Separate Calling Party Number and Billing Number in SIP

- External Presentation Name and Number Overview, on page 1
- Call Processing, on page 2
- Directory Number Overview, on page 4
- SIP Profile Overview, on page 8
- SIP Trunk Overview, on page 10
- Intercluster SME Call Flows, on page 15

External Presentation Name and Number Overview

Cisco Unified Communications Manager Administration can be configured to contain separate calling party and presentation number.

In previous releases, Cisco Unified Communications Manager cannot be configured on a per line basis to have a different number sent to the PSTN in the FROM and PAID header. If a group of users is configured to present the same Calling Line Identification Number to PSTN users, which is a nongeographic E.164 number and cannot be used for billing. Therefore, the users actual DDI must be sent in a different field than the presentation number. With this release, Cisco Unified Communications Manager supports External Presentation Name and Number that is different from existing Identification Name and Number. The configured Presentation Name and Number are for display purpose on the following devices:

- SIP
- SCCP
- Single Number Reach Destination (SNRD)
- CTIRD
- SparkRD

Configuration Overview

You can configure the external presentation name and number feature on the following pages:

- Directory Number Configuration

- SIP Profile Configuration
- Trunk Configuration

Note

- When you configure the External Presentation Information on the SIP Profile Configuration page, the value of **External Presentation Number** and **External Presentation Name** on the SIP Profile Configuration page is used, overriding the settings configured on the Directory Number page.
- When you configure the Presentation Information on the Trunk Configuration page, the value of **Presentation Number** and **Presentation Name** on the Trunk Configuration page is used, overriding the settings configured on the SIP Profile Configuration and Directory Number Configuration pages.

Call Processing

This section describes the incoming and outgoing call behavior when you configure the external presentation name and number feature.

Incoming Call Process

Cisco Unified Communications Manager looks for FROM and PAID header information when there is a call initiated from the PSTN network. The FROM header contains the external presentation name and number (if configured). However, this is not the real identity of a user, it is used only for display purpose. The PAID header contains the identity (original DN or DDI) of the user.

If FROM and PAID headers have different numbers and **Enable External Presentation Name and Number** option is enabled in the SIP Profile Configuration page and **Display External Presentation Name and Number** service parameter value is set to **`True`**, then Cisco Unified Communications Manager displays the FROM header information (configured external presentation name and number) on the called device. Similarly, if an option is disabled, Cisco Unified Communications Manager displays PAID header information (user's original DN or DDI) on the called device.

Note

- By default, **Enable External Presentation Name and Number** field is unchecked.
- Default value of a service parameter **Display External Presentation Name and Number** is False.

Invite Received from the PSTN Network

```
From: "Customer Care" <sip:1800000@example.com>;
To: <sip:someone@example.com>
P-Asserted-Identity: "Your personal adviser <sip:user1@example.com>
Remote-Party-ID: "Your personal adviser <sip:user1@example.com>
```

In the preceding example, FROM header contains a number different from the PAID header. If you check **Enable External Presentation Name and Number** check box and set **Display External**

Presentation Name and Number value to **`True`**, Cisco Unified Communications Manager displays **`Customer Care / 1800000`** on the called device.

If you uncheck the **Enable External Presentation Name and Number** check box or set the **Display External Presentation Name and Number** to **`False`**, then Cisco Unified Communications Manager displays **`Your personal adviser / user1@example.com`** on the called device.

Outgoing Call Process

Let us assume, a user configured with External Presentation Name and Number initiates a call to a PSTN network through the SIP trunk with **Enable External Presentation Name and Number** configured in its SIP Profile. Then, Cisco Unified Communications Manager sends the configured External Presentation Information in the FROM header of the outgoing SIP message and displays on the called device.

If **Enable External Presentation Name and Number** option is disabled or **External Presentation Number** and **External Presentation Name** fields are not configured, the Cisco Unified Communications Manager sends the directory number information in the FROM and PAID headers and displays on the called device.

External Presentation Number Mask Operation

Cisco Unified Communications Manager allows you to mask the external presentation number, to be displayed on the called device. You can mask the presentation number on the Directory Number Configuration, SIP Profile Configuration, and Trunk Configuration pages.

When you enter the digits in the **External Presentation Number** field with trailing X, the value of X is replaced with the directory number information starting from right to left.

Mask Operation on Directory Number Configuration

If you mask **External Presentation Number** as 180011XXXX on Directory Number Configuration page for a Directory Number 5551234, then Cisco Unified Communications Manager displays the presentation number as `1800111234` on the called device.

Mask Operation on SIP Profile Configuration

Let us assume **External Presentation Number** on Directory Number page is 180011XXXX and if you mask **External Presentation Number** on SIP Profile Configuration page as 180022XXXX for a Directory Number 5551234, then Cisco Unified Communications Manager displays the presentation number as `1800221234` on the called device.

Mask Operation on Trunk Configuration

Let us assume **External Presentation Number** on Directory Number page is 180011XXXX and on SIP Profile Configuration page is 180022XXXX. If you mask **Presentation Number** on Trunk Configuration page as 180033XXXX for a Directory Number 5551234, then Cisco Unified Communications Manager displays the presentation number as `1800331234` on the called device.

Directory Number Overview

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Directory Number** menu path to configure Directory Numbers (DNs). Using Cisco Unified Communications Manager Administration, you can configure and modify the DNs that are assigned to specific phones.

A new section **External Presentation Information** is added on the Directory Number Configuration page. The administrator can now configure the presentation name and number of their choice to display on the supported devices for external calls. If an administrator does not want to show users' identity, they have a privilege to display configured **External Presentation Number** and **External Presentation Name** as Anonymous on the called party device.

Directory Number Configuration Tasks

Procedure

	Command or Action	Purpose
Step 1	Add a new end user using one of the following methods: • Import an End User from LDAP, on page 4 • Add an End User Manually, on page 5	If your system is synchronized with a company LDAP directory, you can import the new end user directly from LDAP. Otherwise, you can add and configure the end user manually.
Step 2	Assign a phone to new or existing end user by performing one of the following tasks: • Add New Phone for End User , on page 6 • Move an Existing Phone to a End User, on page 7	You can use the 'Add New Phone' procedure to configure a new phone for the end user using settings from a universal device template. You can also use the 'Move' procedure to assign an existing phone already configured or pre-configured.
Step 3	Configure External Presentation Information on DN, on page 7	To configure the external presentation number and external presentaion name for DNs that are assigned to specific phones.

Import an End User from LDAP

Perform the following procedure to manually import a new end user from a company LDAP directory. If your LDAP synchronization configuration includes a feature group template with a user profile that includes universal line and device templates and a DN pool, the import process automatically configures the end user and primary extension.

Note You cannot add new configurations (for example, adding a feature group template) into an LDAP directory sync after the initial sync has occurred. If you want to edit an existing LDAP sync, you must either use Bulk Administration, or configure a new LDAP sync.

Before you begin

Before you begin this procedure make sure that you have already synchronized Cisco Unified Communications Manager with a company LDAP directory. The LDAP synchronization must include a feature group template with universal line and device templates.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select the LDAP directory to which the user is added.

Step 3 Click **Perform Full Sync**.
Cisco Unified Communications Manager synchronizes with the external LDAP directory. Any new end users in the LDAP directory are imported into the Cisco Unified Communications Manager database.

What to do next

If the user is enabled for self-provisioning, the end user can use the Self-Provisioning Interactive Voice Response (IVR) to provision a new phone. Otherwise, perform one of the following tasks to assign a phone to the end user:

- Add New Phone for End User , on page 6
- Move an Existing Phone to a End User, on page 7

Add an End User Manually

Perform the following procedure to add new end user and configure them with an access control group and a primary line extension.

Note Make sure that you have already set up an access control groups that has the role permissions to which you want to assign your user. For details, see the "Manage User Access" chapter.

Before you begin

Verify that you have a user profile configured that includes a universal line template. If you need to configure a new extension, Cisco Unified Communications Manager uses the settings from the universal line template to configure the primary extension.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick User/Phone Add**.

Step 2 Enter the **User ID** and **Last Name**.

Step 3 From the **Feature Group Template** drop-down list, select a feature group template.

Step 4 Click **Save**.

Step 5 From the **User Profile** drop-down list, verify that the selected user profile includes a universal line template.

Step 6 From the **Access Control Group Membership** section, click the + icon.

Step 7 From the **User is a member of** drop-down list, select an access control group.

Step 8 Under **Primary Extension**, click the + icon.

Step 9 From the **Extension** drop-down list, select a DN that displays as **(available)**.

Step 10 If all line extensions display as **(used)**, perform the following steps:

a) Click the **New...** button.
The **Add New Extension** popup displays.
b) In the **Directory Number** field, enter a new line extension.
c) From the **Line Template** drop-down list, select a universal line template.
d) Click **OK**.
Cisco Unified Communications Manager configures the directory number with the settings from the universal line template.

Step 11 (Optional) Complete any additional fields in the **Quick User/Phone Add Configuration** window.

Step 12 Click **Save**.

What to do next

Perform one of the following procedures to assign a phone to this end user:

- Add New Phone for End User , on page 6
- Move an Existing Phone to a End User, on page 7

Add New Phone for End User

Perform the following procedure to add a new phone for a new or existing end user. Make sure that the user profile for the end user includes a universal device template. Cisco Unified Communications Manager uses the universal device template settings to configure the phone.

Before you begin

Perform one of the following procedures to add an end user:

- Add an End User Manually, on page 5
- Import an End User from LDAP, on page 4

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the end user for whom you want to add a new phone.

Step 3 Click the **Manage Devices**.
The Manage Devices window appears.

Step 4 Click **Add New Phone**.
The Add Phone to User popup displays.

Step 5 From the **Product Type** drop-down list, select the phone model.

Step 6 From the **Device Protocol** drop-down list select SIP or SCCP as the protocol.

Step 7 In the **Device Name** text box, enter the device MAC address.

Step 8 From the **Universal Device Template** drop-down list, select a universal device template.

Step 9 If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10 If you want to use Extension Mobility to access the phone, check the **In Extension Mobility** check box.

Step 11 Click **Add Phone**.
The Add New Phone popup closes. Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12 If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the **Phone Configuration** window.

Move an Existing Phone to a End User

Perform this procedure to move an existing phone to a new or existing end user.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the user to whom you want to move an existing phone.

Step 3 Click the **Manage Devices** button.

Step 4 Click the **Find a Phone to Move To This User** button.

Step 5 Select the phone that you want to move to this user.

Step 6 Click **Move Selected**.

Configure External Presentation Information on DN

Perform the following procedure to configure the external presentation information for DNs that are assigned to specific phones.

Before you begin

- Check the **Enable External Presentation Name and Number** check box on the SIP Profile Configuration page.
- Perform one of the following procedures to add an end user:
  - Add an End User Manually, on page 5
  - Import an End User from LDAP, on page 4
- Assign a phone to a new or existing end user by performing one of the following tasks:

- Add New Phone for End User , on page 6
- Move an Existing Phone to a End User, on page 7

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 From the **Find and List Directory Numbers** page, perform one of the following steps:

- To update a DN, click **Find** and select the Directory Number for which you want to display unique identity.
- To create a new Directory Number, click **Add New**.

Step 3 In the **External Presentation Information** section, enter the name and number that you want to display on the called device.

Note
- **External Presentation Number** field accepts up to 32 digits and can contain the following characters: [0-9, X, *, #, \, +].
- **External Presentation Name** field accepts up to 50 characters.

Step 4 (Optional), if you want to show configured **External Presentation Number** and **External Presentation Name** as anonymous, check the **Anonymous External Presentation** check box.

Note
- By default, the **Anonymous External Presentation** field is unchecked.
- If you check the **Anonymous External Presentation** field:

  External Presentation Number and **External Presentation Name** fields are noneditable. Also, the entries from these fields disappear.

Step 5 Complete the remaining fields on the **Directory Number Configuration** page. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

SIP Profile Overview

A SIP profile is a template that comprises common SIP settings. You must assign a SIP profile for every SIP trunk and SIP device in your network. When you configure a SIP profile and then assign that profile to a SIP trunk, or a SIP device, the system applies the configured SIP settings to that trunk or device.

SIP Profile Configuration Tasks

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profiles, on page 9	Use this procedure to configure a SIP profile.
Step 2	Configure External Presentation Information on SIP Profile, on page 9	To configure the external presentation number and external presentation name for a SIP profile.

Configure SIP Profiles

Use this procedure to configure a SIP profile with common SIP settings that you can assign to SIP devices and trunks that use this profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Perform one of the following steps:

- Click **Find** and select the SIP profile to edit an existing profile, .
- Click **Add New** to create a new profile.

Step 3 If you want your SIP phones and trunks to support IPv4 and IPv6 stacks, check the **Enable ANAT** check box.

Step 4 If you want to assign an SDP transparency profile to resolve SDP interoperability, from the **SDP Transparency Profile** drop-down list.

Step 5 If you want to assign a normalization or transparency script to resolve SIP interoperability issues, from the **Normalization Script** drop-down list, select the script.

Step 6 (Optional) Check the **Send ILS Learned Destination Route String** check box for Global Dial Plan Replication deployments where you may need to route calls across a Cisco Unified Border Element.

Step 7 Complete the remaining fields in the **SIP Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

Configure External Presentation Information on SIP Profile

Use this procedure to configure the separate external presentation name and number on SIP Profile Configuration page.

Before you begin

- Check the **Enable External Presentation Name and Number** check box on the **SIP Profile Configuration** page.
- Set **Display External Presentation Name and Number** parameter value to `True` under Clusterwide Parameters (Device-Phone) section on **Service Parameter Configuration** page.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Perform one of the following steps:

- To edit an existing profile, click **Find** and select the SIP profile.
- To create a new profile, click **Add New**.

Step 3 In the **External Presentation Information** section, enter the name and number that you want to display on the called device.

Note

- **External Presentation Number** field accepts up to 32 digits and can contain the following characters: [0-9, X, *, #, \, +].
- **External Presentation Name** field accepts a maximum of 50 characters.

Step 4 (Optional), if you want to show configured **External Presentation Number** and **External Presentation Name** as anonymous, check the **Anonymous External Presentation** check box.

Note

- By default, the **Anonymous External Presentation** field is unchecked.
- If you check the **Anonymous External Presentation** field:

  External Presentation Number and **External Presentation Name** fields are noneditable. Also, the entries from these fields disappear.

Step 5 Complete the remaining fields in the **SIP Profile Configuration** page. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

SIP Trunk Overview

If you are deploying SIP for call control signaling, configure SIP trunks that connect Cisco Unified Communications Manager to external devices such as SIP gateways, SIP Proxy Servers, Unified Communications applications, remote clusters, or a Session Management Edition.

Within the Cisco Unified CM Administration, the SIP Trunk Configuration window contains the SIP signaling configurations that Cisco Unified Communications Manager uses to manage SIP calls.

SIP Trunk supports the separate presentation name and number that is different from existing Caller ID DN and Caller Name. A new check box **Anonymous Presentation** is provided to show the configured presentation name and number as Anonymous on the called device.

Trunk Configuration Tasks

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Trunk Security Profile, on page 11	Configure SIP trunk security profiles with any security settings that you want to apply to your SIP trunks. For example, you can configure digest authentication, device security mode, and TLS encryption for SIP signaling. If you don't configure SIP trunk security profiles, by default, Cisco Unified Communications Manager applies a nonsecure sip trunk security profile.
Step 2	Configure Common Device Configuration, on page 12	Set up a Common Device Configuration for the trunk. For dual-stack trunks, configure the IP addressing preference.
Step 3	Configure SIP Trunks, on page 13	Configure the SIP trunks in your network. In the **Trunk Configuration** window, configure the SIP settings for your trunks. Assign a SIP profile, SIP trunk security profile, and a Common Device Configuration to your SIP trunk. In addition, assign any SIP normalization or transparency scripts that your trunk connection requires. For example, if your SIP trunk connects to a Cisco TelePresence VCS, you must assign the *vcs-interop* script to the SIP trunk.
Step 4	Configure Presentation Information on SIP Trunks, on page 14	To configure the presentation name and number on SIP Trunk page.

Configure SIP Trunk Security Profile

Configure a SIP Trunk Security Profile with security settings such as digest authentication or TLS signaling encryption. When you assign the profile to a SIP trunk, the trunk takes on the settings of the security profile.

Note If you don't assign a SIP trunk security profile to your SIP trunks, Cisco Unified Communications Manager assigns a nonsecure profile by default.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Click **Add New**.

Step 3 To enable SIP signaling encryption with TLS, perform the following:

a) From the **Device Security Mode** drop-down list, select **Encrypted**.
b) From the **Incoming Transport Type** and **Outgoing Transport Type** drop-down lists, choose **TLS**.
c) For device authentication, in the **X.509 Subject Name** field, enter the subject name of the X.509 certificate.
d) In the **Incoming Port** field, enter the port on which you want to receive TLS requests. The default for TLS is 5061.

Step 4 To enable digest authentication, do the following

a) Check the **Enable Digest Authentication** check box
b) Enter a **Nonce Validity Timer** value to indicate the number of seconds that must pass before the system generates a new nonce. The default is 600 (10 minutes).
c) To enable digest authentication for applications, check the **Enable Application Level Authorization** check box.

Step 5 Complete the additional fields in the **SIP Trunk Security Profile Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Note
You must assign the profile to a trunk in the **Trunk Configuration** window so that the trunk can uses the settings.

Configure Common Device Configuration

A common device configuration comprises a set of optional set of user-specific feature attributes. If you are deploying IPv6, you can use this configuration to assign IPv6 preferences for SIP trunks or SCCP phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Click **Add New**.

Step 3 For SIP trunks, SIP Phones or SCCP phones, choose a value for the **IP Addressing Mode** drop-down list:

- **IPv4 Only**—The device uses only an IPv4 address for media and signaling.
- **IPv6 Only**—The device uses only an IPv6 address for media and signaling.
- **IPv4 and IPv6 (Default)**—The device is a dual-stack device and uses whichever IP address type is available. If both IP address types are configured on the device, for signaling the device uses the **IP Addressing Mode Preference for Signaling** setting and for media the device uses the **IP Addressing Mode Preference for Media** enterprise parameter setting.

Step 4 If you configure IPv6 in your previous step, then configure an IP addressing preference for the **IP Addressing Mode for Signaling** drop-down list:

- **IPv4**—The dual stack device prefers IPv4 address for signaling.
- **IPv6**—The dual stack device prefers IPv6 address for signaling.
- **Use System Default**—The device uses the setting for the **IP Addressing Mode Preference for Signaling** enterprise parameter.

Step 5 Configure the remaining fields in the **Common Device Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Configure SIP Trunks

Use this procedure to configure a SIP trunk. You can assign up to 16 destination addresses for a SIP trunk.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list, choose **SIP Trunk**.

Step 4 From the **Protocol Type** drop-down list, choose the type of SIP trunk that matches your deployment and click **Next**:

- **None (Default)**
- **Call Control Discovery**
- **Extension Mobility Cross Cluster**
- **Cisco Intercompany Media Engine**
- **IP Multimedia System Service Control**

Step 5 (Optional) If you want to apply a **Common Device Configuration** to this trunk, select the configuration from the drop-down list.

Step 6 Check the **SRTP Allowed** check box if you want to allow encypted media over the trunk.

Step 7 Check the **Run on All Active Unified CM Nodes** check box if you want to enable the trunk for all cluster nodes.

Step 8 Configure the destination address for the SIP trunk:

a) In the **Destination Address** text box, enter an IPv4 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.

b) If the trunk is a dual stack trunk, in the **Destination Address IPv6** text box, enter an IPv6 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.

c) If the destination is a DNS SRV record, check the **Destination Address is an SRV** check box.

d) To add additional destinations, click the **(+)**.

Step 9 From the **SIP Trunk Security Profile** drop-down, assign a security profile. If you don't select this option, a nonsecure profile will be assigned.

Step 10 From the **SIP Profile** drop-down list, assign a SIP profile.

Step 11 (Optional) If you want to assign a normalization script to this SIP trunk, from the **Normalization Script** drop-down list, select the script that you want to assign.

Step 12 Configure any additional fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 13 Click **Save**.

Configure Presentation Information on SIP Trunks

Use this procedure to configure the presentation name and number on SIP Trunk page.

Before you begin

- Check the **Enable External Presentation Name and Number** check box on the SIP Profile Configuration page.
- Configure SIP Trunks, on page 13

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list, choose SIP Trunk.

Step 4 From the **Trunk Service Type** drop-down list, choose the type of SIP trunk that you want to configure:

- **None (Default):** The trunk will not be used for Call Control Discovery, Extension Mobility Cross-Cluster, Intercompany Media Engine, or IP Multimedia System Service Control.
- **Call Control Discovery:** The trunk supports the Call Control Discovery feature.
- **Extension Mobility Cross Cluster:** The trunk supports Extension Mobility Cross Cluster.
- **Cisco Intercompany Media Engine:** The trunk supports the Intercompany Media Engine (IME). Make sure that the IME server is installed before you configure this type of trunk.
- **IP Multimedia System Service Control:** Choose this option to enable the trunk with support for IP Multimedia System Service Control.

Step 5 Click **Next**.

Step 6 In the **Presentation Information** section, enter the name and number that you want to display on the called device.

Note

- **Presentation Number** field accepts up to 32 digits and can contain the following characters: [0-9, X, *, #, \, +].
- **Presentation Name** field accepts a maximum of 50 characters.

Step 7 (Optional) If you want to show the presentation name and number as anonymous, check the **Anonymous Presentation** check box.

Note

- By default, the **Anonymous Presentation** field is unchecked.
- If you check the Anonymous External Presentation field:

  Presentation Number and **Presentation Name** fields are noneditable. Also, the entries from these fields disappear.

Step 8 (Optional) Check the **Send Presentation Name and Number only in the FROM header and not in the other identity headers** check box, if you want to send presentation information that is configured on the SIP Trunk only to FROM header.

Step 9 Configure any additional fields in the **Trunk Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 10 Click **Save**.

Intercluster SME Call Flows

The Cisco Unified Communications Manager Session Management Edition software is same as the Cisco Unified Communications Manager used mainly for a call routing between clusters or various devices. With this release, Cisco Unified Communications Manager supports the intercluster SME calls.

Incoming Calls

Let us assume a user from a PSTN network initiates a call with **Enable External Presentation Name and Number** enabled in its SIP profile. If **Display External Presentation Name and Number** service parameter is set to **`True`**, then Cisco Unified Communications Manager sends the presentation number information to the X-Cisco-Presentation header and displays on the called device. The FROM and PAID headers contains the identity of the user that is the user's DN or DDI.

If **Display External Presentation Name and Number** service parameter is set to **`False`**, then Cisco Unified Communications Manager sends the presentation number information to the X-Cisco-Presentation header. The FROM and PAID headers contains the user’s DN or DDI and displays on the called device.

Outgoing Calls

A user who is configured with **External Presentation Name** and **External Presentation Number** initiates a call to a PSTN network through intercluster SIP trunks. If **Enable External Presentation Name and Number** check box is disabled in its SIP profile, then, Cisco Unified Communications Manager sends the original directory number information in the FROM and PAID headers and displays on the called device and configured External Presentation Information in the X-Cisco-Presentation header. Similarly, if **Enable External Presentation Name and Number** check box is enabled in its SIP profile, Cisco Unified Communications Manager sends the configured External Presentation Information in the FROM header and displays on the called device and original Directory Number in the PAID header.