NOA_OPRREQ_SUBSCRIBER
17	NOA_OPRREQ_NATIONAL
18	NOA_OPRREQ_INTERNATIONAL
19	NOA_OPRREQ_NO_NUM
20	NOA_CARRIER_NO_NUM
21	NOA_950_CALL
22	NOA_TEST_LINE_CODE

Table 1 Valid Values for defaultpnnoa Property (continued)

Value	Description
23	NOA_INT_INBOUND
24	NOA_NAT_OR_INTL_CARRIER_ACC_CODE_INC
25	NOA_CELL_GLOBAL_ID_GSM
26	NOA_CELL_GLOBAL_ID_NMT_900
27	NOA_CELL_GLOBAL_ID_NMT_450
28	NOA_CELL_GLOBAL_ID_AUTONET
29	NOA_PORTED_NUMBER
30	NOA_PISN_SPECIFIC_NUMBER
31	NOA_UK_SPECIFIC_ADDRESS
32	NOA_SPARE
33	NOA_MCI_VNET
34	NOA_INTERNATIONAL_OPR_TO_OPR_OUTSIDE_WZI
35	NOA_INTERNATIONAL_OPR_TO_OPR_INSIDE_WZI
36	NOA_DIRECT_TERMINATION_OVERFLOW
37	NOA_ISN_EXTENDED_INTERNATIONAL_TERMINATION
38	NOA_TRANSFER_ISN_TO_ISN
39	NOA_CREDIT_CARD
40	NOA_DEFINED_IN_SSUTR
41	NOA_DEFINED_IN_SSUTR2
42	RESERVED
43	NOA_DISCARDED

DefaultPNNPI Property

This property displays the default Presentation Number NPI value and Table 2 lists the valid values.

Default Value: 0

The following example shows the **defaultpnnpi** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000",defaultpnnpi="6"
```

Table 2 Valid Values for defaultpnnpi Property

Value	Description
0	Not used.
1	NPI_NONE
2	NPI_E164
3	NPI_DATA
4	NPI_TELEX
5	NPI_PNP

Table 2 Valid Values for defaultpnnpi Property (continued)

Value	Description
6	NPI_NATIONAL
7	NPI_TELEPHONY
8	NPI_MARITIME_MOBILE
9	NPI_LAND_MOBILE
10	NPI_ISDN_MOBILE

DefaultPNPres Property

This property displays the Default Presentation Number Presentation Indicator value and Table 3 lists the valid values.

Default Value: 0

The following example shows the **defaultpnpres** property for the TDM_ISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="1000",defaultpnpres="6"
```

:

Table 3 Values for defaultpnpres Property

Value	Description
0	Not used.
1	PRES_NO_INDICATION
2	PRES_ALLOWED
3	PRES_RESTRICT
4	PRES_UNAVAIL

EnableipScreening Property

This property enables the incoming trunk group to select dial plan based on IP address, source ID and CLI prefix tables. lists valid values.

Default Value: 0

The following example shows the **enableipscreening** property for the EISUP trunk group:

```
mml> prov-add:trnkgrpprop:name="550",enableipscreening="1"
mml> prov-add:trnkgrpprop:name="2000",enableipscreening="1"
```

Table 4 Values for enableipscreening Property

Value	Description
0	no dial plan lookup
1	require dial plan lookup

SIPipSource Property

This property tells MDL to use IP packet source address or IP address from SDP in INVITE message to do dial plan selection for SIP calls.

Default Value: 0

The following example shows the **sipipsource** property for the SIP trunk group:

```
mml> prov-add:trnkgrpprop:name="550",sipipsource="0"
```

Table 5 Values for sipipsource Property

Value	Description
0	IP packet source address
1	IP address from SDP

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

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

Reference Information

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

- Billing Interface, page 17
- Result Type Definitions, page 18
- NOA and NPI Codes, page 22

Billing Interface

The Source IP Address tag (4204), shown in Table 6, has been added to support Advanced Screening and Modification.

Source IP Address (Tag: 4204)

Table 6 Source IP Address Description Form

Name: Source IP Address	**Tag:** 4204	**Source:** MDL
Description/Purpose: Source IP address used to identify the source which sends the call setup message in incoming SIP and H.323 calls.		
Format: IA5	**Length in Octets:** 1-23	
Data Value: IPV4 format. Example: 10.1.22.115		
ANSI/ITU Variations: None.		
Extended Data Value: No extended value.		
General Information: ·This source IP address is used to look up a dial plan in the IP Address table if the trunk group property EnableIPScreening is set to 1.		
MGC Release: Release 9.4(1).		

Answered (1010)	Deselected (1020)	Aborted (1030)	Release (1040)	Interrupted (1050)	Ongoing (1060)	Maintenance (1070)	External DB (1080)	End of Call (1110)
Y	N	Y	Y	N	N	N	N	Y

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

Result Type Definitions

The following result type definitions are modified (SCREENING and CG_PRES_IND) and the other result types listed in Table 7 are added for this feature.

Modified and Added Result Types

Table 7 Modified and Added Result Type Definitions

Result Number.	Result Type	Dataword1	Dataword2	Dataword3	Dataword4	Analysis Points		Result Type Valid For			
						Intermediate	End Point	A-digit analysis	B-digit analysis	Cause	Pre-analysis
23	SCREENING	Screen Type	Service Name	**New dial plan index if pass**	**New dial plan index if fail**	X		X	X		
37	CG_PRES_IND	**1 = Restricted** **2 = Allowed** **3 = Unavailable**	0 (not used)	0 (not used)	0 (not used)	X		X	X		

Table 7 Modified and Added Result Type Definitions (continued)

Result Number.	Result Type	Dataword1	Dataword2	Dataword3	Dataword4	Analysis Points		Result Type Valid For			
						Intermediate	End Point	A-digit analysis	B-digit analysis	Cause	Pre-analysis
49	PNMODDIG	Application point	Number of digits to remove	Modification Name	0 (not used)	X		X	X		
50	PN_NUMBER_TYPE	Internal NOA value (0-43)	0 (not used)	0 (not used)	0 (not used)	X		X	X		
51	PN_PRES_IND	1 = Restricted 2 = Allowed 3 = Unavailable	Local/Remote	RouteListId	AnnData	X		X	X		
52	CG_SCREEN_IND	1 = Network Provided 2 = UPVP 3 = UPNV 4 = UPVF 5 = spare1	0	0	0	X		X	X		
53	PN_SCREEN_IND	1 = Network Provided 2 = UPVP 3 = UPNV 4 = UPVF 5 = spare1	0	0	0	X		X	X		
54	A_NUM_NPI_TYPE	Internal NPI value (0-10)	0	0	0	X		X	X		
55	CG_PN_COPY	Index to Network Numbering string	0	0	0	X		X	X		
56	PN_NPI_TYPE	Internal NPI value (0-10)	0	0	0	X		X	X		

SCREENING

The SCREENING result type delivered from either A-number or B-number analysis indicates that the A-number must be screened against the screening files configured for a specific customer group ID.

Dataword1 (screen type) identifies the type of screening that must be requested.

• ScreenType—must be one of the following:

– 1 = Whitelist—If the presented A-number is not found in the screening files, then the screening is considered to have failed and the call is released.

– 2 = Blacklist—If the presented A-number is found in the screening files, then the screening is considered to have failed and the call is released.

Dataword2 (service name) identifies the type of service that is associated with the name.

• Service Name—When screening is triggered by B-number analysis, a service name (such as “800,” “900,” or “FreePhone”) is used to identify which list of calling numbers (A-numbers) is associated with that service. The service name is passed, as read, when the screening request is made.

Note Service names are limited to 10 alphanumeric characters. Spaces are not allowed.

Dataword3 (index to the Dial Plan table if screening passes) and dataword4 (index to the Dial Plan table if screening fails) are added to the SCREENING result type only for the A-digit tree. If the screening passes or fails, re-start with the Pre-analysis after a dial plan changeover. This treatment is similar to the NEW_DIALPLAN result type. If neither dataword3 nor dataword4 is provisioned, no change in functionality occurs.

If SCREENING (A white) and CG_SCREEN_IND (UPVF) are both configured in the result type and SCREENING is passed, the screening indicator is always set to UPVP even if the user tries to overwrite it with the CG_SCREEN_IND result type.

CG_PRES_IND

The CG_PRES_IND result type has dataword1 modified to include an additional value (3). The values of dataword1 are now: Restricted (1), Allowed (2), and Unavailable (3).

PNMODDIG

The PNMODDIG result type modifies the presentation number received on any incoming message. This parameter populates or modifies a specified number of digits from any point in the generic number-ACgPN or Presentation Number in the BTNUP and UK-ISUP protocol variants.

Dataword1 (Application point) indicates the point (digit) in the digit string to begin applying the modification. The range is from 1 through the total number of digits in the digit string (32 maximum). Entering a value of “98” causes the removal of digits to begin at the end of the digit string and move backward.

Dataword2 (Number of digits to remove) indicates the number of digits to remove. The range is from 0 through the number of digits remaining in the digit string from the application point (32 maximum). To remove the entire number, regardless of the number of digits it contains, enter the value “99” for this dataword.

Dataword3 (Modification name) indicates the name of the modification string. If required, this is a name that specifies the digit modification string that is to be inserted beginning at the application point.

PN_NUMBER_TYPE

The PN_NUMBER_TYPE result type is used to modify the number type of the presentation number. The NOA modification field of the presentation number or the generic number will be modified.

Dataword1 value is the internal NOA value. The value range is 0 (default) through 43.

PN_PRES_IND

The PN_PRES_IND result type is the presentation indicator of the presentation number or the generic number is modified with this result type.

Dataword1 is the presentation number indicator value. The value range is 1 through 3.

- 1 - Restricted
- 2 - Allowed
- 3 - Unavailable

CG_SCREEN_IND

The CG_SCREEN_IND result type is the screening indicator of the calling party number is modified with this result type.

Dataword1 is the calling party number screening indicator value. The value range is 1 through 5.

- 1 - NP (Network Provided)
- 2 - UPVP (user provided verified and passed)
- 3 - UPNV (user provided not verified)
- 4 - UPVF (user provided verified and failed)
- 5 - spare1

PN_SCREEN_IND

The PN_SCREEN_IND result type is the screening indicator of the presentation number or the generic number will be modified with this result type.

Dataword1 is the presentation number screening indicator value. The value range is 1 through 5.

- 1 - NP (Network Provided)
- 2 - UPVP (user provided verified and passed)
- 3 - UPNV (user provided not verified)
- 4 - UPVF (user provided verified and failed)
- 5 - spare1

A_NUM_NPI_TYPE

The A_NUM_NPI_TYPE result type is for CgPN; PN (GN-ACgPN) should be mapped from the original. CgPN if it was populated by a swap or if a new provision use a default value (E.164).

Datawrod1 indicates the internal NPI value. The value range is 0 (default) through 10.

CG_PN_COPY

The CG_PN_COPY result type allows automatic filling of the CgPN address with the provisioned network number when the existing address digits are moved to the GN-ACgPN. The associated NOA, NPI, SI, and PI fields are copied from the calling party number to GN-ACgPN. Currently the following associated data is set in Call Context for CgPn: NOA- NAT, SI-Network Provided, and PI- Allowed. If dataword1 is null, then the CgPN is left intact after the existing digits are moved. PN is a historical term, although still used a lot, but the correct term is GN-ACgPN.

Note The TNUP protocol variant only has a PN.

PN_NPI_TYPE

The PN_NPI_TYPE result type is for NPI and PN. The call context for storing A-number screening indication, A-number presentation indication, A-number NPI value, generic number NOA value, generic number screening indication, generic number presentation indication, and CBI_IND for BTNUP and UKISUP protocol variants is updated, based on generic analysis results.

All results are collected and then are processed in a logical order, first checking for any call rejection cases (for example, Analysis failure, Cause, or Blacklist). Then any results that should be processed ahead of the others (for example, screening (no point in processing if this does not pass) or ported

number handling where a number must be prefixed and then passed back in to start analysis again. Then any results, (for example, More-info requests, Test calls, and then finally all other results (ROUTE -Number modifications, and so on) are processed.

Dataword1 is the internal NPI value. The value range is 0 (default) through 10.

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

NOA and NPI Codes

No NOA or NPI codes are added, modified, or deleted for this feature.

For information on other NOA and NPI codes for the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide*.

Advanced Screening and Modification Screening Examples

Advanced Screening and Modification Screening Example (UPVP)

This feature can be used when a call with a CgPn “703-123-4567” ingresses to a PGW 2200. In this example, since CgPn contains “703123” and the call matches an IP address in the dial plan, the PGW 2200 sets SI to UPVP and passes the CgPn on unmodified.

Scenario

A call with a CgPn “703-123-4567” ingresses to a PGW 2200. Since CgPn contains “703123” and the call matches an IP address in the dial plan, PGW 2200 sets SI to UPVP and passes on the CgPn unmodified.

This scenario occurs when you want CallerID terminals to display part of your calling number (such as a building’s main number), but want to keep private your actual number for services, such as 911 ID.

Step 1 User at telephone with CgPn= 703-123-4567 dials your telephone.

Step 2 The H.323 gatekeeper sends the SETUP message to the PGW 2200.

Step 3 The PGW 2200 determines source IP address in the SETUP message.

Step 4 The PGW 2200 selects the dial plan corresponding with the IP address in your company.

Step 5 The PGW 2200 sees that the CgPn (CLI) “703123” prefix screened = valid.

Step 6 The PGW 2200 sets the following:

- SI to UPVP (user provided, verified, and passed)

Step 7 The PGW 2200 sends the IAM to the PSTN with screened CLI.

Step 8 You answer the call.

Advanced Screening and Modification Screening Example (NP)

Scenario

Call with CgPn “703-123-4567” comes into PGW 2200. Since CgPn contains “4567” and the call matches an IP address in the dial plan, PGW 2200 sets SI to NP and passes on the CgPn unmodified.

This scenario could occur if an IP phone is configured incorrectly and could be done to ensure that the an incorrect CgPN is not displayed.

Step 1 User at telephone with CgPn= “703-123-4567” dials your telephone.

Step 2 The H.323 gatekeeper sends the SETUP message to the PGW 2200.

Step 3 The PGW 2200 determines the source IP address in the SETUP message.

Step 4 The PGW 2200 selects the dial plan corresponding with the IP address in your company.

Step 5 The PGW 2200 sees that the CgPn (CLI) “4567” and prefix screened = failed.

Step 6 The PGW 2200 sets the following:

- SI to NP (Network Provided)
- CgPn to 234500

Step 7 The PGW 2200 sends the IAM to the PSTN with screened CLI.

Step 8 You answer the call.

Advanced Screening and Modification Example (Source-Based Routing)

Scenario

The following scenario is typical of a company in which internal company calls can be routed over an IP network by entering only a few digits of the other telephone’s extension, as opposed to the full telephone number.

Step 1 User at telephone with CgPn= “703-123-4567” dials “4568“.

Step 2 CSPS sends SIP INVITE (4568) to the PGW 2200.

Step 3 The PGW 2200 examines message and identifies the source IP address.

Step 4 The PGW 2200 uses source IP address to determine if the dial plan for company Y may be used.

Step 5 Dial plan for company Y on the PGW 2200 adds a prefix of “703-123” to the dialed number.

Step 6 The PGW 2200 selects SIP route for “703-123-4568”.

Step 7 The PGW 2200 sends INVITE to“703-123-4568”.

Step 8 User at telephone with CgPn=“703-123-4568” answers the call.

Untrusted Calls Ingressing to the PGW 2200 Softswitch

When interested filtering an untrusted SIP domain call that ingresses to the PGW 2200 Softswitch, you can configure a dial plan as follows:

- Trust calls in which IP address and calling party number are allowed.
- Trust calls in which IP address is allowed, even if the calling party number is restricted.
- Do not trust calls in which the IP address is restricted, even if the calling party number is allowed.

Overview of Untrusted Call Process

An overview of a sample untrusted call process is listed below:

Step 1 Incoming SIP call ingresses to at the PGW 2200 Softswitch.

Step 2 PGW 2200 Softswitch analyzes the SIP call data and uses a specified dial plan to determine if the call is trusted or not trusted:

If IP address	And Calling Party Number	PGW 2200 Softswitch
Is allowed	Is allowed	Trusts the call.
	Is restricted	Trusts the call.
Is restricted	Is allowed	Does not trust the call.

Step 3 PGW 2200 Softswitch passes the trusted calls with outgoing data created by a dial plan.

Glossary

Table 8 contains definitions of acronyms and technical terms used in this Advanced Screening and Modification feature.

Table 8 Acronyms and Definitions

Term	Description
Call return	Calling Line Identification service that allows users to identify the last call dialed to your telephone. For example, users in the United Kingdom can dial 1471 (or American users dial *69) to find out who made the last call to their telephone.
Caller display	See Calling Line Identification Presentation.
Calling Line Identification Presentation (CLIP)	A supplementary service that shows the caller's identity to telephones that support with Caller ID.

Table 8 Acronyms and Definitions (continued)

Term	Description
Calling Line Identification Restriction (CLIR)	A supplementary service that allows calling users to hid their identity from callers with Caller ID. The CLIR service may operate in the following modes: • **Permanent Mode.** Network automatically invokes CLIR on all calls originated by the calling user. • **Temporary Mode.** Allows the served user to indicate on per call basis whether or not presentation of the served user's calling line identity is allowed. Where CLIR temporary mode is used, a 'Temporary Mode Default' is supplied as a subscription option. This is either: – **Presentation Not Restricted** CLIR is not invoked unless explicitly requested by the caller – **Presentation Restricted** CLIR is always invoked unless explicitly disabled by the caller
Calling Line Identify (CLI)	Calling Line Identity. CLI information is classified the following way: • *Available*: CLI exists and can be passed to the called customer's NTP on the terminating network. • *Unavailable*: CLI does not exist (or the originating network does not support the CLIR service) or interworking has been encountered and the CLI cannot be passed. • *Withheld*: CLI is not for transmission to the called customer's NTP on the terminating network, because the calling customer is directly connected to a network that supports the CLIP service and has invoked CLIR.
Calling Party Number (CgPN)	The Calling Party Number contains the number of the Calling Party, also called the "A Number" or CLI.
CLI Blocking Indicator	The CBI is a parameter in BTNUP that is used like a PI.
CLI display service and related services	the delivery to the customer's NTP of information that allows that customer to gain access to the caller's CLI. This could be in the form of information that is displayed, recorded, interpreted by a database or provided by means of an audio message or by other means.
COL display service and related services	the delivery to the customer's NTP of information that allows that customer to gain access to the COL. This could be in the form of information that is displayed, recorded, interpreted by a database or provided by means of an audio message, or by other means.
COLI	Connect Line Identity

Table 8 Acronyms and Definitions (continued)

Term	Description
Connected Line Identification (COL)	The COL is either a: • *Network Number* that unambiguously identifies the egress port from the public network, or • *Presentation Number* that identifies the NTP to which a subsequent call can be made. COL information is classified the following way: • *Available*: COL exists and can be passed to the called customer's NTP on the terminating network. • *Unavailable*: COL does not exist (or the originating network does not support the COLR service) or interworking has been encountered and the COL cannot be passed. • *Withheld*: COL is not for transmission to the called customer's NTP on the terminating network, because the calling customer is directly connected to a network that supports the COLP service and has invoked COLR.
Customer Group ID	This is an existing parameter in the PGW 2200 (CustGrpID) that is used to select a dial plan.
Default Number (DN)	See Network Provided Number.
GN	Generic Number
Indirect Access Network	A network that provides telecommunication service to an end user via the switched access network of another network operator.
Network Number (NN)	Digits that comprise a E.164 [2] number that identify the ingress or ingress port to the public network. NN identifies the actual network termination from which the call originates/ terminates. A NN may be: • network provided (NP) • user provided verified and passed (UPVP) • user provided not verified (UPNV). However, the use of a UPNV-NN is not permitted.
Network Provided (NP) Number	NP number identifies a Network Terminating Point. A NP number may be a network number or a presentation number. On ISDN calls it is forwarded by the network if there is no special arrangement, and the customer's equipment does not send a number, or the number sent fails screening.
Network Terminating Point (NTP)	Annex A 2(I) of British Telecom's Licence for fixed link terminating networks.
Number Plan Indicator (NPI)	NPI is used to indicate which numbering plan the associated number belongs to.
Originating Network	the network to which the customer who originates the call is directly connected.
Presentation Indicator (PI)	The PI is used to indicate if the associated number should not be presented. Values are: • (1) presentation allowed • (2) presentation restricted • (3) address not available

Table 8 Acronyms and Definitions (continued)

Term	Description
Presentation Number (PN)	The Presentation number is a second CLI that may be provided by the user. The presentation number is displayed instead of the Calling Party Number depending on the availability and screening indicators of both the Calling Party Number and the Presentation Number. Presentation number is also referred to as Presentation CLI. **Note** Not all signaling types may be able to carry both a CLI and Presentation CLI.
Presentation Number (PN)	a number that identifies the *network termination point (NTP)* to which a return or subsequent call can be made. • Presentation Number is used when the network number of the calling or connected customer is not suitable for display. This is important where PABXs have separate incoming and outgoing lines. • Presentation Number is also known as Presentation CLI. • A presentation number may be network provided (NP), user provided verified and passed (UPVP) or user provided not verified (UPNV).
Receiving Network	The network in receipt of a call across any interconnect. The *receiving network* is also a *transit network* or a *terminating network* for that call.
Screening indicator (SI)	The SI indicates the level of screening that has been applied to the associated CLI. Values are: • 1 - User provided, not verified (UPNV): a number that is supplied by a user which identifies a *NTP* and has not been subjected to screening or editing by the network. • 2 - User provided, verified and passed (UPVP): number whose most significant part is network provided and whose least significant part is supplied by a user and successfully checked by the network for length and range, and which identifies a *NTP*. A user provided, verified and passed number may be a network number or a presentation number. • 3 - User provided, verified and failed (UPVF) • 4 - Network provided (NP)
Standard CLI blocking prefix	The prefix generally used (‘141’ in the United Kingdom) to invoke the CLIR service where it is provisioned in Temporary Mode with default ‘**presentation not restricted**.’
Standard CLI unblocking prefix	The prefix generally used (‘1470’ in the United Kingdom) to prevent usage of the CLIR service where it is provisioned in Temporary Mode with default ‘**presentation restricted.**’
Terminating Network	The network to which the customer who receives a call is directly connected.
Transit Network	A network through which a call passes.
UPNV screening indicator	User provided, not verified. See Screening indicator (SI).
UPVF screening indicator	User provided, verified and failed. See Screening indicator (SI).
UPVP screening indicator	User provided, verified and passed. See Screening indicator (SI).

SIP Call Traces

The following SIP call traces are provided:

- Terminating SIP call
- SIP Call Setup and teardown

Note CANCEL is used to terminate a pending session.
BYE is used to terminate an established session.

Terminating SIP Call

```
BYE sip:23198@172.18.192.232:5060 SIP/2.0
Via: SIP/2.0/UDP  172.17.207.91:50494
From: <sip:23198@172.18.192.232>;tag=a73kszlfl
To: <sip:15691@10.80.17.134>;tag=48C5EA10-16DD
Date: Sun, 14 Mar 1993 22:08:50 GMT-5
Call-ID: c2943000-50405d-6af10a-382e3031@10.80.17.134
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6
Route: <sip:15691@10.80.17.134:5060>
Timestamp: 732164935
CSeq: 101 BYE
Content-Length: 0
```

SIP Call Setup and Teardown

```
11:19:38.667282  10.0.0.1:50313 10.0.0.2:5060  SIP.. ->  INVITE sip:4151234567@10.0.0.2 SIP/2.0
                                                         Via: SIP/2.0/UDP 10.0.0.1:5060
                                                         From: "4440000001" <sip:7031234567@10.0.0.2>
                                                         ;tag=003094c3c070004139755cf2-6e02ec80
                                                         To: <sip:4151234567@10.0.0.2>
                                                         Call-ID: Hardware-Address-2@10.0.0.1
                                                         CSeq: 101 INVITE
                                                         User-Agent: Cisco-SIP-IP-Phone/3
                                                         Contact: sip:7031234567@10.0.0.1:5060
                                                         Expires: 180
                                                         Content-Type: application/sdp
                                                         Content-Length: 273
                                                         Accept: application/sdp

                                                         v=0
                                                         o=CiscoSystemsSIP-IPPhone-UserAgent 10147 5278 IN IP4 10.0.0.1
                                                         s=SIP Call
                                                         c=IN IP4 10.0.0.1
                                                         t=0 0
                                                         m=audio 27768 RTP/AVP 0 8 18 101
                                                         a=rtpmap:0 PCMU/8000
                                                         a=rtpmap:8 PCMA/8000
                                                         a=rtpmap:18 G729a/8000
                                                         a=rtpmap:101 telephone-event/8000
                                                         a=fmtp:101 0-15

11:19:38.671607  10.0.0.2:3370  10.0.0.3:5060   SIP.. -> INVITE sip:4151234567@company.com:
                                                         5060 SIP/2.0
                                                         Record-Route: <sip:4151234567@10.0.0.2:5060; maddr=10.0.0.2>
                                                         Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                         Via: SIP/2.0/UDP 10.0.0.1:5060
                                                         From: "4440000001" <sip:7031234567@10.0.0.2>
                                                         ;tag=003094c3c070004139755cf2-6e02ec80
                                                         To: <sip:4151234567@10.0.0.2>
                                                         Call-ID: Hardware-Address-2@10.0.0.1
                                                         CSeq: 101 INVITE
```

```
                                                User-Agent: Cisco-SIP-IP-Phone/3
                                                Contact: sip:7031234567@10.0.0.1:5060
                                                Expires: 180
                                                Content-Type: application/sdp
                                                Content-Length: 273
                                                Accept: application/sdp

                                                v=0
                                                o=CiscoSystemsSIP-IPPhone-UserAgent 10147 5278 IN IP4 10.0.0.1
                                                s=SIP Call
                                                c=IN IP4 10.0.0.1
                                                t=0 0
                                                m=audio 27768 RTP/AVP 0 8 18 101
                                                a=rtpmap:0 PCMU/8000
                                                a=rtpmap:8 PCMA/8000
                                                a=rtpmap:18 G729a/8000
                                                a=rtpmap:101 telephone-event/8000
                                                a=fmtp:101 0-15

11:19:38.740368  10.0.0.3:5060   10.0.0.2:5060  SIP.. -> SIP/2.0 100 Trying
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>
                                                ;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 INVITE
                                                Content-Length: 0


11:19:38.860158  10.0.0.3:5060   10.0.0.2:5060  SIP.. -> SIP/2.0 183 Session Progress
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 INVITE
                                                Contact:  <sip:4151234567@company.com:5060>
                                                Content-Type: application/sdp
                                                Content-Length: 202

                                                v=0
                                                o=- 31 0 IN IP4 172.22.121.99
                                                s=Cisco SDP 0
                                                c=IN IP4 172.22.121.99
                                                t=0 0
                                                m=audio 16938 RTP/AVP 0 101
                                                a=rtpmap:101 telephone-event/8000
                                                a=fmtp:101 0-15
                                                a=X-sqn:0
                                                a=X-cap: 1 image udptl t38

11:19:38.870150  10.0.0.3:5060   10.0.0.2:5060  SIP.. -> SIP/2.0 200 Ok
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>
                                                ;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 INVITE
                                                Contact:  <sip:4151234567@company.com:5060>
                                                Record-Route: <sip:4151234567@10.0.0.2:5060; maddr=10.0.0.2>
                                                Content-Type: application/sdp
                                                Content-Length: 202

                                                v=0
                                                o=- 31 0 IN IP4 172.22.121.99
                                                s=Cisco SDP 0
                                                c=IN IP4 172.22.121.99
                                                t=0 0
                                                m=audio 16938 RTP/AVP 0 101
                                                a=rtpmap:101 telephone-event/8000
                                                a=fmtp:101 0-15
                                                a=X-sqn:0
```

```
                                                a=X-cap: 1 image udptl t38

11:19:39.370264  10.0.0.3:5060   10.0.0.2:5060  SIP.. -> SIP/2.0 200 Ok
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 INVITE
                                                Contact:  <sip:4151234567@company.com:5060>
                                                Record-Route: <sip:4151234567@10.0.0.2:5060;maddr=10.0.0.2>
                                                Content-Type: application/sdp
                                                Content-Length: 202

                                                v=0
                                                o=- 31 0 IN IP4 172.22.121.99
                                                s=Cisco SDP 0
                                                c=IN IP4 172.22.121.99
                                                t=0 0
                                                m=audio 16938 RTP/AVP 0 101
                                                a=rtpmap:101 telephone-event/8000
                                                a=fmtp:101 0-15
                                                a=X-sqn:0
                                                a=X-cap: 1 image udptl t38

11:19:40.380318  10.0.0.3:5060   10.0.0.2:5060  SIP.. -> SIP/2.0 200 Ok
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 INVITE
                                                Contact:  <sip:4151234567@company.com:5060>
                                                Record-Route: <sip:4151234567@10.0.0.2:5060;maddr=10.0.0.2>
                                                Content-Type: application/sdp
                                                Content-Length: 202

                                                v=0
                                                o=- 31 0 IN IP4 172.22.121.99
                                                s=Cisco SDP 0
                                                c=IN IP4 172.22.121.99
                                                t=0 0
                                                m=audio 16938 RTP/AVP 0 101
                                                a=rtpmap:101 telephone-event/8000
                                                a=fmtp:101 0-15
                                                a=X-sqn:0
                                                a=X-cap: 1 image udptl t38

11:19:41.274772  10.0.0.2:3370  10.0.0.3:5060   SIP.. -> ACK sip:4151234567@company.com:5060 SIP/2.0
                                                Record-Route: <sip:4151234567@10.0.0.2:5060;maddr=10.0.0.2>
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 ACK
                                                User-Agent: Cisco-SIP-IP-Phone/3
                                                Content-Length: 0


11:19:41.328689  10.0.0.2:3370  10.0.0.3:5060   SIP.. -> ACK sip:4151234567@company.com:5060 SIP/2.0
                                                Record-Route: <sip:4151234567@10.0.0.2:5060;maddr=10.0.0.2>
                                                Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                Via: SIP/2.0/UDP 10.0.0.1:5060
                                                From: "4440000001" <sip:7031234567@10.0.0.2>
                                                ;tag=003094c3c070004139755cf2-6e02ec80
                                                To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                Call-ID: Hardware-Address-2@10.0.0.1
                                                CSeq: 101 ACK
                                                User-Agent: Cisco-SIP-IP-Phone/3
                                                Content-Length: 0
```

```
11:19:41.412749  10.0.0.2:3370  10.0.0.3:5060   SIP.. -> ACK sip:41512345678@company.com:5060 SIP/2.0
                                                         Record-Route: <sip:4151234567@10.0.0.2:5060; maddr=10.0.0.2>
                                                         Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-1
                                                         Via: SIP/2.0/UDP 10.0.0.1:5060
                                                         From: "4440000001" <sip:7031234567@10.0.0.2>
                                                         ;tag=003094c3c070004139755cf2-6e02ec80
                                                         To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                         Call-ID: Hardware-Address-2@10.0.0.1
                                                         CSeq: 101 ACK
                                                         User-Agent: Cisco-SIP-IP-Phone/3
                                                         Content-Length: 0

11:19:51.116233  10.0.0.2:3371  10.0.0.3:5060   SIP.. -> BYE sip:41512345678@company.com:5060 SIP/2.0
                                                         Record-Route: <sip:4151234567@10.0.0.2:5060; maddr=10.0.0.2>
                                                         Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-3
                                                         Via: SIP/2.0/UDP 10.0.0.1:5060
                                                         From: "4440000001" <sip:7031234567@10.0.0.2>
                                                         ;tag=003094c3c070004139755cf2-6e02ec80
                                                         To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                         Call-ID: Hardware-Address-2@10.0.0.1
                                                         CSeq: 102 BYE
                                                         User-Agent: Cisco-SIP-IP-Phone/3
                                                         Content-Length: 0


11:19:51.170257  10.0.0.3:5060   10.0.0.2:5060  SIP.. -> SIP/2.0 200 Ok
                                                         Via: SIP/2.0/UDP 10.0.0.2:5060;branch=Hardware-Address-3
                                                         Via: SIP/2.0/UDP 10.0.0.1:5060
                                                         From: "4440000001" <sip:7031234567@10.0.0.2>
                                                         ;tag=003094c3c070004139755cf2-6e02ec80
                                                         To: <sip:4151234567@10.0.0.2>;tag=2078917053

                                                         Call-ID: Hardware-Address-2@10.0.0.1
                                                         CSeq: 102 BYE
                                                         Content-Length: 0
```