Application Notes for Configuring SIP Trunking Using Cisco Unified Communications Manger Release 9.1 or 8.6 with Avaya Session Border Controller for Enterprise Release 6.2 and Verizon Business SIP – Issue 1.0

Abstract

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between Cisco Unified Communications Manager and the Verizon Business IP. In the sample configuration, the Cisco Unified Communications Manager solution consists of a sole publisher/subscriber, Cisco Unity 7.0, and Cisco SIP endpoints.

The Verizon Business SIP offer referenced within these Application Notes enables a business to send and receive calls via standards-based SIP trunks, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Cisco Unified Communications Manager with Avaya Session Border Controller for Enterprise Release 6.2 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

Information in these Application Notes has been obtained through Tekvizion labs interoperability testing and additional technical discussions. Testing was conducted in the Tekvizion Test Lab, utilizing a Verizon Business SIP Trunk test service as a test SIP trunk.

 7/15/2013

Table of Contents

1. Introduction

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between Verizon Business SIP Trunking Service and Cisco Unified Communications Manager solution. In the sample configuration, the Cisco Unified Communications Manager solution consists of a sole publisher/subscriber, Cisco Unity 7.0, and Cisco SIP endpoints.

Cisco Unified Communications Manager with Avaya Session Border Controller for Enterprise Release 6.2 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

In the sample configuration, An Avaya Session Border Controller for Enterprise (SBCE) is used as an edge device between the Cisco Unified Communications Manager and Verizon business. Verizon Business SIP trunk is a sample test trunk used in this testing, while any SIP trunk can be deployed in the same mode as per the field deployment. The Avaya SBCE performs SIP header manipulation and provides topology hiding.

Customers using Cisco Unified Communications Manager with the Verizon Business SIP Trunk service are able to send and receive PSTN via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The Cisco Unified Communications Manager location was connected to the Verizon Business SIP test service, as depicted in **Figure 1**. The Avaya SBCE and Cisco Unified Communications Manager were configured to use the Verizon SIP test trunk. This allowed Cisco Unified Communications Manager to receive and send calls from the PSTN via the SIP protocol.

2.1. Interoperability Testing

The testing included executing the test cases detailed in Reference [VZ-Test-Plan], which contains the Verizon SIP Interoperability Lab Test Plan. To summarize, the testing included the following successful SIP trunk interoperability testing:

- SIP OPTIONS monitoring of the health of the SIP trunk was not verified.
- Proper recovery from induced failure conditions such as Cisco Unified Communications Manager reboots, and IP network outages between Verizon and Cisco Unified Communications Manager, of short and long durations.
- Incoming calls from the PSTN were routed to the numbers assigned by Verizon Business to the Cisco Unified Communications Manager location. These incoming calls arrived via the SIP Line configured in Section 5.4 and were answered by Cisco SIP telephones and Cisco Unity voicemail.

- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a call before the Cisco Unified Communications Manager party has answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a number directed to a busy Cisco Unified Communications Manager user, a Cisco Unified Communications Manager user, or an Cisco Unified Communications Manager user that is logged out (i.e., assuming no redirection is configured for these conditions). Proper termination of an inbound call left in a ringing state for a relatively long duration.
- The display of caller ID on display-equipped Cisco Unified Communications Manager telephones was verified. The Cisco Unified Communications Manager capability to use the caller ID received from Verizon to look up and display a name from a configurable directory was also exercised successfully.
- Privacy requests for inbound calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67), the inbound call can be successfully completed to an Cisco Unified Communications Manager telephone user while presenting a "WITHHELD" or anonymous display to an Cisco Unified Communications Manager user (i.e., rather than the caller's telephone number).
- Inbound long holding time call stability.
- Cisco Unified Communications Manager complies with RFC 3261 SIP Methods.
- Cisco Unified Communications Manager can use UDP for SIP transport with Verizon Business.
- Cisco Unified Communications Manager can use a configured UDP or TCP port for SIP signaling with Verizon Business.
- Cisco Unified Communications Manager accepts the full SIP headers sent by Verizon Business.
- Cisco Unified Communications Manager sends SIP 180 RINGING (no SDP in 180) for inbound calls and ring back tone is heard by the caller.
- Cisco Unified Communications Manager does not return a SIP 302 to Verizon.
- Telephony features such as hold and resume, transfer of calls to other Cisco Unified Communications Manager users, and conference calls.
- Incoming voice calls using the G.729(a) and G.711 ULAW codecs, and proper protocol procedures related to media.
- DTMF transmission using RFC 2833. Successful Cisco Unity menu navigation for incoming calls.
- Outgoing calls from the Cisco Unified Communications Manager location to the PSTN were routed via a SIP Line to the Verizon Business SIP Trunk test service. The display of caller ID on display-equipped PSTN telephones was verified. In the context of inbound calls using Verizon SIP trunk test service, inbound calls arriving via the SIP Line configured in Section 5.4 could be forwarded to the Verizon SIP Trunk test Service.

- Call Forwarding of Verizon calls to PSTN destinations via the Verizon SIP Trunk service documented in reference, presenting true calling party information to the PSTN phone. See Section 2.2 for additional information.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. The following observations may be noteworthy:

1. Cisco Unified communications does not have analog phone ports. This limitation prevented the testing of Fax calls. Fax testing requires a separate piece of hardware. IADs or Media Gateways can be used.

2. Although the Verizon Business SIP trunking test service supports transfer using the SIP REFER method. Cisco Unified Communications Manager does not support sending REFER, Cisco Unified Communications Manager did not send REFER to Verizon in the verified configuration.

3. During interoperability testing, one Avaya SBCE was used to support Verizon SIP trunk test service for inbound and outbound calls. One SIP Trunk was created on Cisco Unified Communications Manager to connect the Avaya SBCE.

4. The SIP protocol allows sessions to be refreshed for calls that remain active for some time. In the tested configuration, Cisco Unified Communications Manager send SIP re-INVITE messages to refresh a session. In the tested configuration, this is transparent to the users that are party to the call in that the media paths remain established.

5. Proper DiffServ markings for Avaya SBCE SIP signaling and RTP media were not tested. The QOS markings are not propagated by our Internet Service Provider.

6. IP address and port were used instead of FQDNs. DNS SRV resolution was not tested.

2.3. Support

2.3.1. Avaya

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

2.3.2. Verizon

For technical support on Verizon Business SIP Trunking service, visit online support at http://www.verizonbusiness.com/us/customer/

3. Reference Configuration

Figure 1 illustrates an example Cisco Unified Communications Manager solution connected to the Verizon Business SIP Trunk test service. The Cisco equipment is located on a private IP subnet. An enterprise edge router provides access to the Verizon Business network via a Verizon VPN. This VPN is provisioned for the Verizon Business SIP Trunk test service between the enterprise edge and Service provider.

In the sample configuration, the Avaya SBCE receives traffic from the Verizon Business SIP trunking test service on port 5060 and sends traffic to port 5072, using UDP for network transport, as required by the Verizon Business SIP Trunk test service. The Avaya SBCE in turn sends and receives traffic to and from Cisco Unified Communications Manager using UDP port or TCP port 5060. Verizon provided two numbers associated with the SIP Trunk test service. These numbers were mapped to Cisco Unified Communications Manager directory numbers.

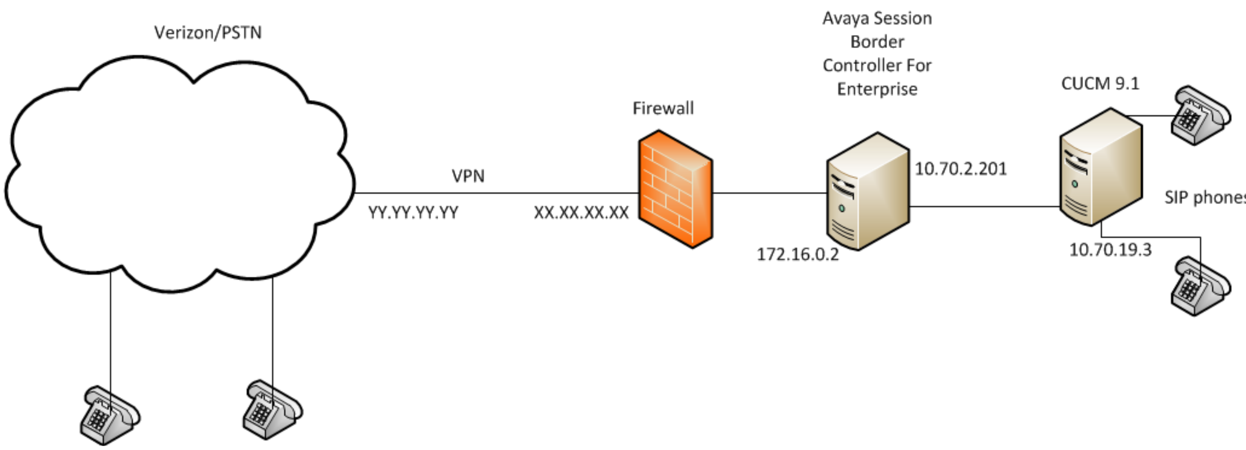


Figure 1: Cisco Unified Communications Manager with Verizon SIP Trunking Service.

Note: Firewall and VPN connectivity between Service Provider and the Enterprise edge (in this case Test Lab environment) are optional components and can be setup based on the network planning requirements of the customer.

4. Equipment and Software Validated

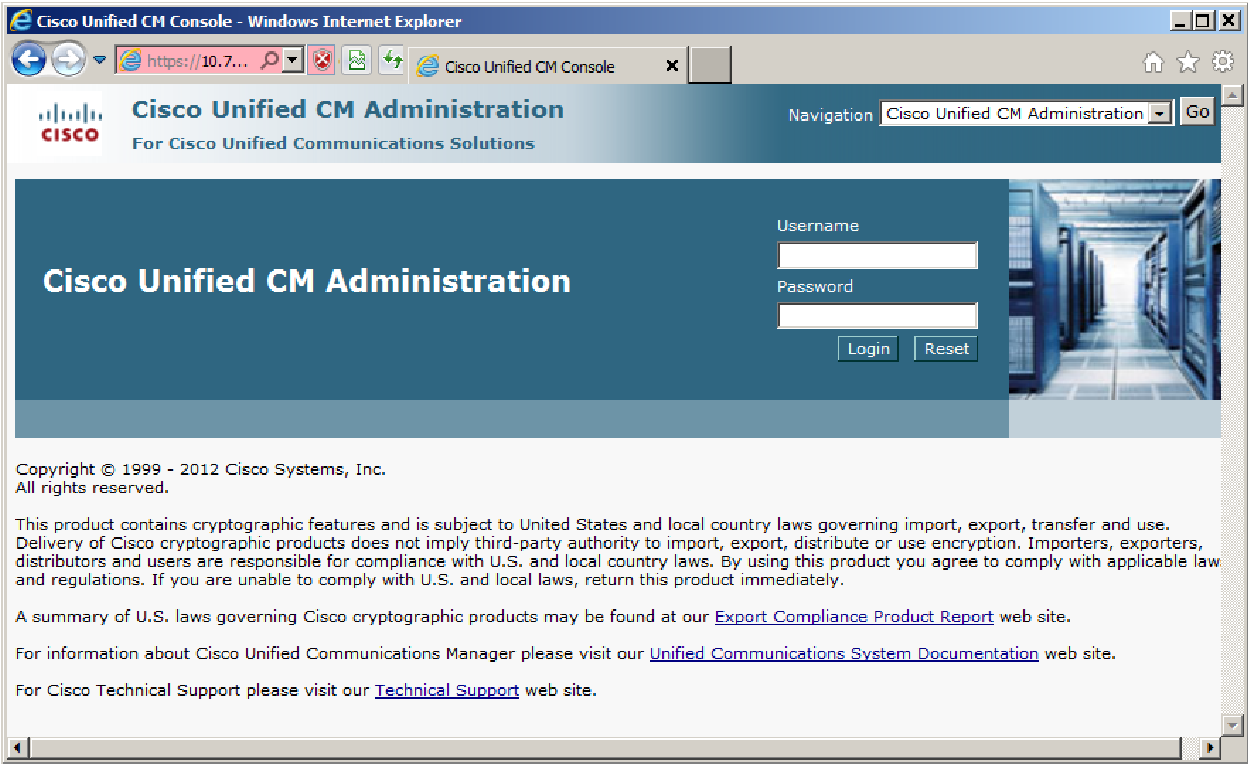
Table 1 shows the equipment and software used in the sample configuration.

Equipment	Software
Avaya Session Border Controller for Enterprise	Release 6.2
Cisco Unified Communications Manager	Release 9.1/8.6
Cisco SIP phones 7961	SIP41.9-3-1SR1-1S
Cisco SIP phones 7942	SIP42.9-3-1SR1-1S

Table 1: Equipment and Software Tested

5. Cisco Unified Communications Manager Configuration

Cisco Unified Communications Manager is configured via http://<IP address or FQDN>/ccmadmin. For more information on Cisco Unified Communications Manager
Manager, consult reference [2]. From the Cisco Unified Communications Manager admin web page, make sure that "Cisco Unified CM administration**"** is selected in **Navigation** that is in the upper right box.
Enter the **username** and **password** ant the Click the **Login** button.



Note: Most of the screenshots are taken from CUCM 9.1 testing while appropriate configurations needs to be configured with CUCM 8.6.

5.1. Physical Network

The Cisco Unified Communications Manager network configuration is typically done during installation. Consult reference [1] for more information on the topics in this section.

5.2. Licensing

On Cisco Unified Communications Manager Release 9.1, a new implementation for licensing was put in place. Now, a Licensing Manager is required and may be an external entity. Consult reference [3] for more information about generating and installing licenses.

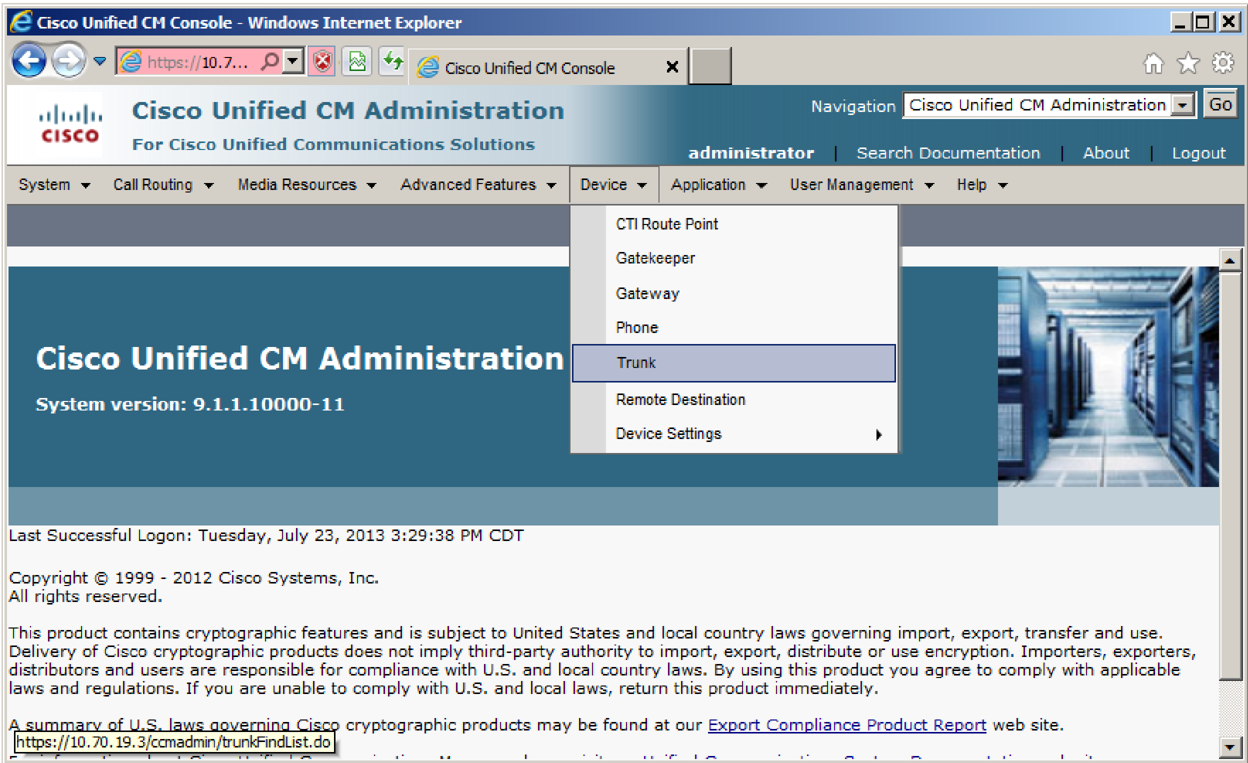
5.3. System Settings

This section illustrates the configuration of system settings. The settings presented here simply illustrate the sample configuration and are not intended to be prescriptive. Make sure that installation instructions in reference [1] were followed and the servers are ready to be configured. Default values were used as possible to provision information.

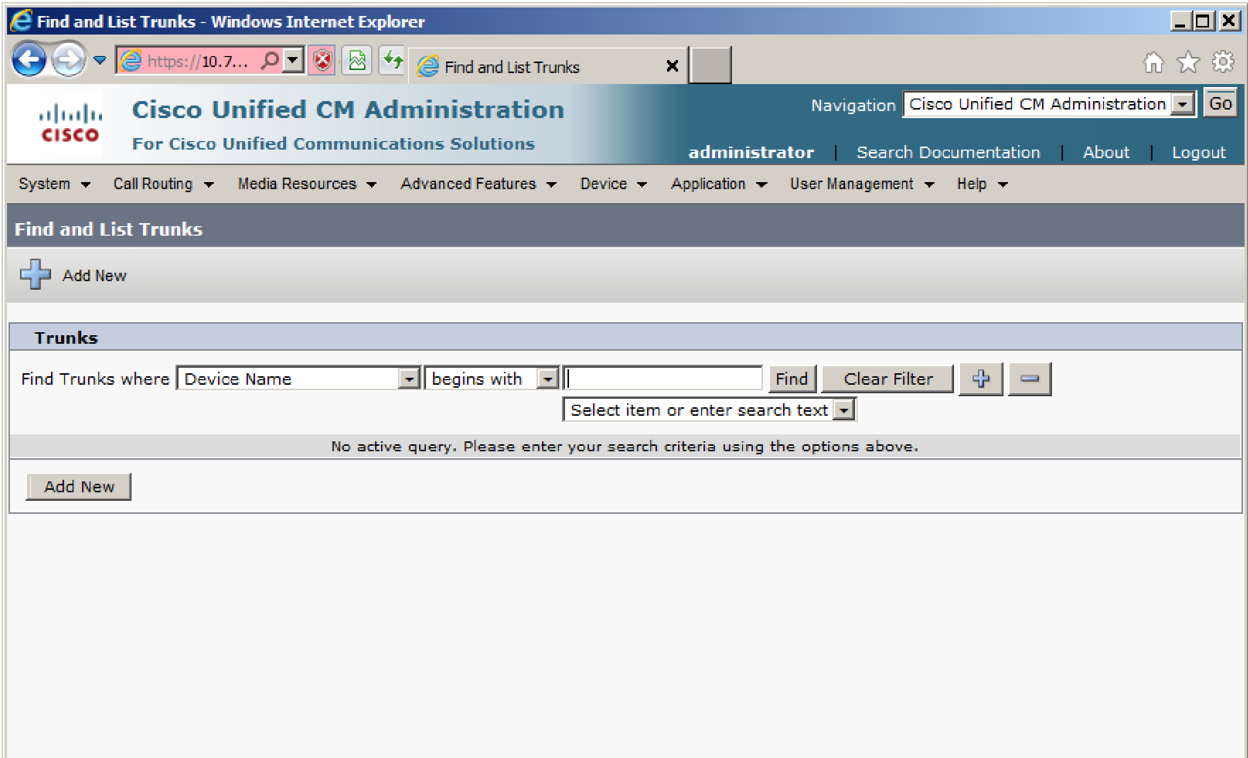
There are only 2 elements required to be created to communicate with Avaya Session Border Controller for Enterprise.

5.3.1. SIP Trunk

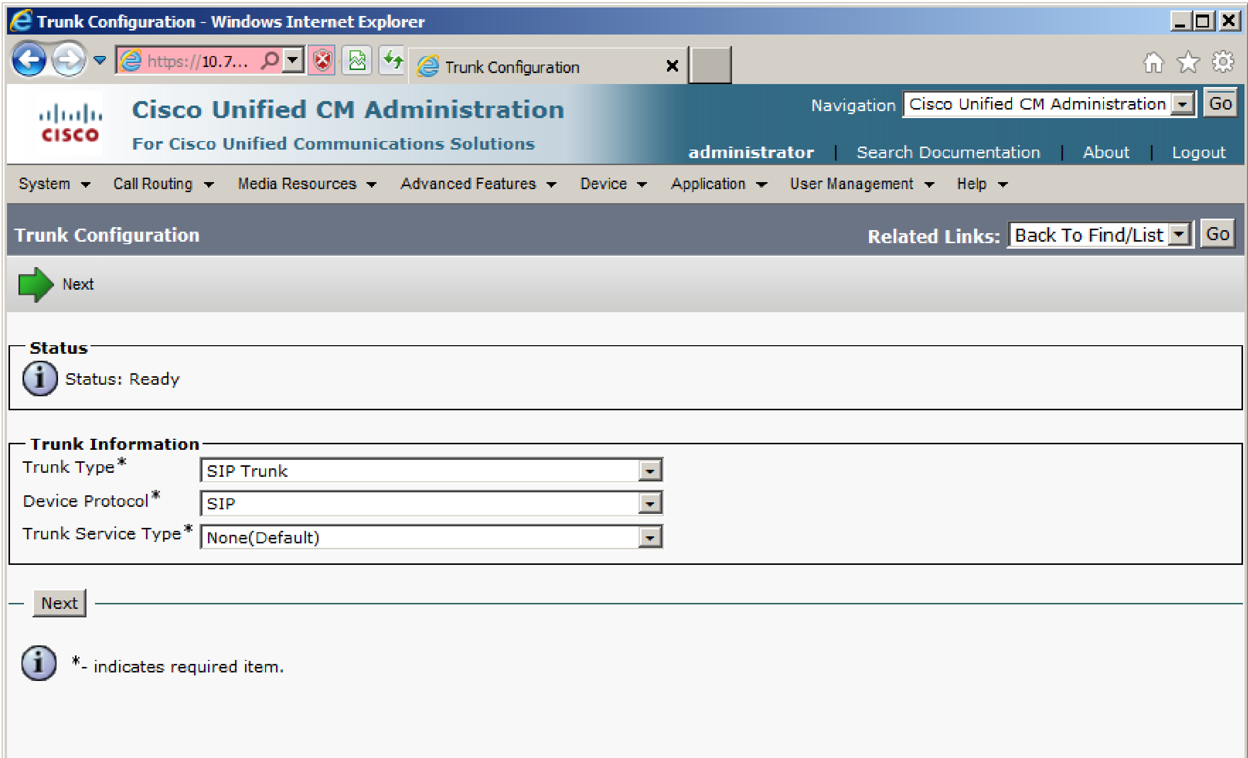
To configure a SIP trunk from the **Device** Menu Select **Trunk**.



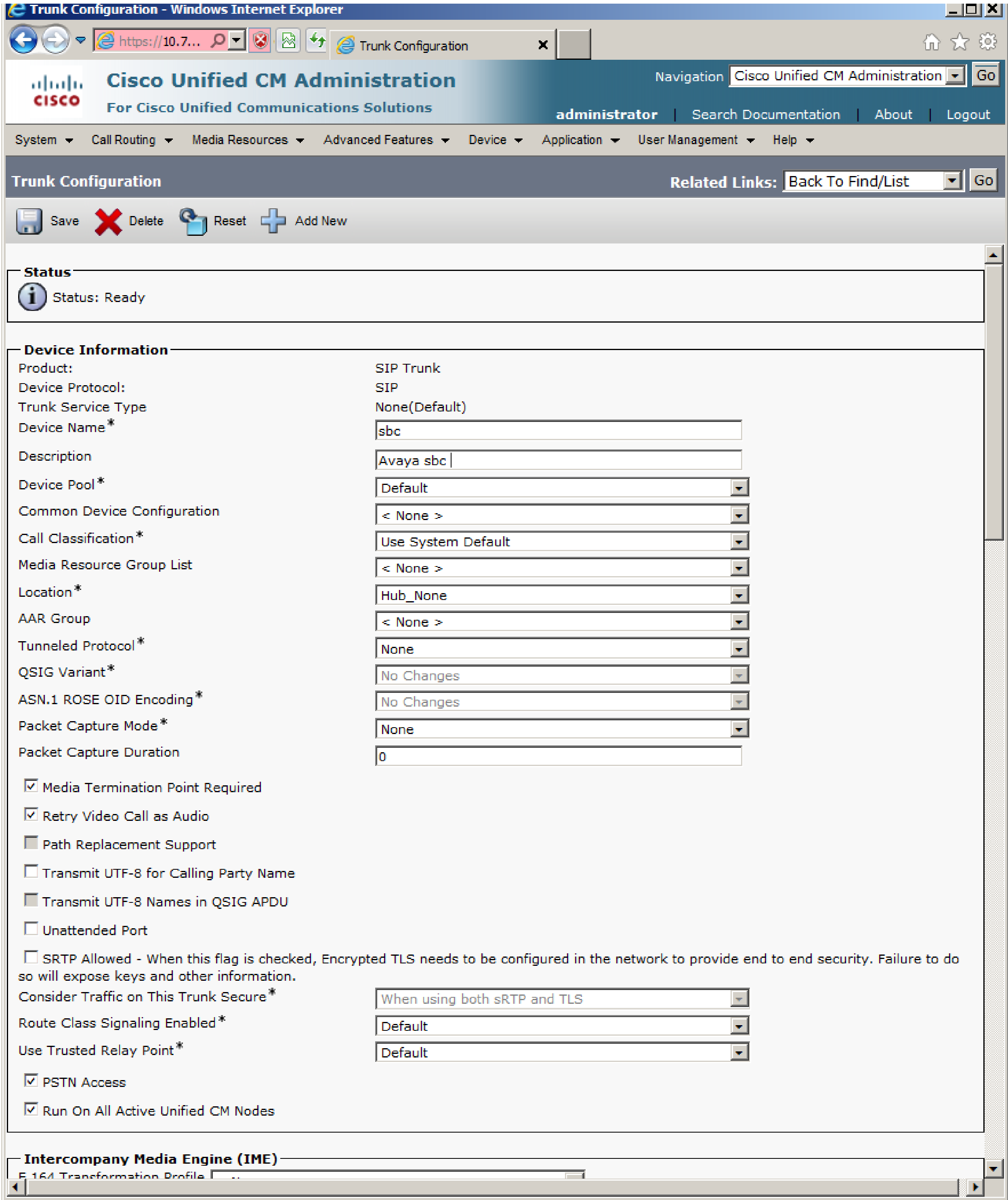
Click the **Add New** Button.



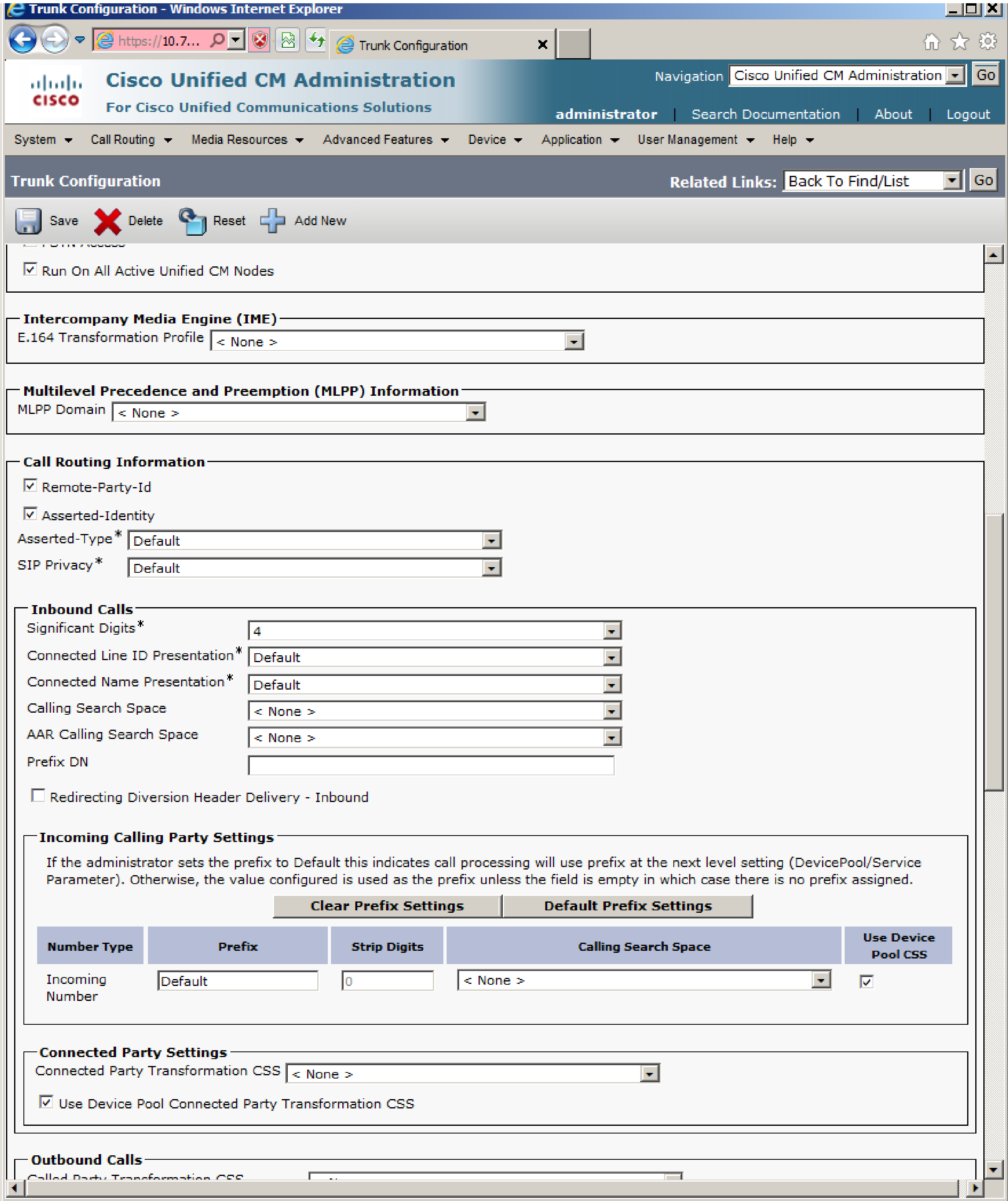
Select “SIP trunk” as the **Trunk Type**.
Select “SIP” as the **Device Protocol**.
Leave “None” as **Trunk Service Type**.
Click the **Next** button.


Trunk Configuration - Windows Internet Explorer
https://10.7...
Trunk Configuration
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Help
Trunk Configuration
Related Links: Back To Find/List Go
Next
Status
Status: Ready
Trunk Information
Trunk Type* SIP Trunk
Device Protocol* SIP
Trunk Service Type* None(Default)
Next
*- indicates required item.

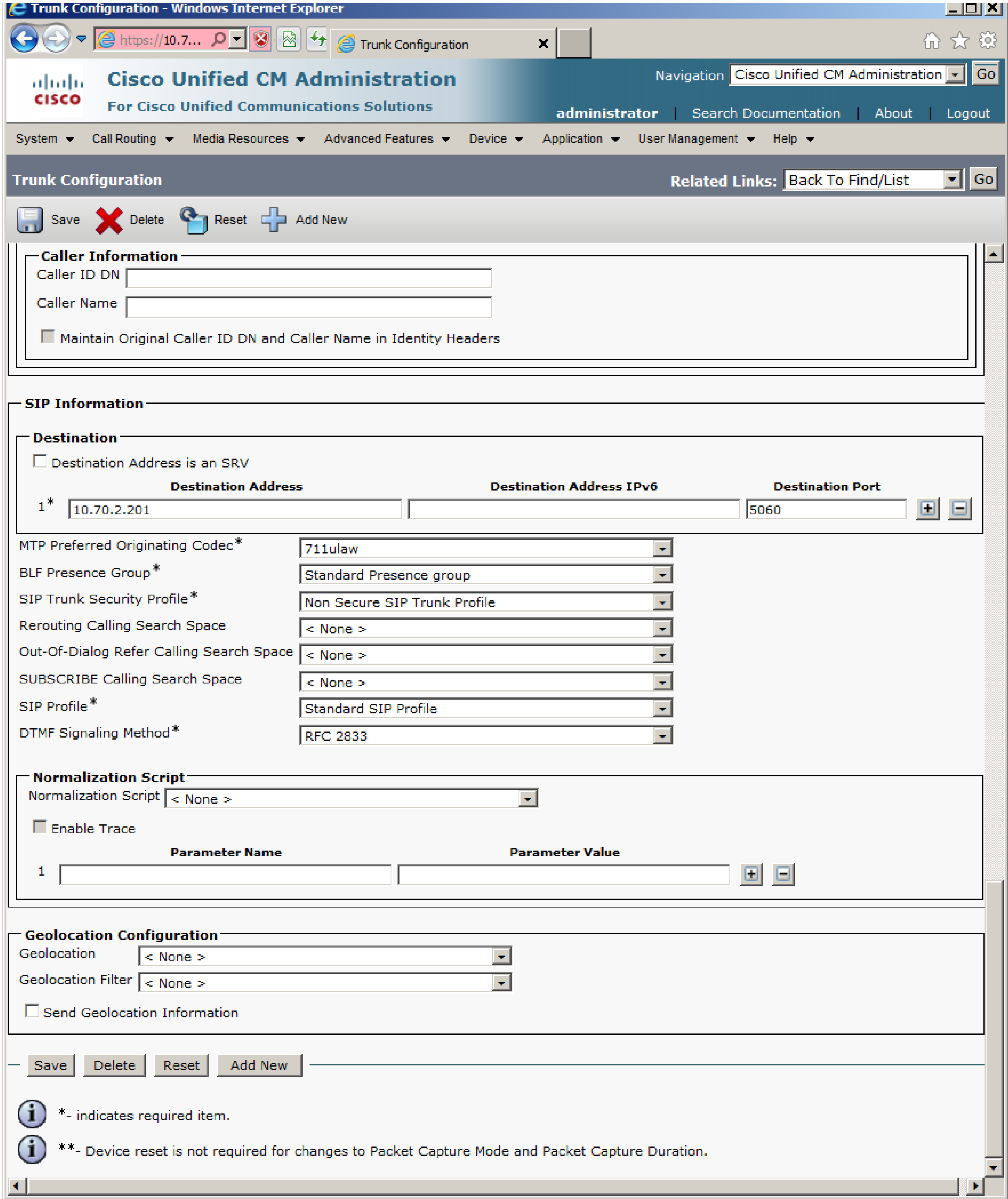
The **Trunk Configuration** screen appears.
Enter a **Device Name**. (In this example the device name is sbc)
Enter a **Description**.
Select a **Device Pool**. (The device pools are created as part of the initial configuration). In case that additional Device pools are not configured, a "Default" device pool can be selected. "Default" is the value that was selected for this example. Consult reference [2] for more information on how to setup Device Pools.
Check the **Media Termination Point Required** checkbox.
Check the **Run On All Active Unified CM Nodes** checkbox.
Scroll down to see the rest of the parameters.


Trunk Configuration - Windows Internet Explorer
https://10.7...
Trunk Configuration
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Help
Trunk Configuration
Related Links: Back To Find/List Go
Save Delete Reset Add New
Status
Status: Ready
Device Information
Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type None(Default)
Device Name* sbc
Description Avaya sbc
Device Pool* Default
Common Device Configuration < None >
Call Classification* Use System Default
Media Resource Group List < None >
Location* Hub_None
AAR Group < None >
Tunneled Protocol* None
QSIG Variant* No Changes
ASN.1 ROSE OID Encoding* No Changes
Packet Capture Mode* None
Packet Capture Duration 0
Media Termination Point Required
Retry Video Call as Audio
Path Replacement Support
Transmit UTF-8 for Calling Party Name
Transmit UTF-8 Names in QSIG APDU
Unattended Port
SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
Consider Traffic on This Trunk Secure* When using both sRTP and TLS
Route Class Signaling Enabled* Default
Use Trusted Relay Point* Default
PSTN Access
Run On All Active Unified CM Nodes
Intercompany Media Engine (IME)

Select the number of **Significant Digits**. Usually, this number is the length of the directory numbers.
Scroll down to see the rest of the parameters.



On **Destination Adresss**. Enter the Internal IP of the Avaya Session Border Controller for Enterprise. In our example, from **Figure 1** is 10.70.2.201.
On **Destination Port**. Enter the listening port on the Avaya Session Border Controller for Enterprise.Usually this value is “5060”.
On **SIP Trunk Security Profile**. Select “Non Secure SIP Trunk Profile”.
On **SIP Profile**. Select “Standard SIP Profile”.
On **DTMF Signaling Method**. Select “RFC 2833”.
Click the **Save** button.

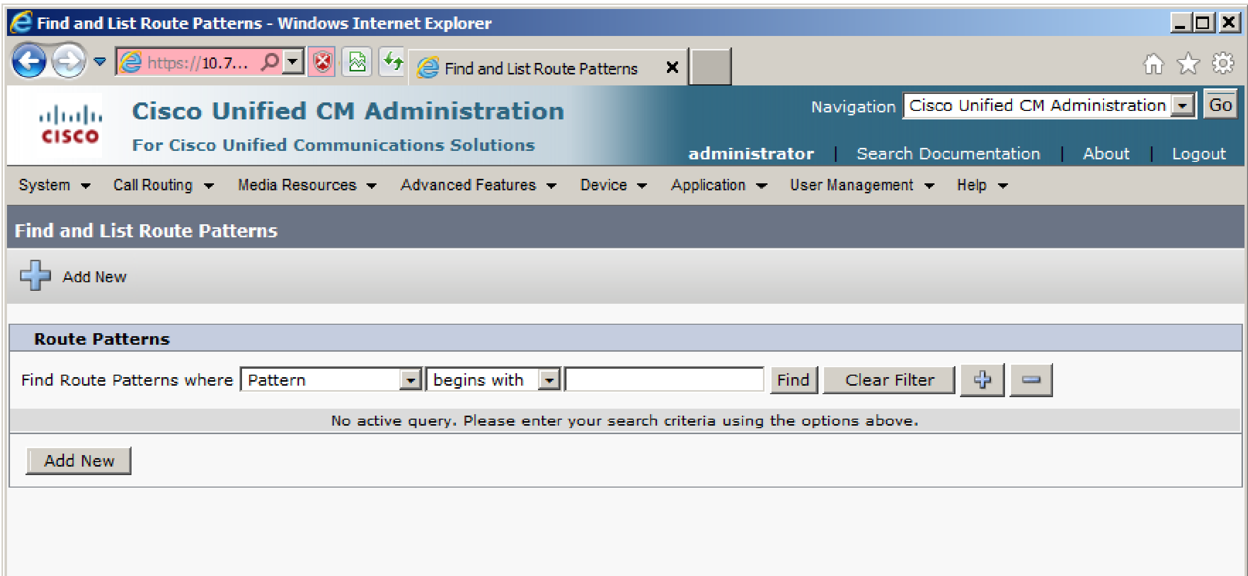

Trunk Configuration - Windows Internet Explorer
https://10.7...
Trunk Configuration
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Help
Trunk Configuration
Related Links: Back To Find/List Go
Save Delete Reset Add New
Caller Information
Caller ID DN
Caller Name
Maintain Original Caller ID DN and Caller Name in Identity Headers
SIP Information
Destination
Destination Address is an SRV
Destination Address
Destination Address IPv6
Destination Port
1* 10.70.2.201 5060
MTP Preferred Originating Codec* 711ulaw
BLF Presence Group* Standard Presence group
SIP Trunk Security Profile* Non Secure SIP Trunk Profile
Rerouting Calling Search Space < None >
Out-Of-Dialog Refer Calling Search Space < None >
SUBSCRIBE Calling Search Space < None >
SIP Profile* Standard SIP Profile
DTMF Signaling Method* RFC 2833
Normalization Script
Normalization Script < None >
Enable Trace
Parameter Name
Parameter Value
1
Geolocation Configuration
Geolocation < None >
Geolocation Filter < None >
Send Geolocation Information
Save Delete Reset Add New
*- indicates required item.
**- Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

5.3.2. Route Pattern

On Cisco Unified Communications Manager Route Pattern are used to send specific patterns to a certain trunk or gateway.

On the **Call Routing** menu, go to **Route/Hunt** and then **Route Pattern**.

Click the **Add New** button.



Enter a **Route Pattern**. In the example 9.@ was used. 9 is the digit used to go out on most PBX. . The dot divides in 2 parts. The “@” represent a numbering plan. The numbering plan is selected below. Consult reference [2] for more information on how to create route patterns.

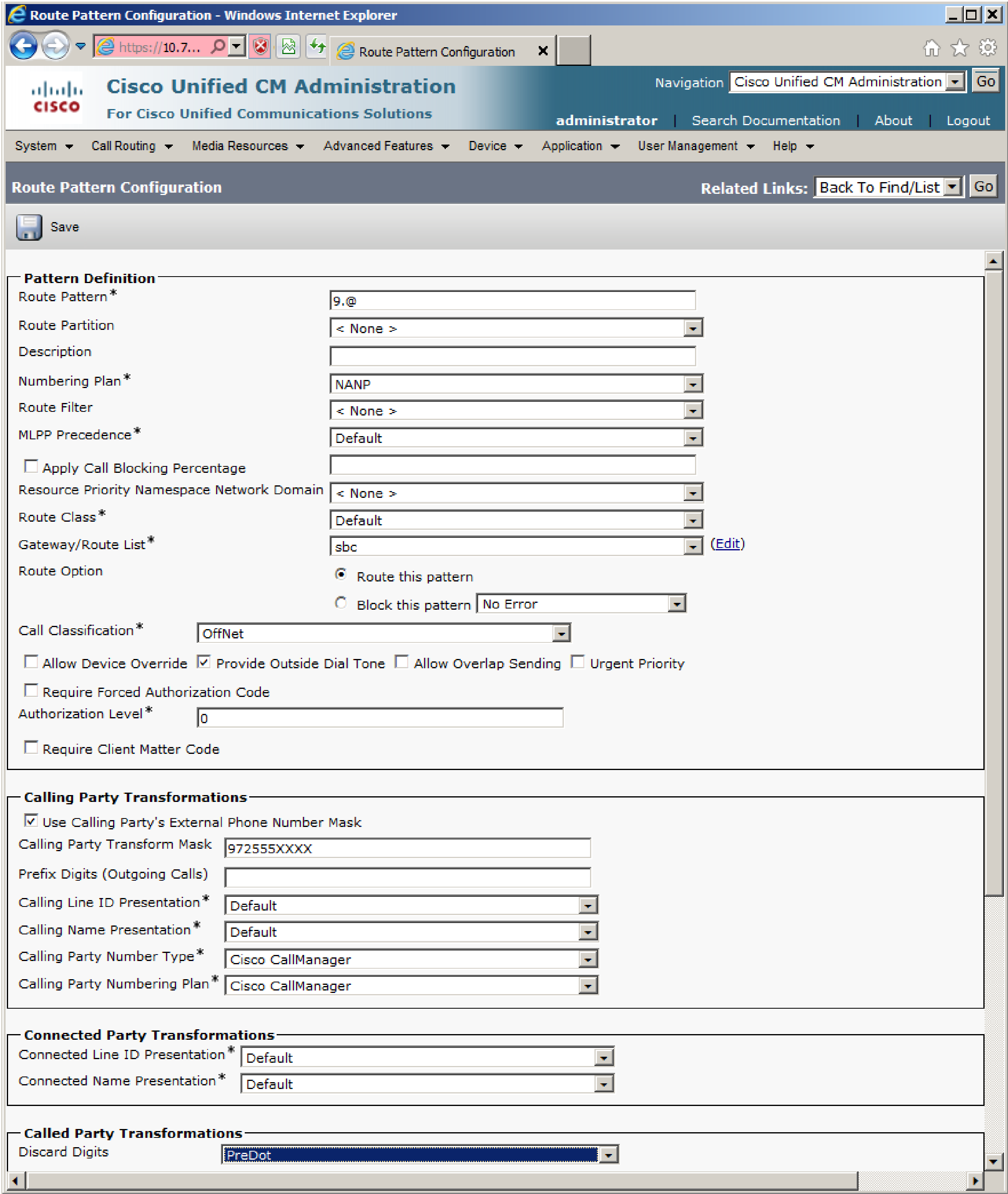
In the **Numbering plan** select “NANP”.

In the **Gateway/Route List** select the SIP trunk just added. (i.e. sbc)

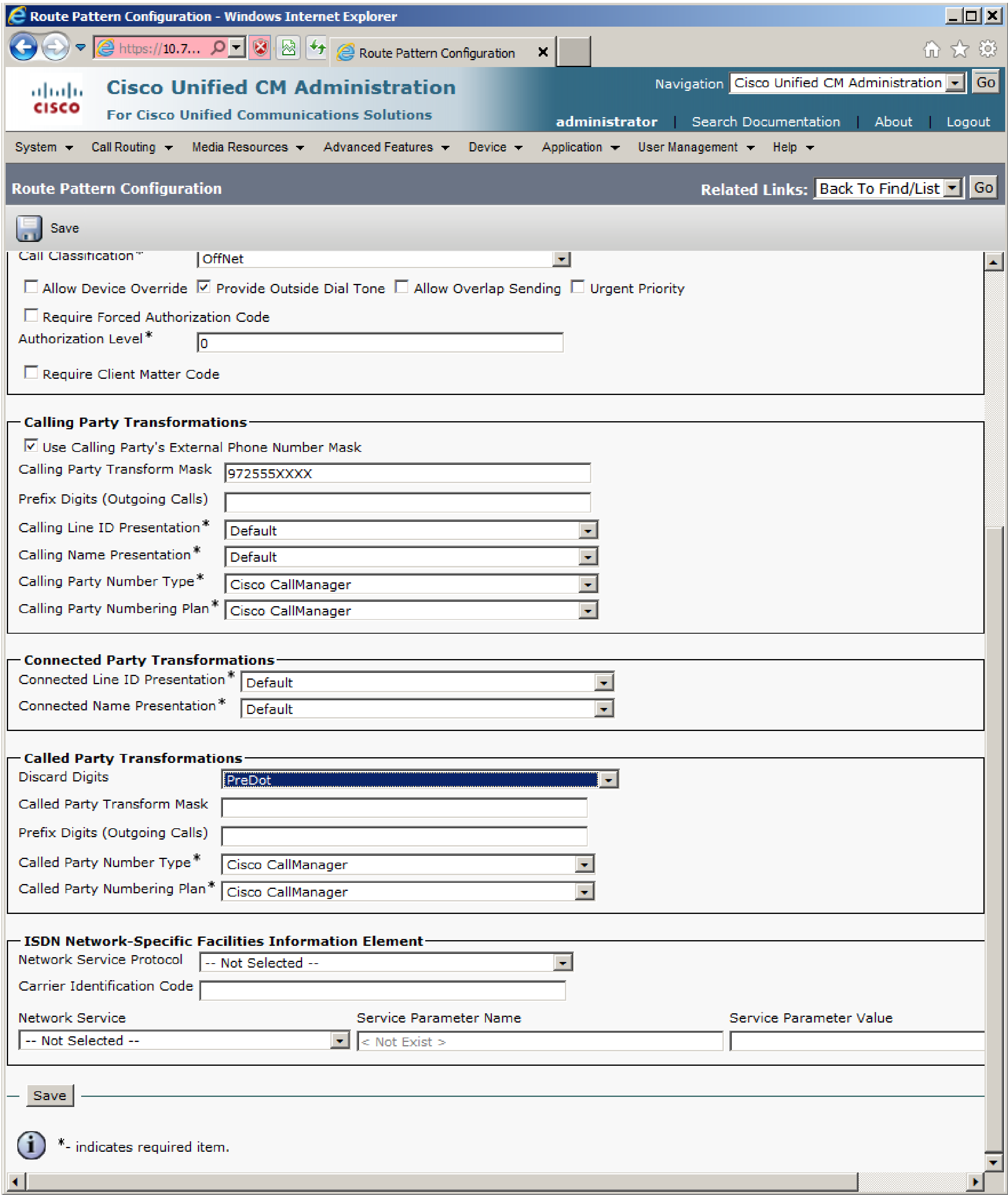
In the **Calling Party Transform Mask** enter the six digit suffix of your phone numbers. Followed by XXXX. The number of X’s depends on the length of the directory numbers

For example, if the service provider gave the phone numbers9725550000 to 9725559999. And it was decided that the length will be 4 digits. The mask will be 972555XXXX. The mask is needed otherwise Cisco Unified Communications managers sends the directory number as the originating number.

Scroll down to see the rest of the settings.

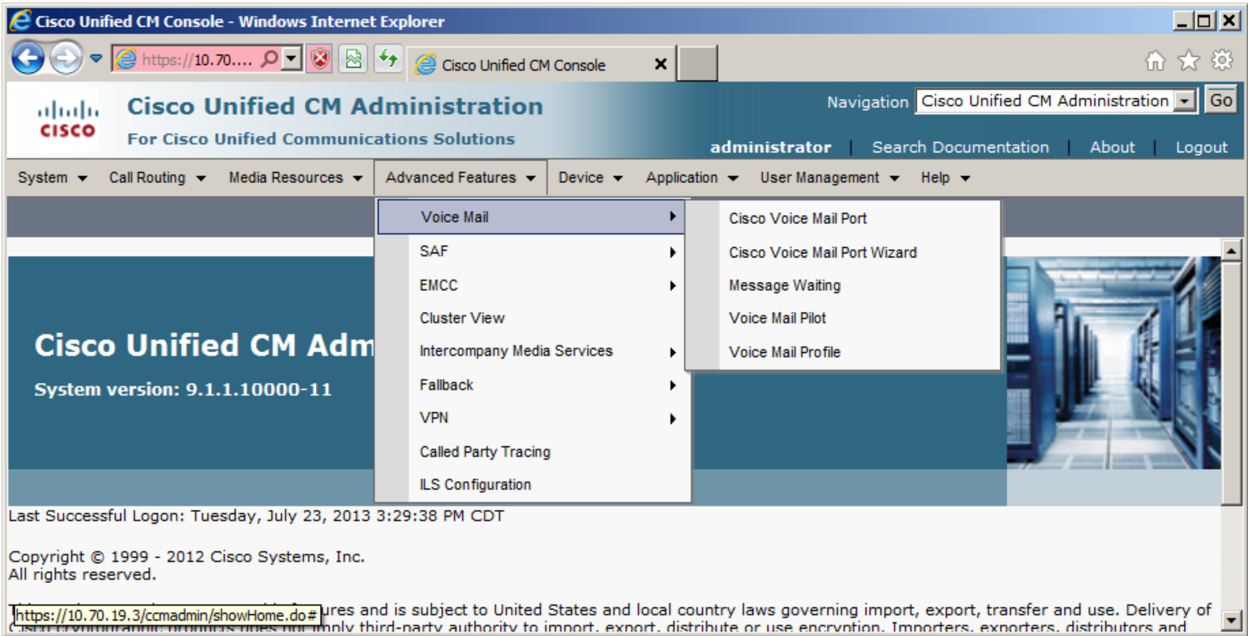

Route Pattern Configuration - Windows Internet Explorer
https://10.7...
Route Pattern Configuration
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
administrator
Search Documentation
About
Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Help
Route Pattern Configuration
Related Links:
Back To Find/List
Go
Save
Pattern Definition
Route Pattern*
9.@
Route Partition
< None >
Description
Numbering Plan*
NANP
Route Filter
< None >
MLPP Precedence*
Default
Apply Call Blocking Percentage
Resource Priority Namespace Network Domain
< None >
Route Class*
Default
Gateway/Route List*
sbc
(Edit)
Route Option
Route this pattern
Block this pattern
No Error
Call Classification*
OffNet
Allow Device Override
Provide Outside Dial Tone
Allow Overlap Sending
Urgent Priority
Require Forced Authorization Code
Authorization Level*
0
Require Client Matter Code
Calling Party Transformations
Use Calling Party's External Phone Number Mask
Calling Party Transform Mask
972555XXXX
Prefix Digits (Outgoing Calls)
Calling Line ID Presentation*
Default
Calling Name Presentation*
Default
Calling Party Number Type*
Cisco CallManager
Calling Party Numbering Plan*
Cisco CallManager
Connected Party Transformations
Connected Line ID Presentation*
Default
Connected Name Presentation*
Default
Called Party Transformations
Discard Digits
PreDot

In the **Discard Digits** select “PreDot”. This removes the 9 from the dialed number. Click the **Save** button.



5.3.3. Voicemail

To view or change voicemail settings, select the **Advanced Features** menu and then **Voicemail** as shown in the following screen. Consult reference [2] for more information on the topics in this section.



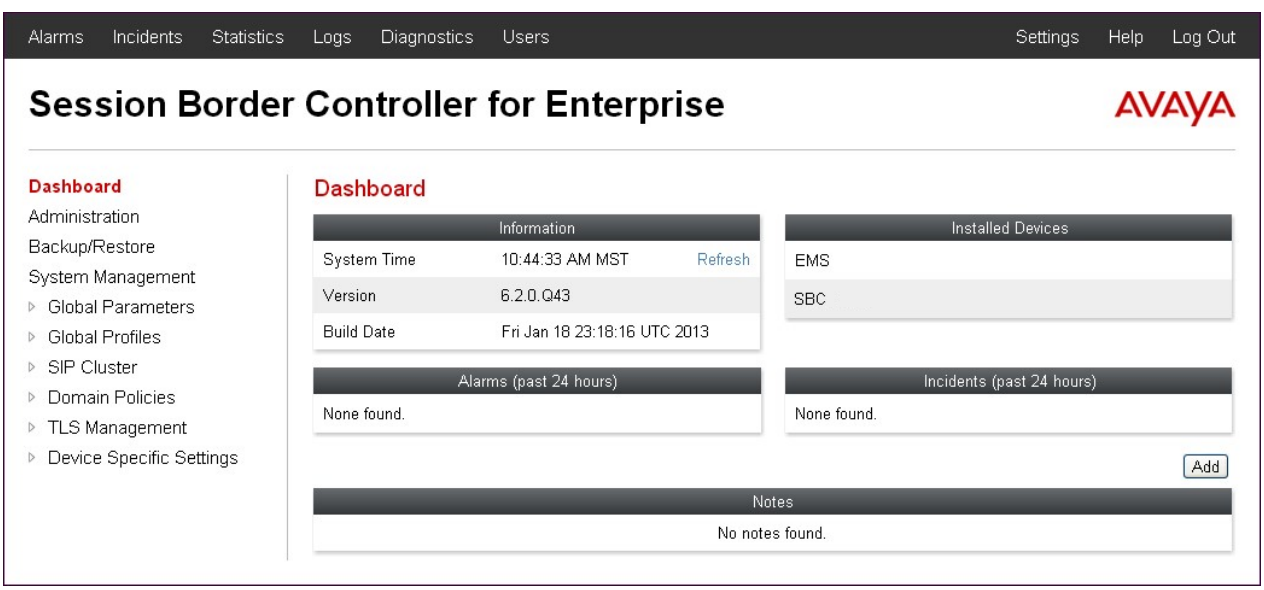
6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed. Also, it is assumed the management configuration, licensing and initial commissioning of the SBC has already been done

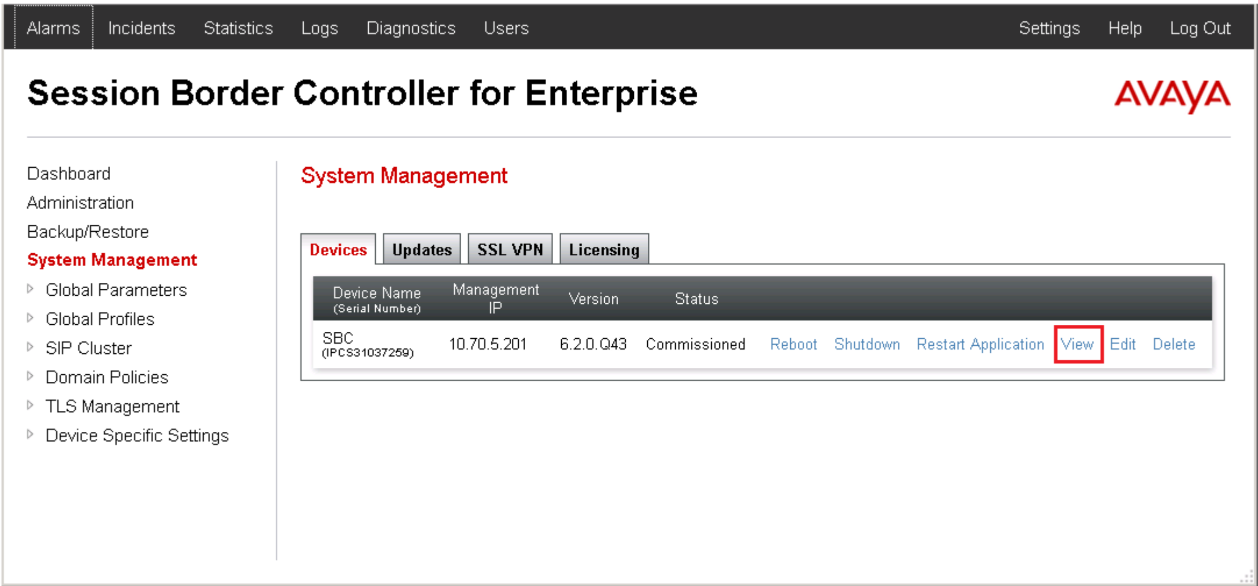
Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management LAN IP address of the Avaya SBCE.

Enter appropriate credentials and click **Log In**.

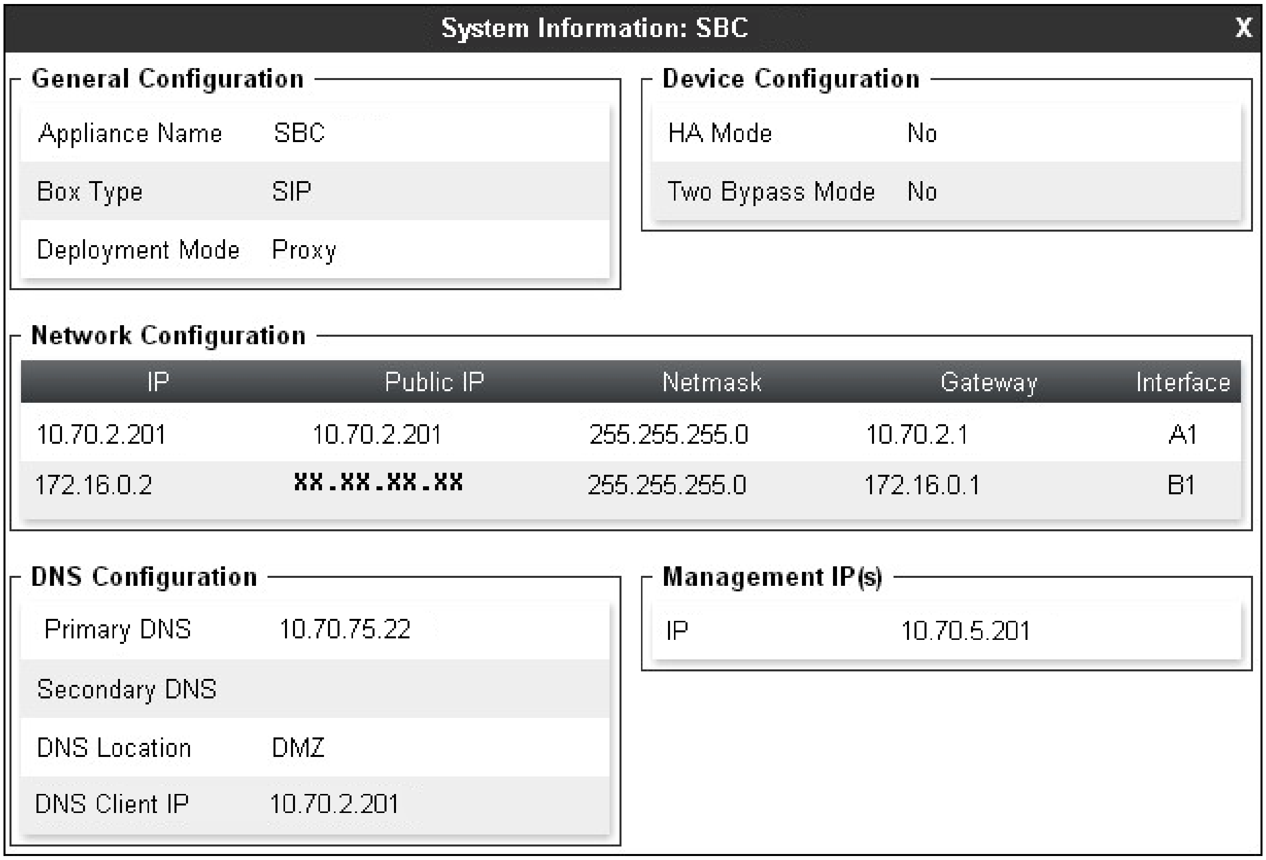
The Dashboard for the Avaya SBCE will appear.



To view system information that was configured during installation, click on **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **SBC** is shown. To view the configuration of this device, click **View** as highlighted below.

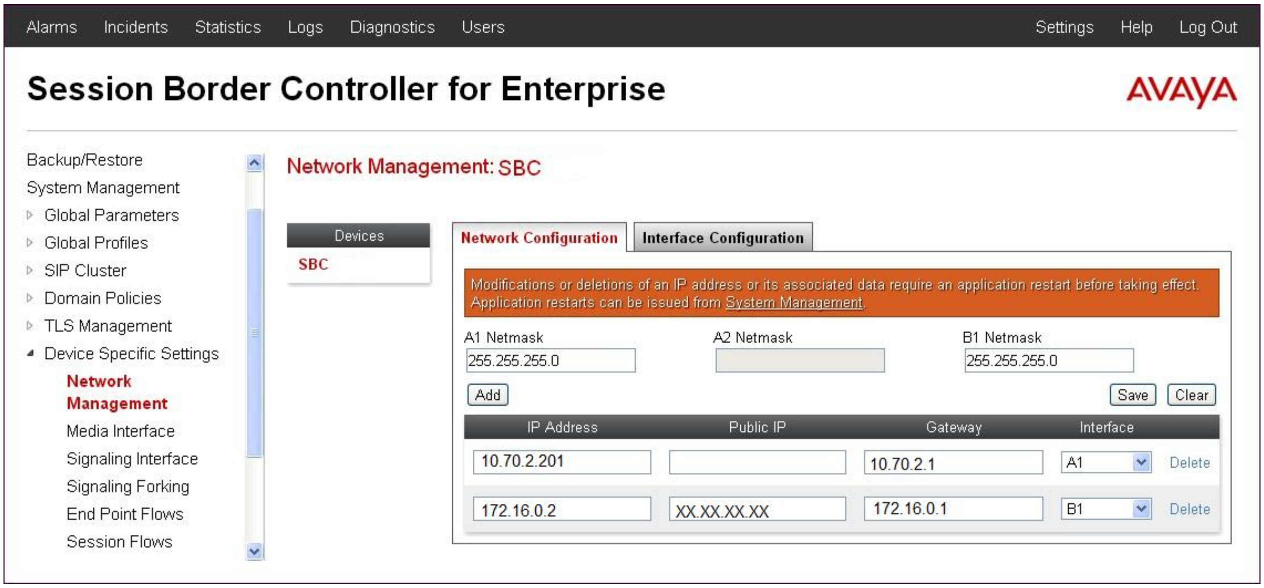


The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. IP address was given to include DNS. Default values were used for all other fields.

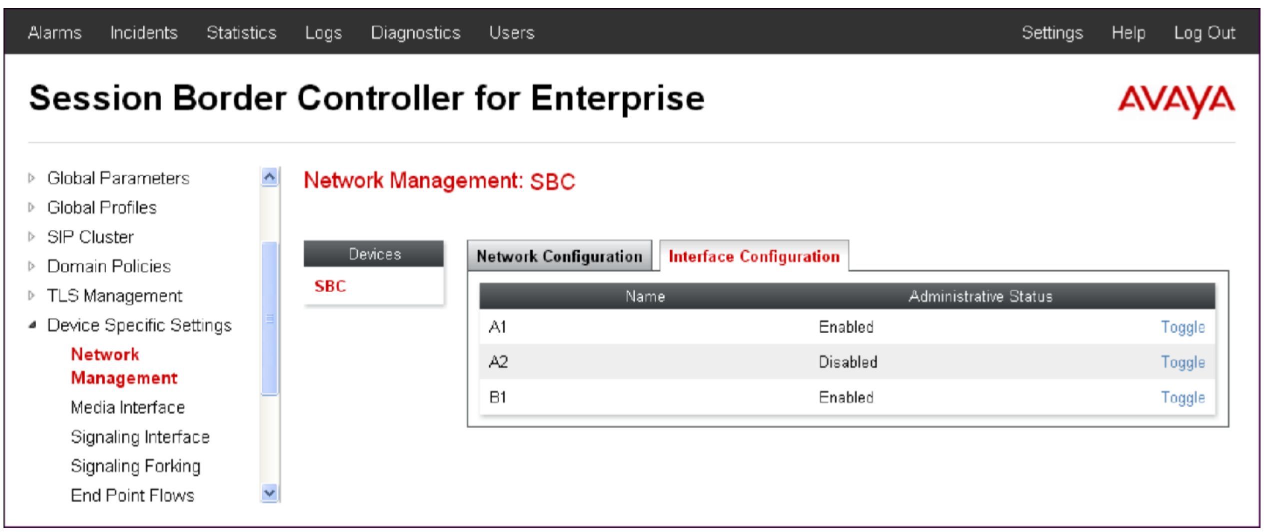


6.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the enterprise interface is assigned to **A1** and the interface towards Verizon is assigned to **B1**. The public interface is shown as XX.XX.XX.XX as an example. In a deployment, if the Firewall is Natting the SBC IP enter the Public IP field is used to put the Natted public IP of the SBC. If there is no NAT then that field is kept blank.



The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle** button.

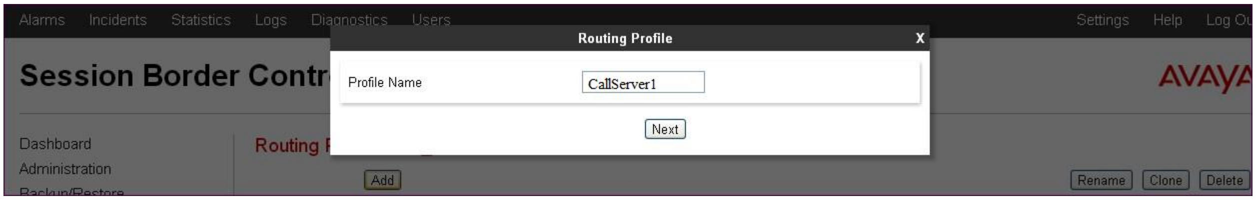


Note: Screenshots are obtained with Portwell CAD version of ASBCE. Based on the platform used the number of interfaces will vary.

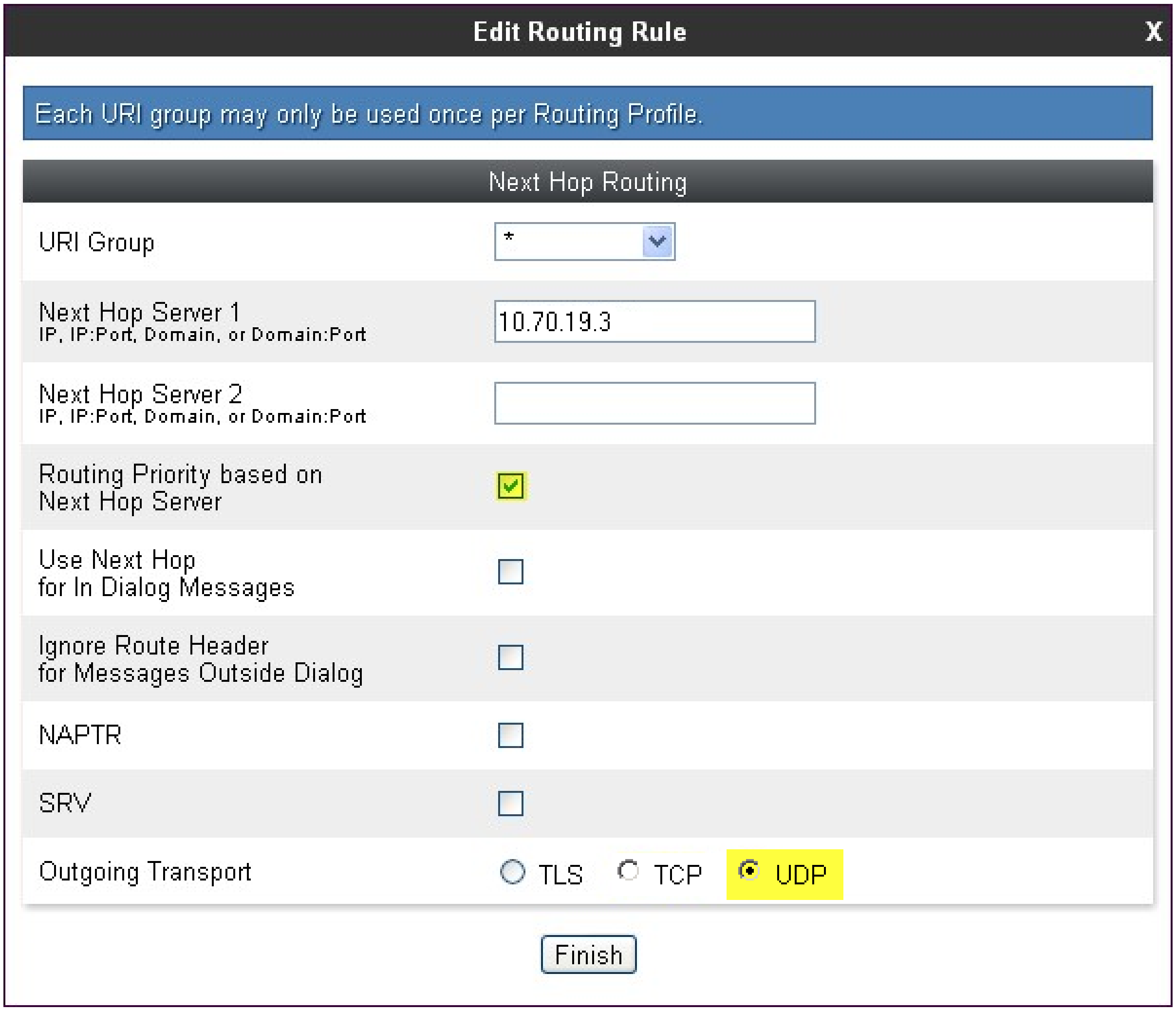
6.2. Routing Profile

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

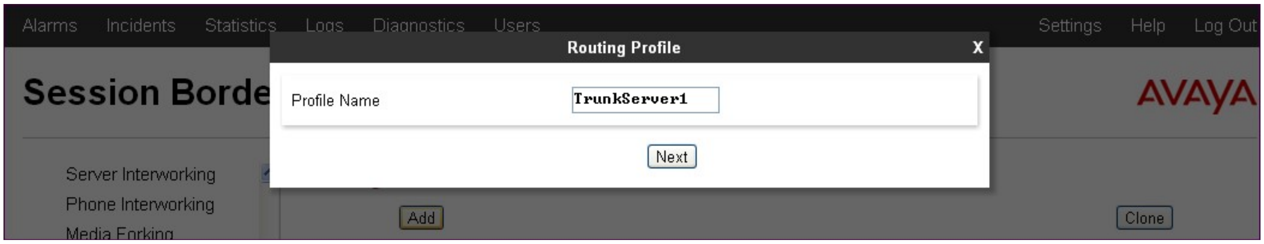
To add a routing profile for Cisco Unified Communications Manager, navigate to **Global Profiles → Routing** and select **Add** (not shown). Enter a **Profile Name** and click **Next** to continue.

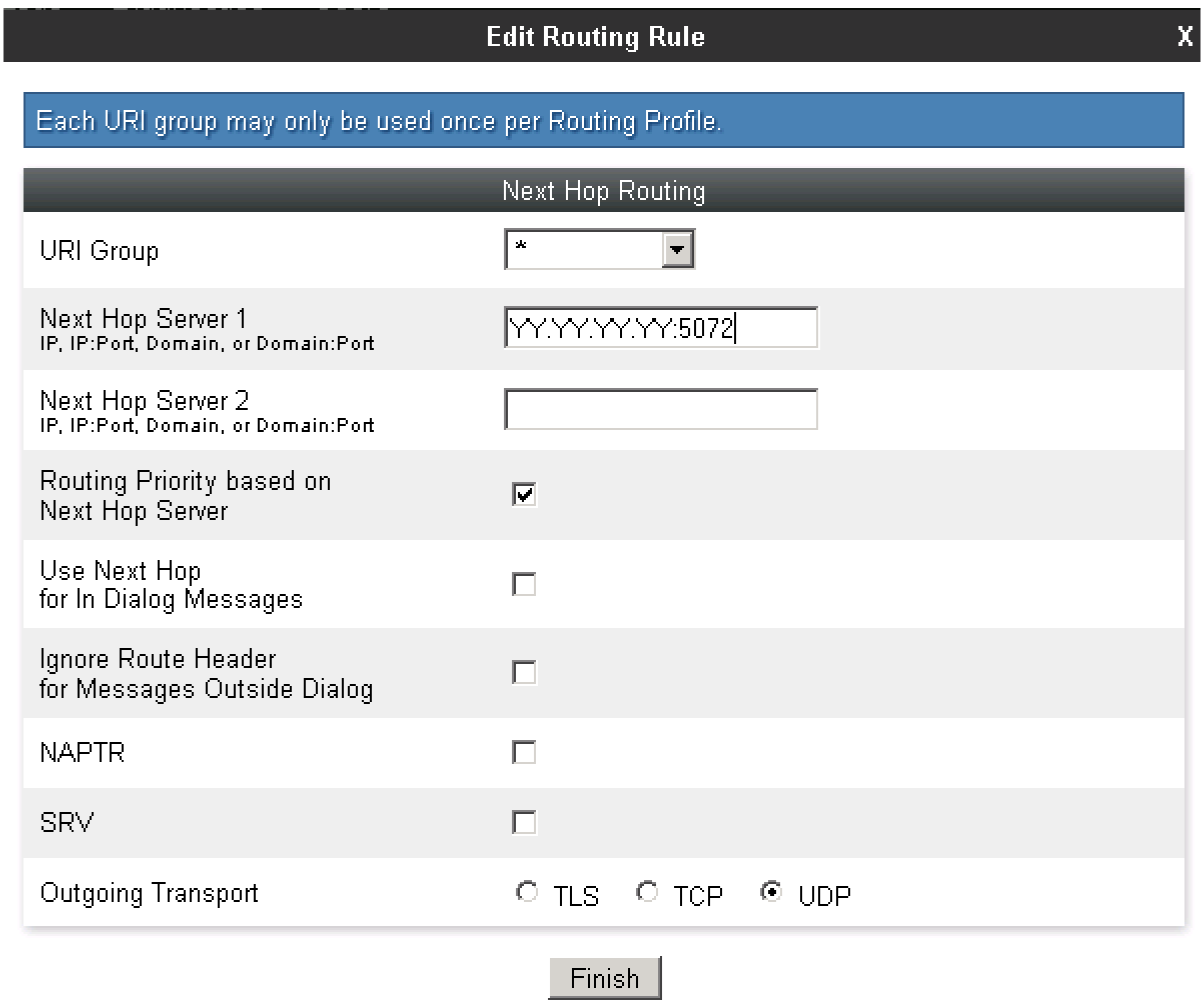


The following screen illustrates the Routing Profile named "CallServer1" created in the sample configuration for Cisco Unified Communications Manager. The **Next Hop Server 1** IP address must match the IP address of the Cisco Unified Communications Manager LAN settings in Figure 1. Leave the **Routing Priority based on Next Hop Server** box checked and select **TCP or UDP** for the **Outgoing Transport field.** The **non Secure SIP Trunk Profile** in Cisco Unified Communications Manager is configured to listen on both protocols. In our example **UDP** was selected.


Edit Routing Rule
X
Each URI group may only be used once per Routing Profile.
Next Hop Routing
URI Group
*
Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port
10.70.19.3
Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port
Routing Priority based on Next Hop Server
Use Next Hop for In Dialog Messages
Ignore Route Header for Messages Outside Dialog
NAPTR
SRV
Outgoing Transport
TLS
TCP
UDP
Finish

A new routing profile named “TrunkServer1” was created for the Verizon SIP Trunk test service. The **Next Hop Server 1** IP address must match the IP address and port of the Verizon SIP Trunk test service in Figure 1. Leave the **Routing Priority based on Next Hop Server** box checked and select **UDP** or TCP for the **Outgoing Transport field. Current Example is shown with UDP**





Note: The sample routing configurations are as per Verizon test SIP trunk configuration requirements and can be modified as per the trunk provider utilized in the deployment. Port 5072 is a non-default SIP Port utilized in this test deployment as per the test requirements and shall be modified based on the Service provider and field deployment requirements.

6.3. Server Interworking Profile

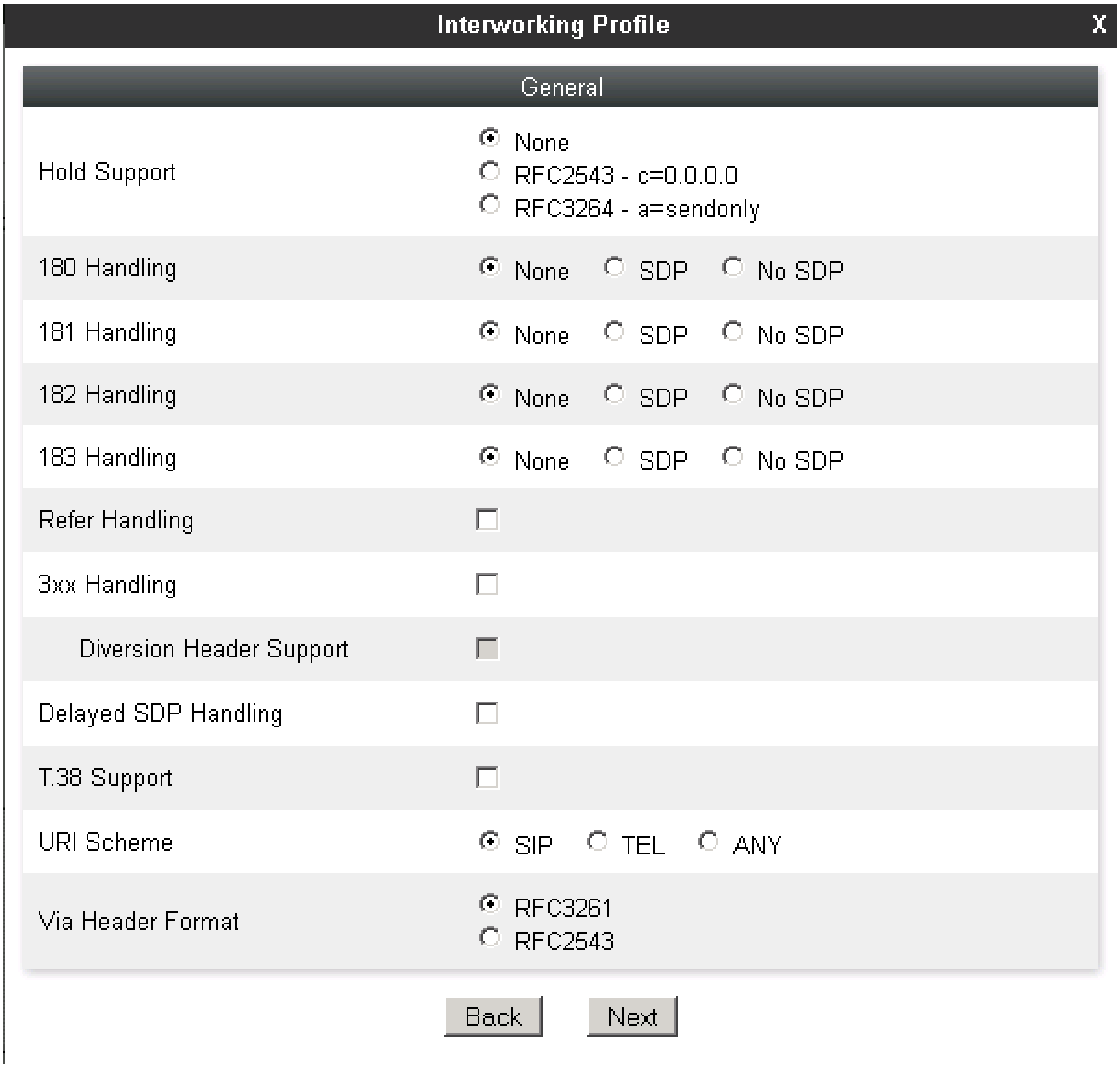
The Server Internetworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking profiles were created for Cisco Unified Communications Manager and Verizon Business SIP Trunk test service.

6.3.1. Server Interworking Profile – Cisco Unified Communications Manager

In the sample configuration, the Cisco Unified Communications Manager Server Interworking profile was created. To add a Server Interworking Profile for Cisco Unified Communications Manager, navigate to **Global Profiles → Server Interworking**, click the **Add** button. Enter a **Profile Name** and click **Next** to continue. In the example callserver1 was used.

Use default values for all fields and click **Next** to continue.

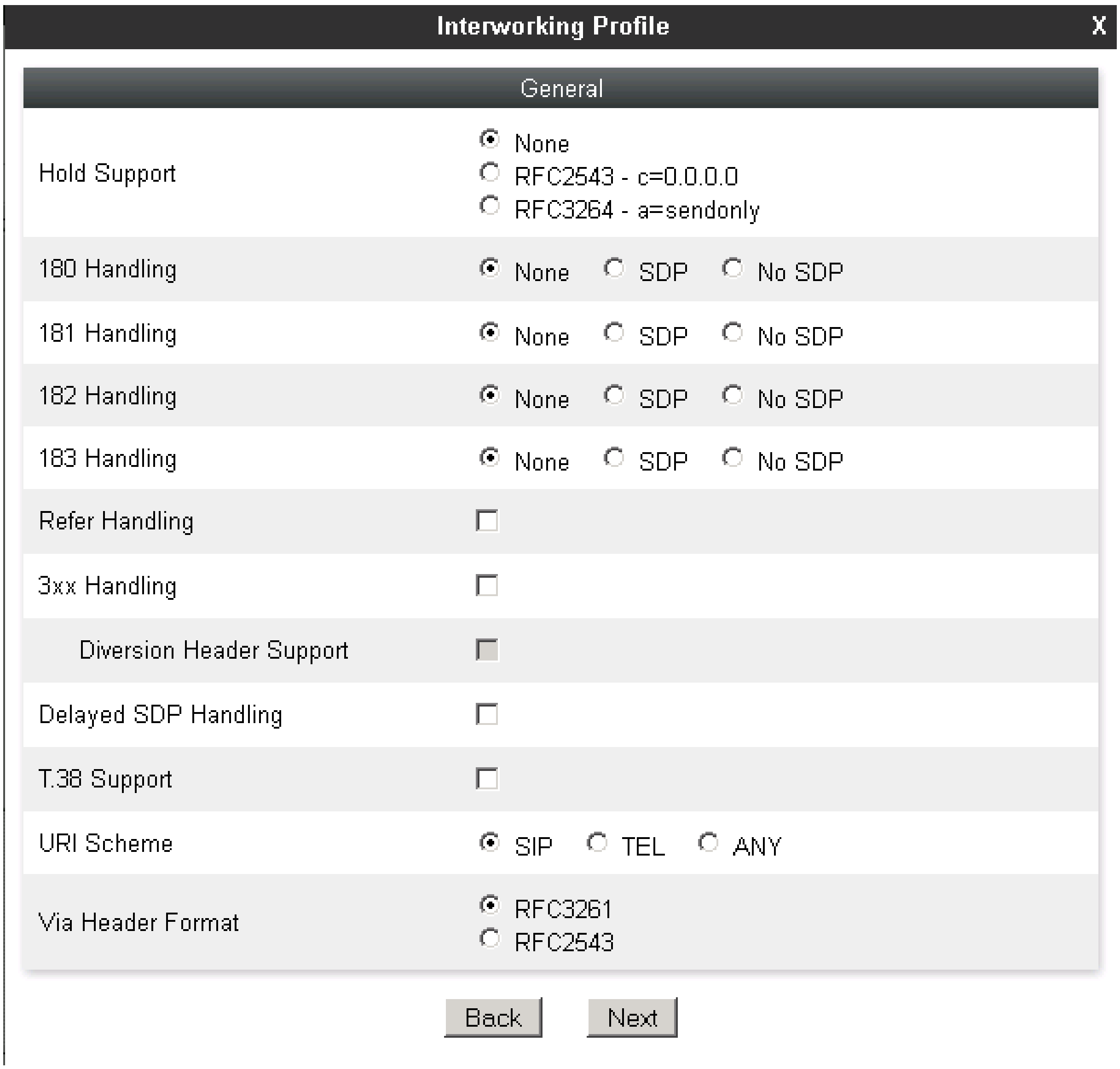


Default values can be used for the next windows that appear. Click **Next** to continue, then **Finish** to save the changes (not shown).

6.3.2. Server Interworking Profile – Verizon

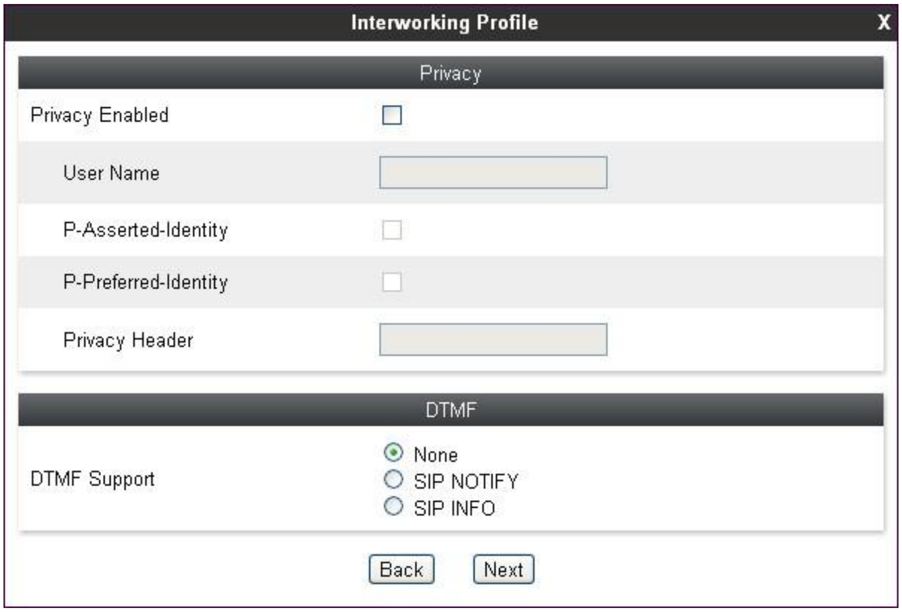
To create a new Server Interworking Profile for Verizon, navigate to **Global Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**. In the example TrunkServer1 was used.

Use default values for all remaining fields. Click **Next** to continue.

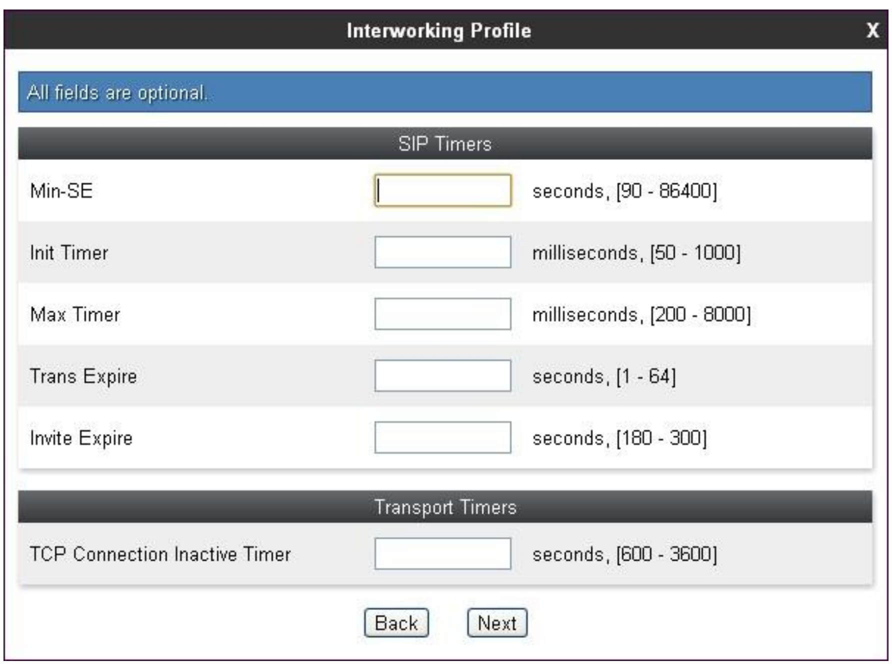


Note: The above configurations are standard Trunk server profile configurations in Avaya session border controller for Enterprise with Verizon Test trunk Service. Above values shall be modified based on the field service provider and deployment requirements.

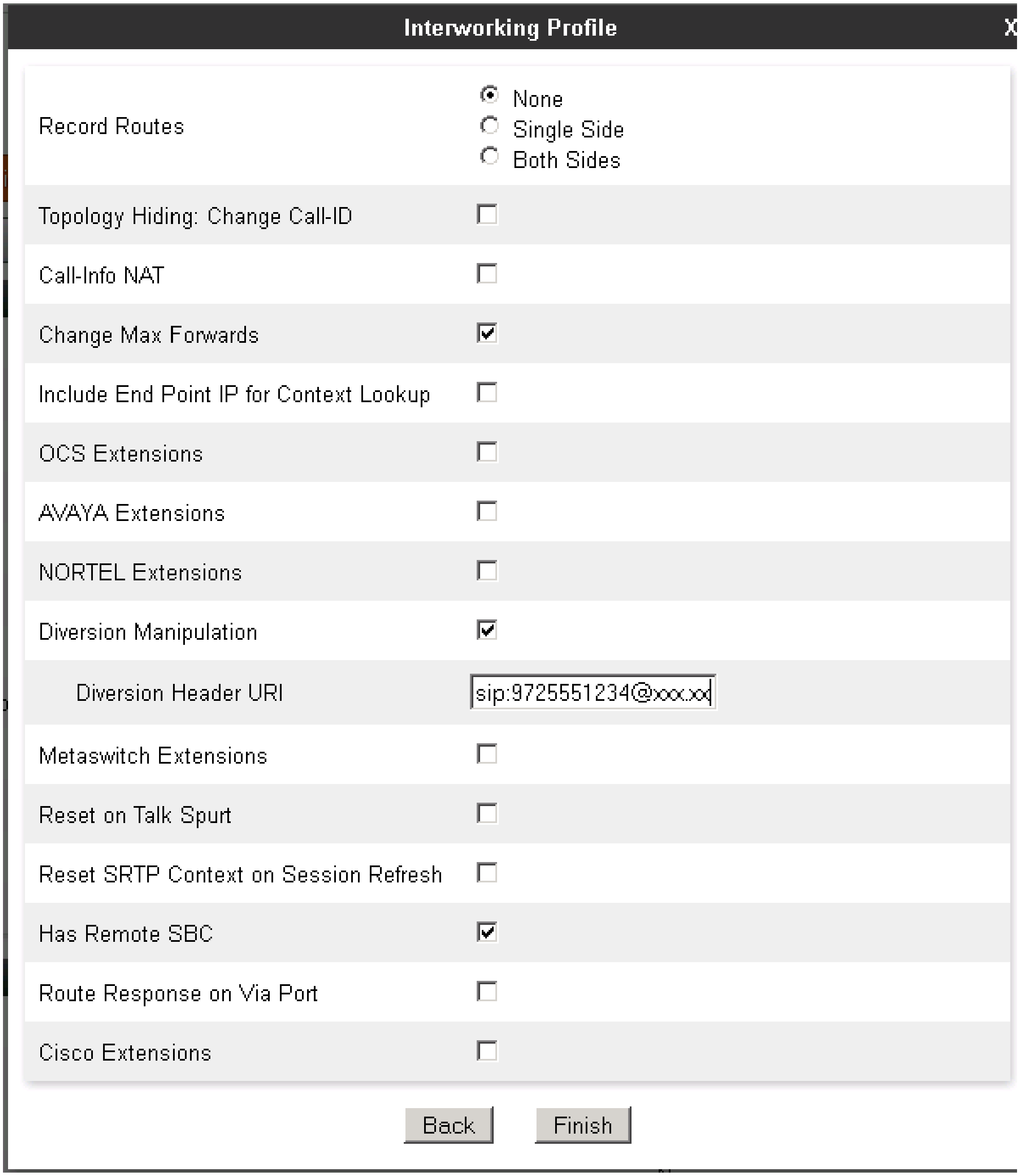
Default values can be used for the **Privacy** and **DTMF** sections on the following screen. Click **Next** to continue.



Default values can be used for the **SIP Timers** and **Transport Timers** sections on the following screen. Click **Next** to continue.



Select “None” for **Record Routes**. This is the setting that was used for testing. Check **Diversion Manipulation**. This setting is required for some call forward and transfer to PSTN scenarios. If this field is check all calls will include a DIVERSION header. If this is not desirable, it can be left uncheck. However, some call forward and transfer scenarios will not work which requires Diversion support. If the Diversion support is required, Enable the **Diversion Manipulation** field then enter the main number assigned to the company in the format sip:MainNumber@FirewallPublicIP. In our case the main number is 9728551234 and the Firewall IP is represented by xx.xx.xx.xx. Use the Natted public IP of the SBC, Default values can be used for all remaining fields. Click **Finish** to save changes.



Note: The above configurations are as configured in test environment of Avaya session border controller with Verizon Test trunk Service as per this deployment. Above values shall be modified based on the field service provider and deployment requirements.

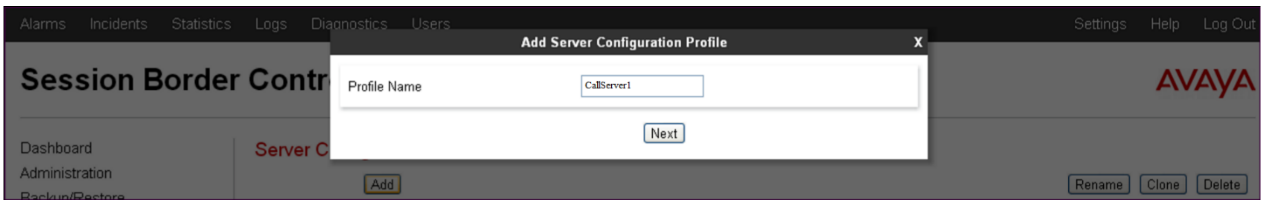
6.4. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs are used to configure and manage various SIP call server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

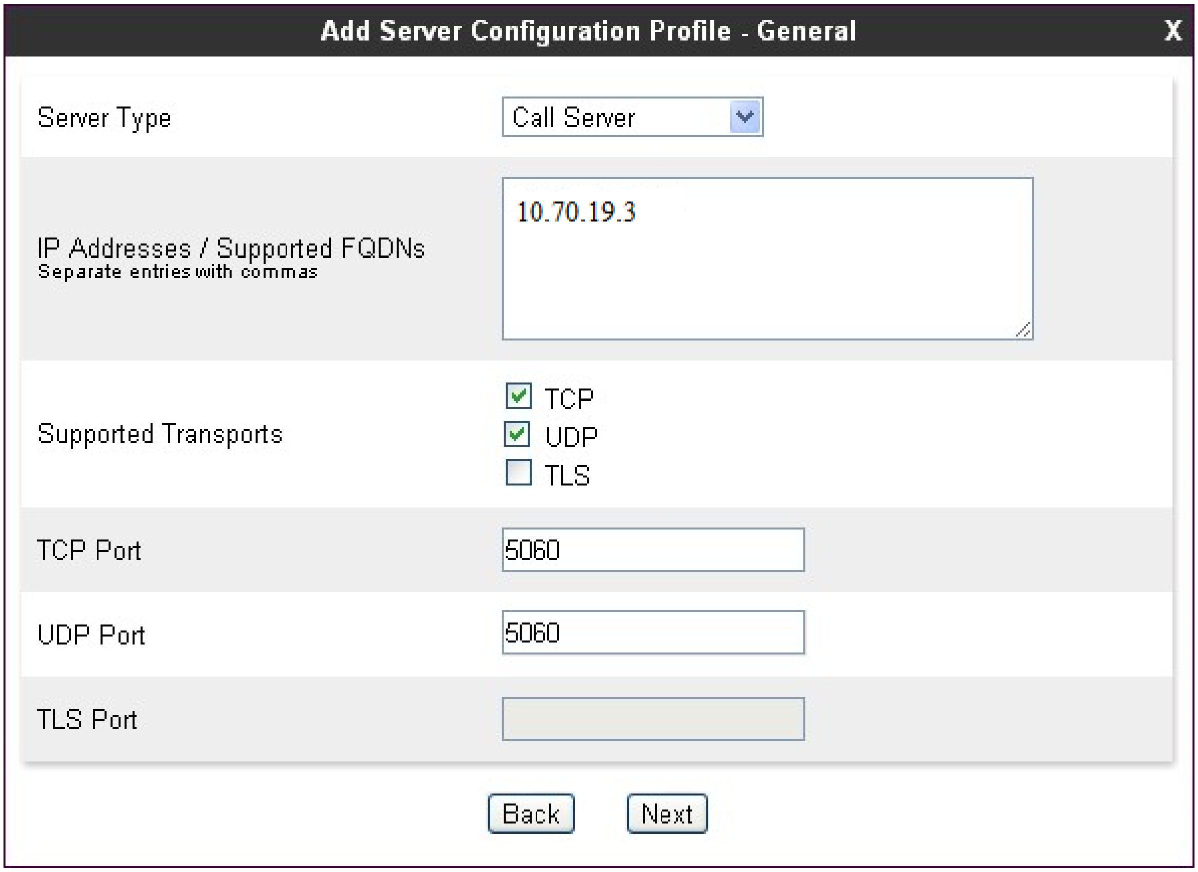
In the sample configuration, separate Server Configurations were created for Cisco Unified Communications Manager and Verizon Business SIP Trunk test service.

6.4.1. Server Configuration – Cisco Unified Communications Manager

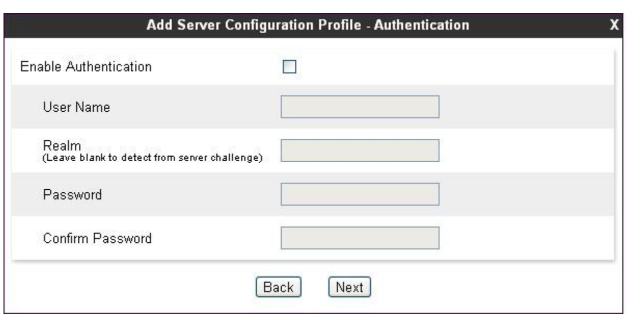
To add a Server Configuration Profile for Cisco Unified Communications Manager, navigate to **Global Profiles → Server Configuration** and click **Add** (not shown). Enter a descriptive name for the **Profile Name** and click **Next**.

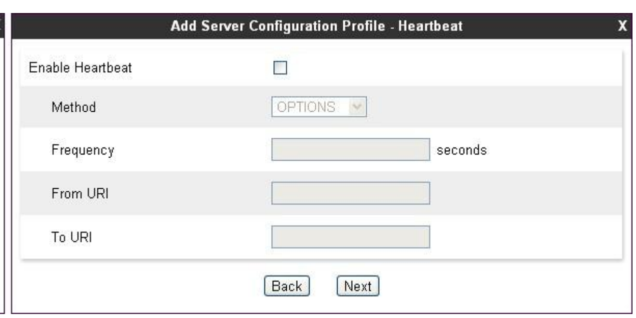


The following screens illustrate the Server Configuration for the Profile name "Cisco Unified Communications Manager". In the **General** parameters, select "Call Server" from the **Server Type** drop-down menu (not shown). In the **IP Addresses / Supported FQDNs** area, the IP Address of the Cisco Unified Communications Manager LAN 1 interface in the sample configuration is entered. In the **Supported Transports** area, "UDP" and "TCP" is selected, and the **UDP Port** and **TCP port** is set to "5060". If adding a new profile, click **Next**. If editing an existing profile, click **Finish** (not shown).

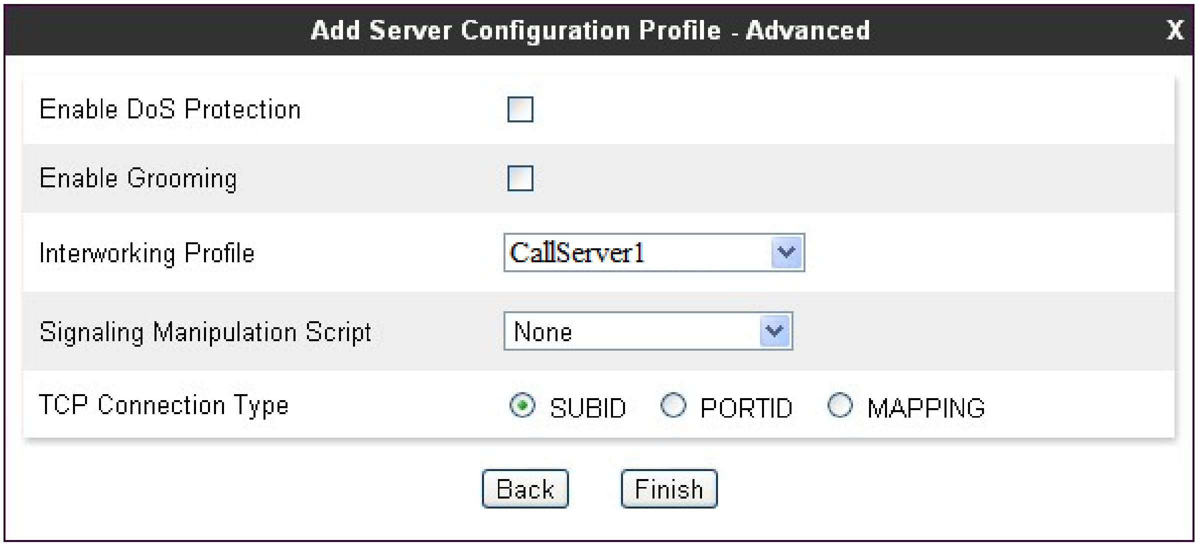


In the next two windows that appear, verify **Enable Authentication** and **Enable Heartbeat** are unchecked. Cisco Unified Communications Manager does not require authentication and the Heartbeat feature is not necessary because Avaya SBCE will forward SIP OPTIONS from Verizon to the Cisco Unified Communications Manager. Click **Next** to continue.





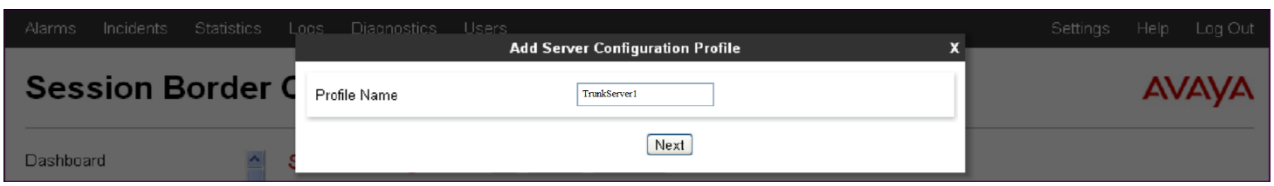
In the new window that appears, select the **Interworking Profile** created for Cisco Unified Communications Manager in Section 6.3.1. Use default values for all remaining fields. Click **Finish** to save the configuration.



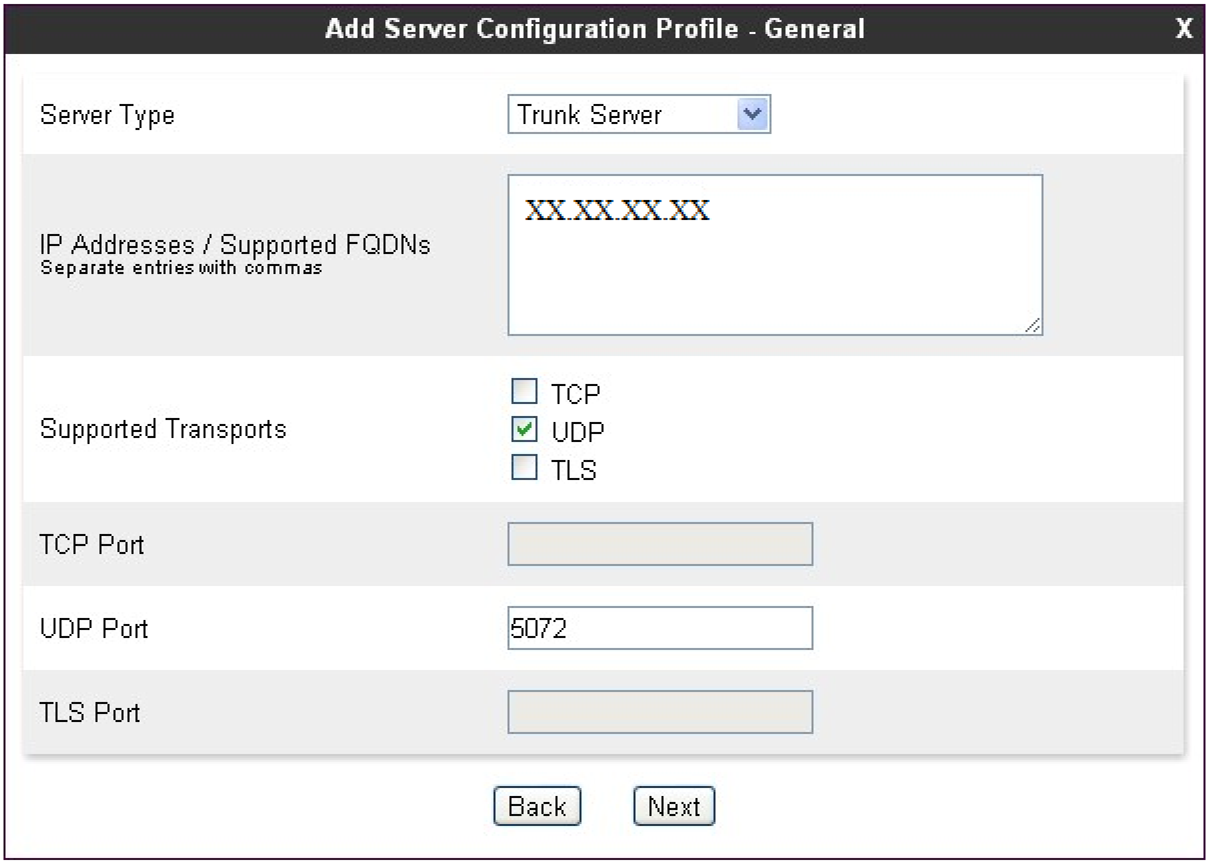
Note: If TCP was select as a protocol, then Selecting **Enable Grooming** is recommended.

6.4.2. Server Configuration - Verizon

To add a Server Configuration Profile for Verizon, navigate to **Global Profiles → Server Configuration** and click **Add**. Enter a descriptive name for the **Profile Name** and click **Next**.

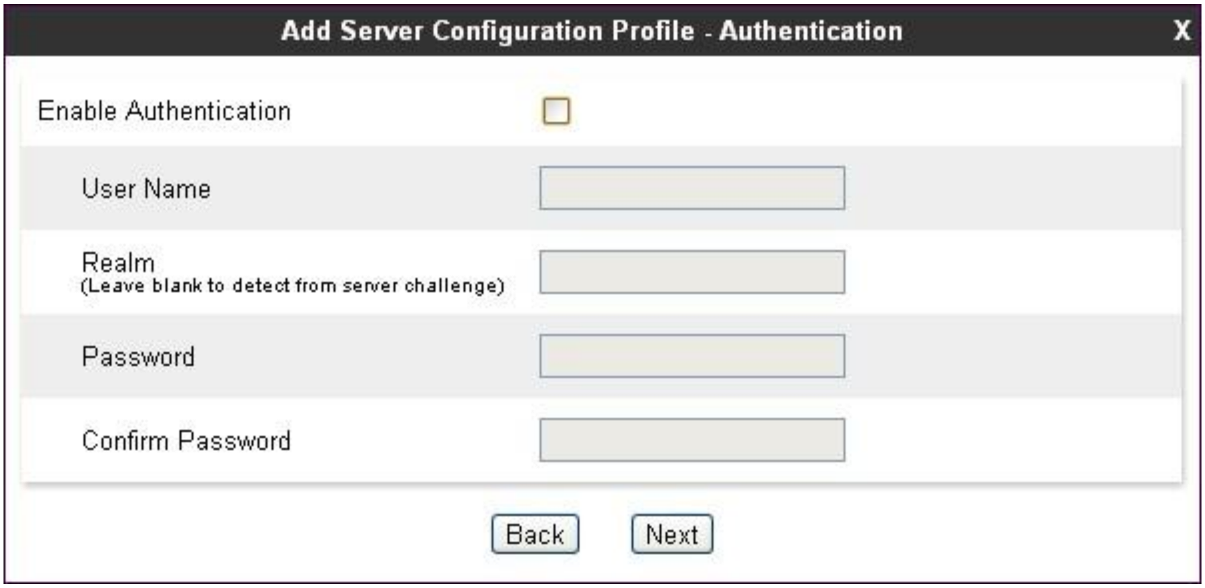


The following screens illustrate the Server Configuration for the Profile name "TrunkServer1". In the **General** parameters, select "Trunk Server" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Verizon-provided IP address is entered. In the sample configuration this is "XX.XX.XX.XX". In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to "5072". Click **Next** to continue. The actual values provided by Verizon should be used.

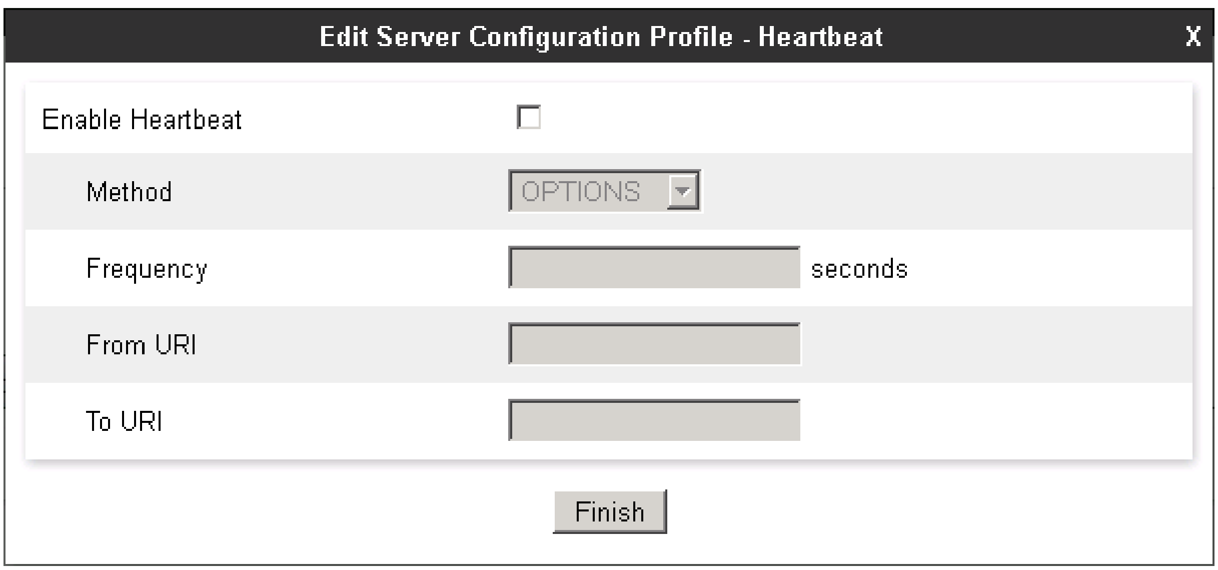


Note: The above configurations are as per the Server configuration profile in Avaya session border controller with Verizon Test trunk Service with Transport and port number based on the provider. Above values shall be modified based on the field service provider and deployment requirements.

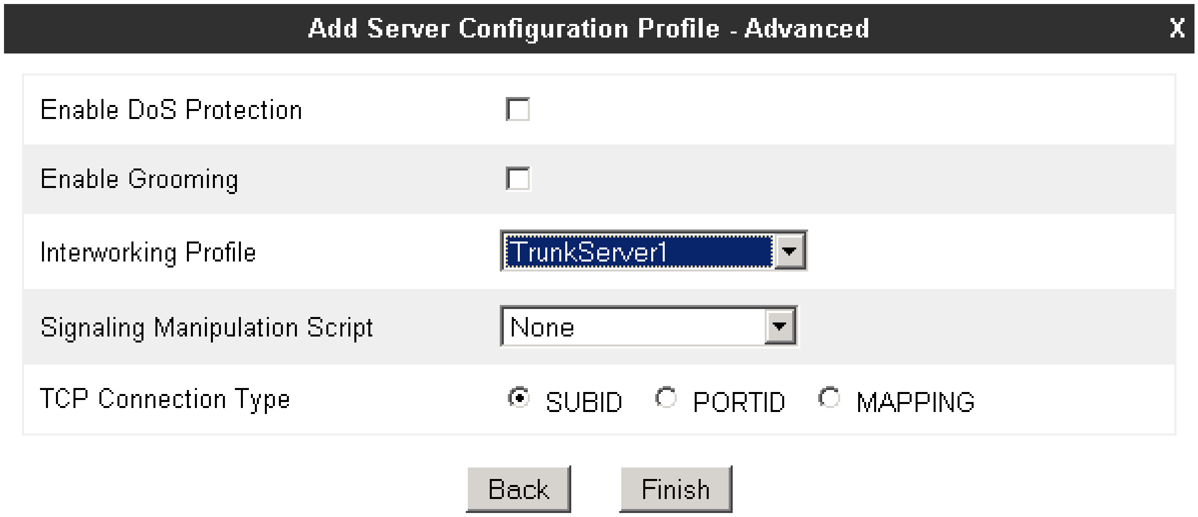
Verify **Enable Authentication** is unchecked as Verizon does not require authentication. If the service provider used in the deployment requires Authentication this needs to be enabled and appropriate values are expected to be configured. Click **Next** to continue.



Click **Next** to continue.



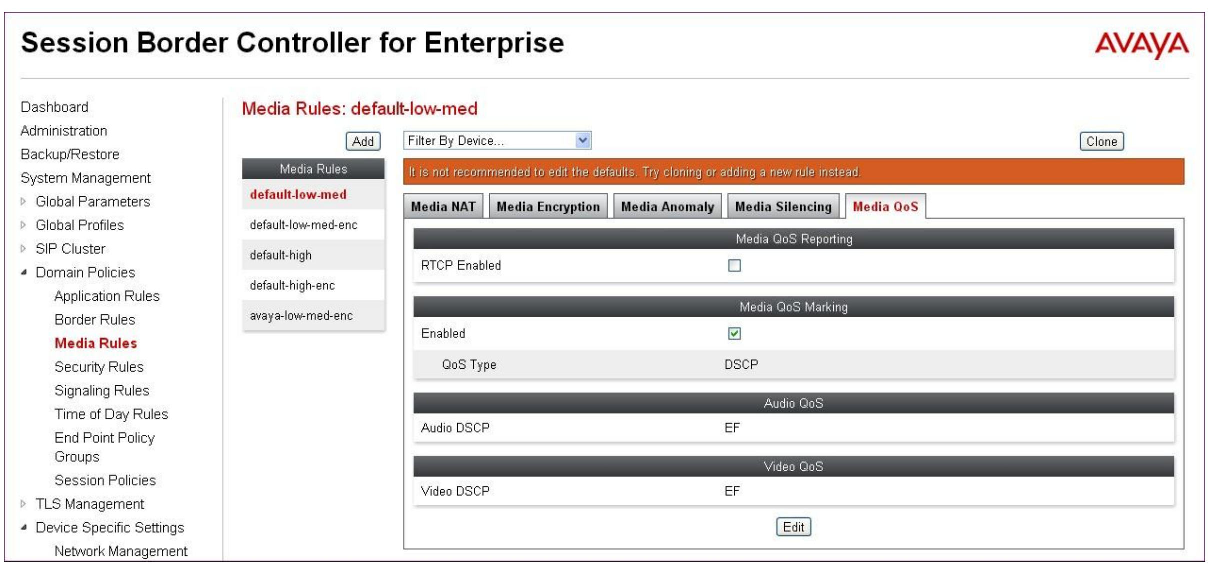
In the new window that appears, select the **Interworking Profile** "Trunkserver1" created previously in Section 6.3.2. Use default values for all remaining fields. Click **Finish** to save the configuration.



6.5. Media Rule

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

Select **Domain Policies → Media Rules** from the left-side menu as shown below. In the sample configuration, a single default media rule "default-low-med" was used with the **Audio and Video DSCP** values "EF" (**E**xpedited **F**orwarding) set for **Media QoS** as shown below.



Note: QOS Bit marking is not mandatory and can be disabled. If QOS Bit marking is required the above procedure can be used to achieve the requirement.

6.6. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

The "default" signaling rule can be used for Verizon and Cisco Unified Communications Manager.

6.7. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. In the sample configuration, a single default application rule "default" was used. For field deployment create an application rule with the concurrent sessions purchased (not shown).

6.8. Endpoint Policy Groups

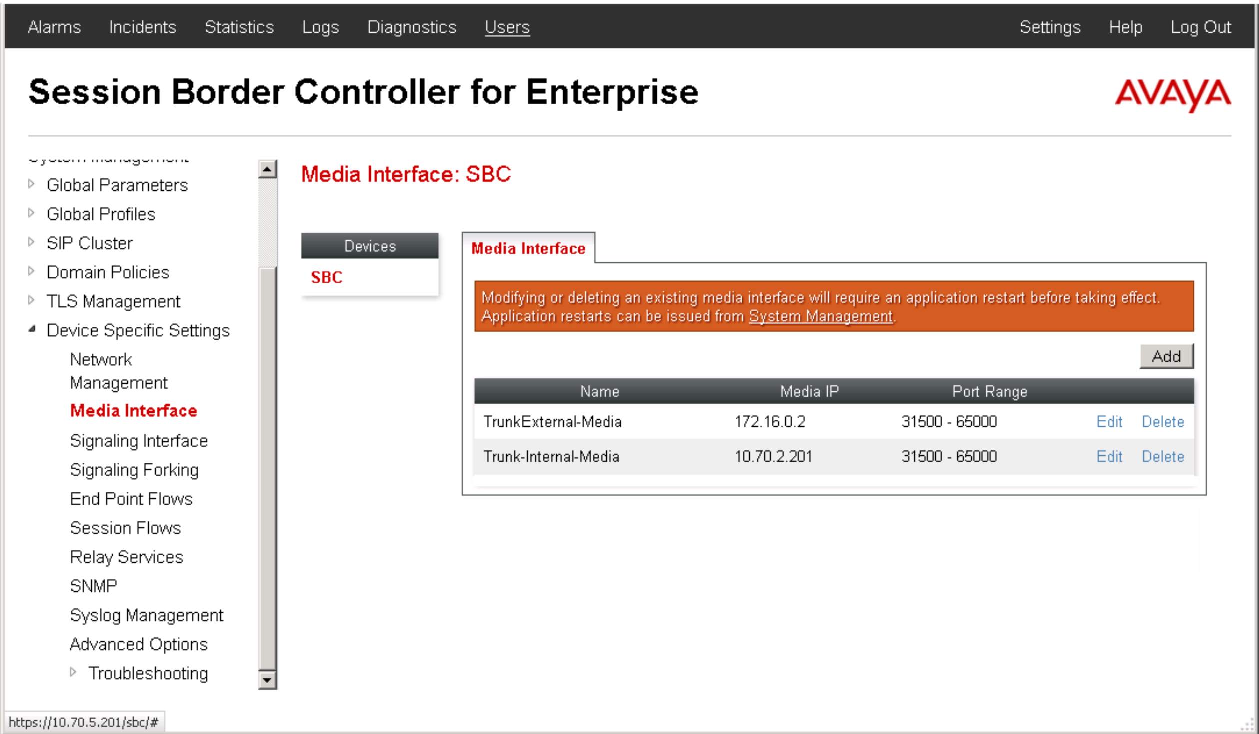
The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in Section 6.11.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** (not shown)**.** The "default-low" predefined Endpoint Policy Group was used for both Cisco Unified Communications Manager and Verizon in section 6.11.

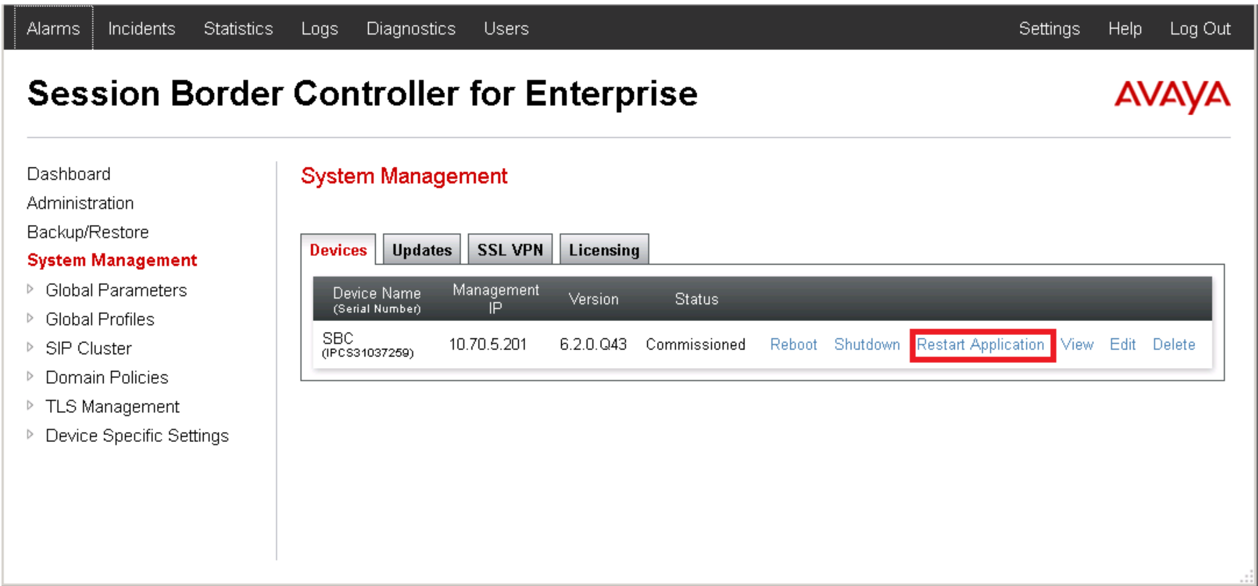
6.9. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP media interface for the inside and outside IP interfaces.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**. The following screen shows the media interfaces defined for the sample configuration.



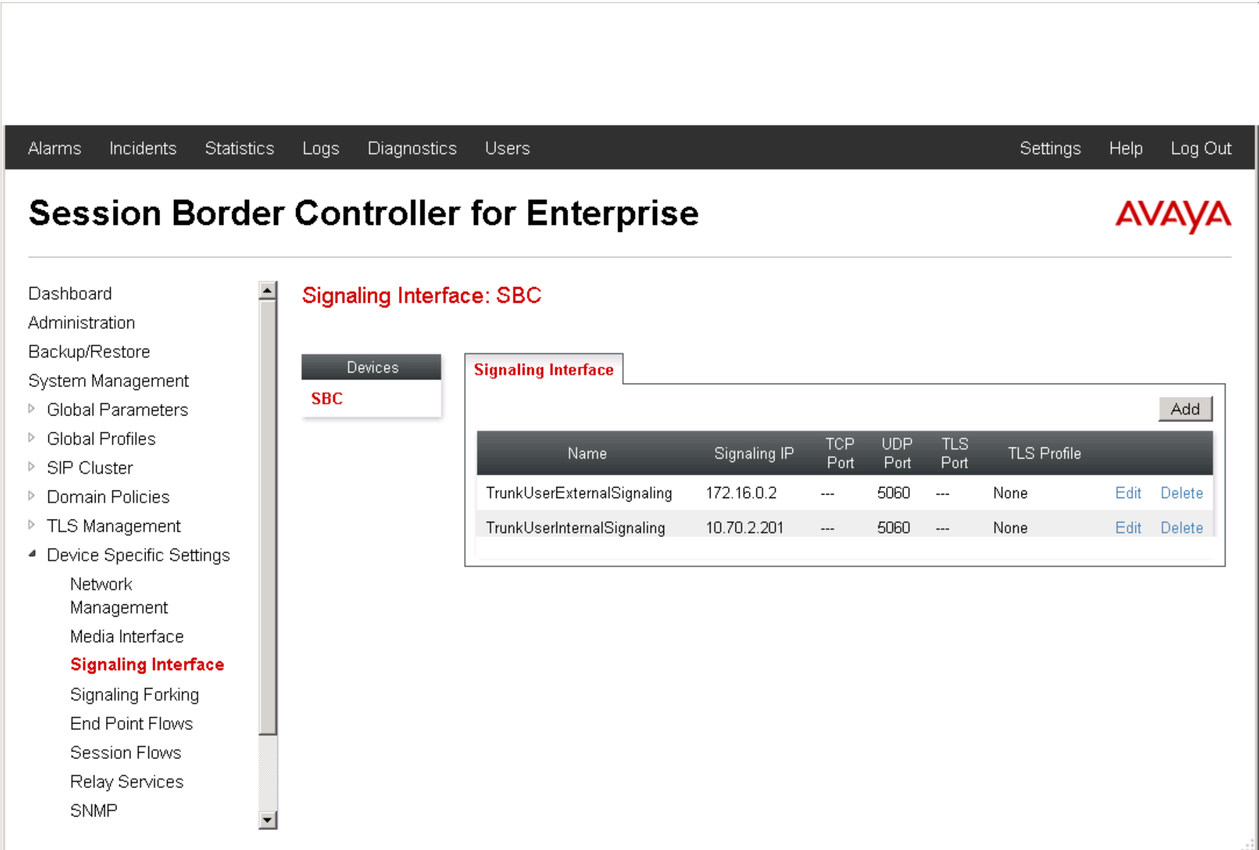
When the media interfaces are modified, an application restart is necessary before the changes will take effect. Navigate to **System Management** and click **Restart Application** as highlighted below.



6.10. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**. The following screen shows the signaling interfaces defined for the sample configuration.



Note: TCP and/or UDP can be used for configuration as required for deployment.

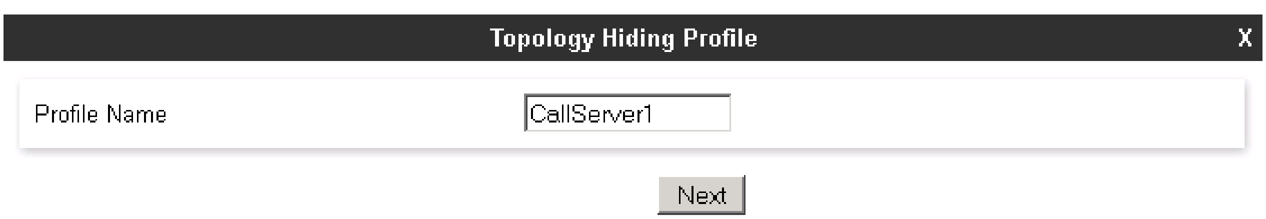
6.11. Topology Hiding

Topology hiding allows manipulating the Request-Line, FROM, TO, RECORD-ROUTE, VIA headers and SDP.

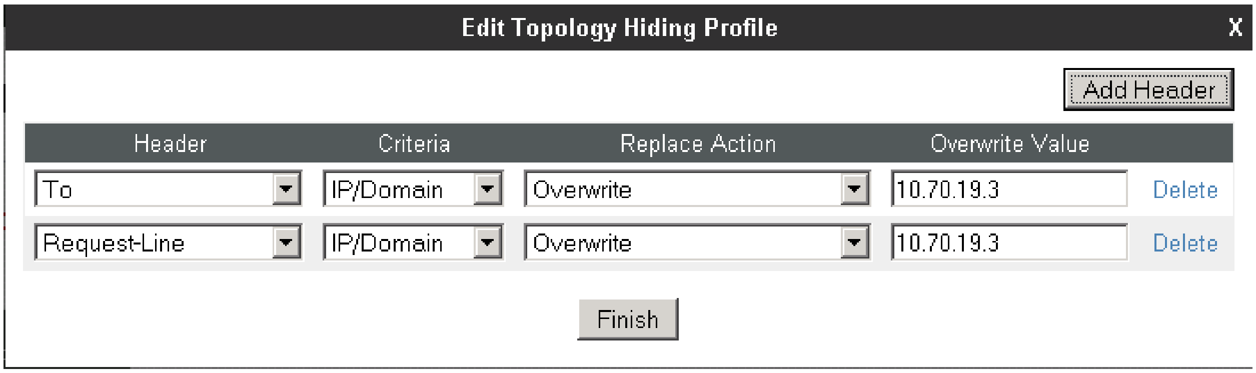
6.11.1. Topology Hiding – Cisco Unified Communications Manager

A topology profile is created to manipulate URI to match CUCM domain/IP.

Go to **Global Profiles-> Topology hiding**. Click the **Add** button. Enter a profile name. Click the **Next** button.



Make sure that the **Request-Line** and **TO** headers are added. Select Overwrite as the “Replace Action” for both headers. Enter the FQDN/IP of the CUCM the “Overwrite Value”. Click the **Finish** button. In our example the CUCM IP address is 10.70.19.3.



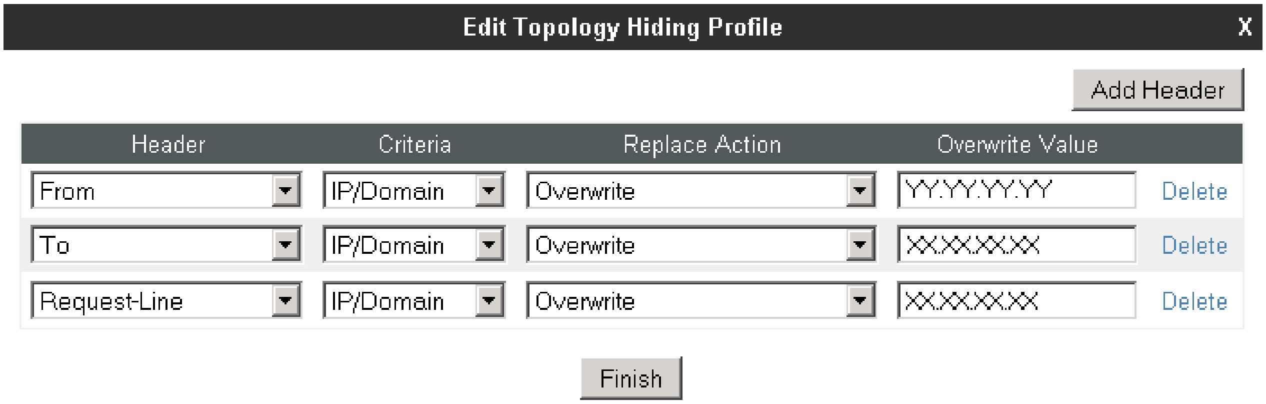
Note: Overwrite action is used as an example setting which solved the purpose in this test environment. Options under Replace Action shall be used based on the field requirement to achieve required action.

6.11.2. Topology Hiding - Verizon

A topology profile is created to manipulate URI to match the Public NATted IP.

Go to **Global Profiles-> Topology hiding**. Click the **Add** button. Enter a profile name. Click the **Next** button.

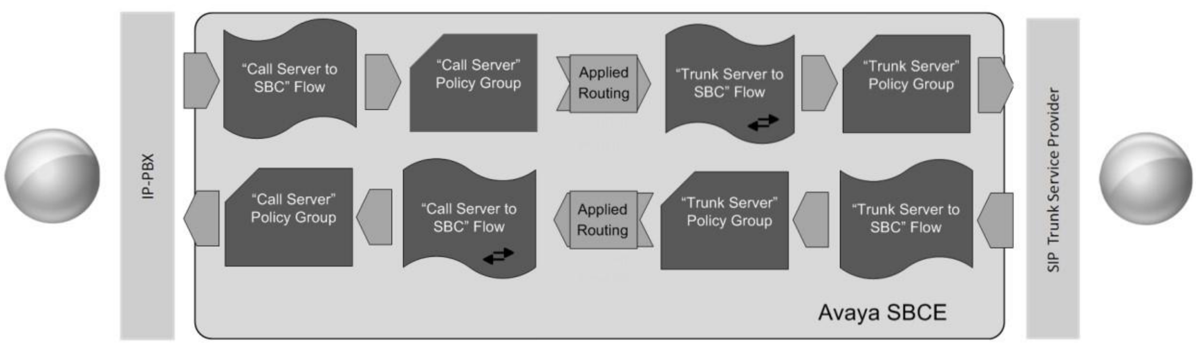
Make sure that the **Request-Line** and **TO** headers are added. Select Overwrite as the **Replace Action** for both headers. Enter the public IP of the Firewall **Overwrite Value**. Add the **FROM** header. Select Overwrite as the **Replace Action.** Enter the IP address of Verizon SIP service. Click the **Finish** button. In our example the Public IP address is shown as XX.XX.XX.XX. Enter the NATted public IP of the SBC. Also, Verizon SIP service IP is represented by YY.YY.YY.YY. In here apply the IP address given by Verizon.



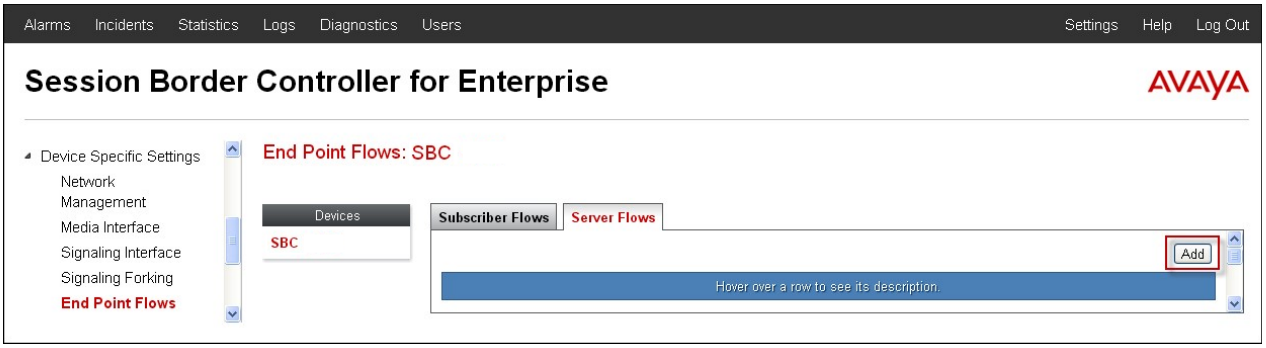
Note: Overwrite action is used as an example setting which solved the purpose in this test environment. Options under Replace Action shall be used based on the field requirement to achieve required action.

6.12. End Point Flows - Server Flow

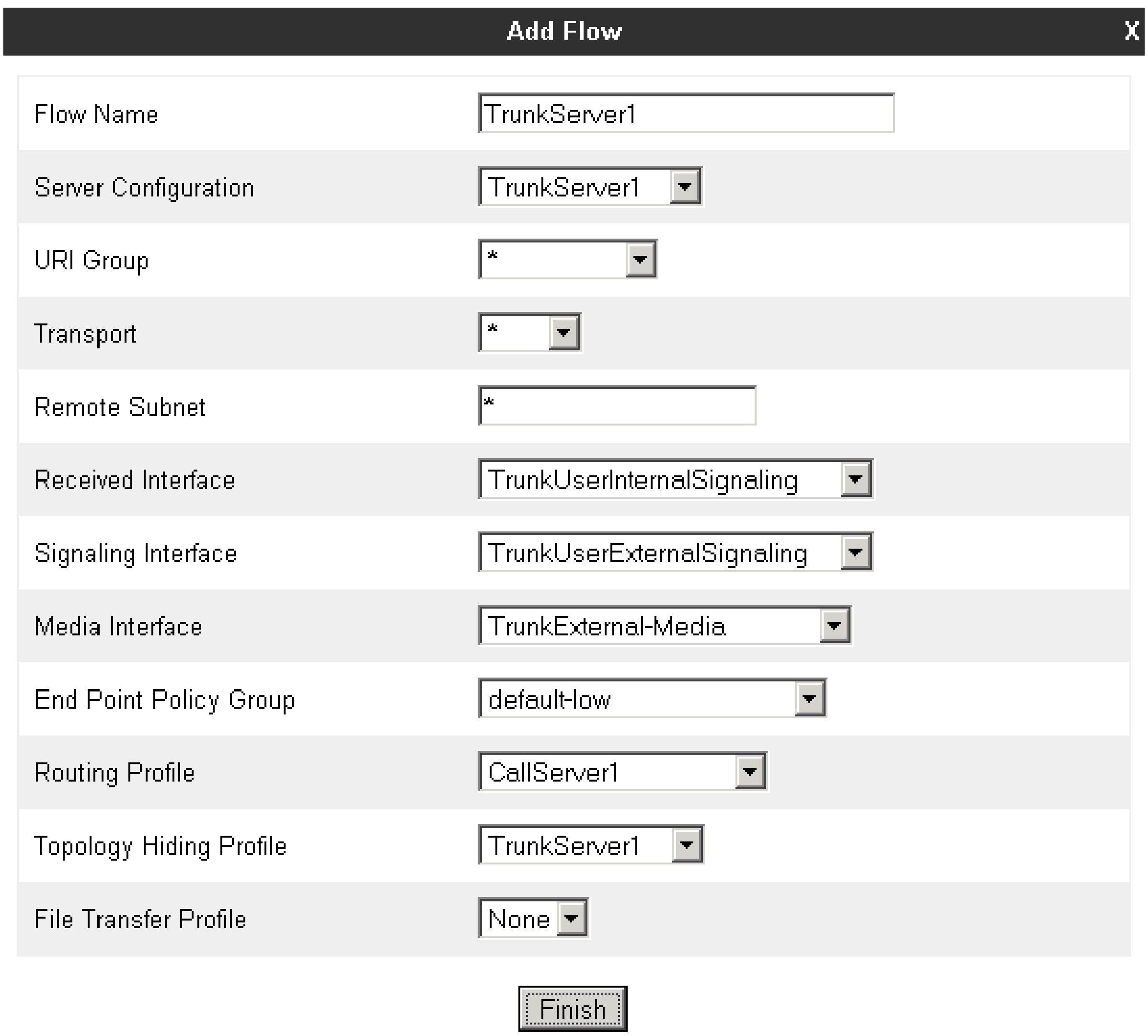
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the SBCE to secure a SIP Trunk call.



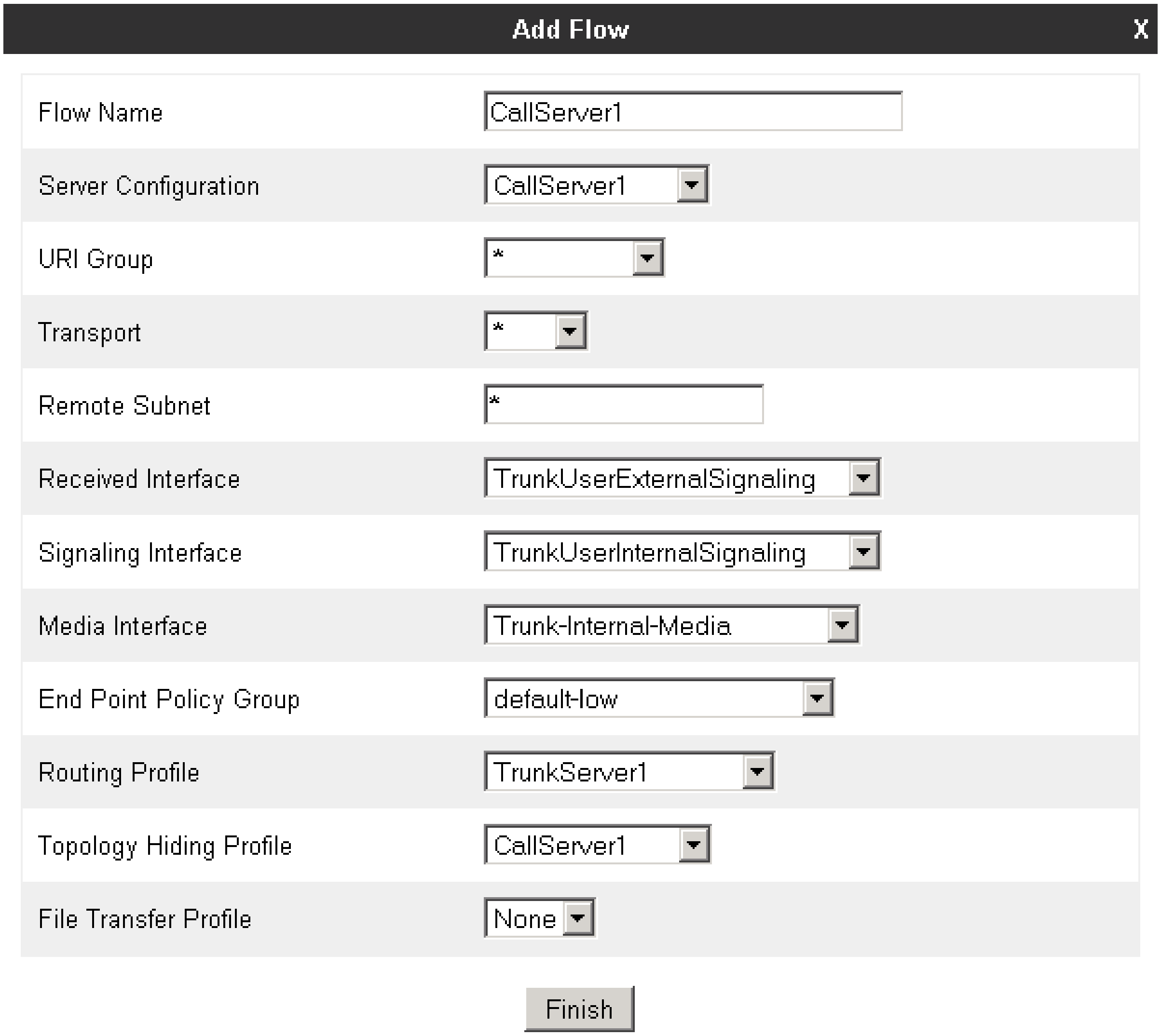
To create a Server Flow for Cisco Unified Communications Manager and Verizon Business IP Contact Center SIP Trunk service, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** as highlighted below.



The following screen shows the flow named "TrunkServer1" configured in the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections. Click **Finish**.



Similarly, “CallServer1” was configured in this sample configuration as shown below.



7. Verizon Business Configuration

Information regarding Verizon Business SIP Trunking service offer can be found by contacting a Verizon Business sales representative, or by visiting http://www.verizonenterprise.com/solutions/public_sector/federal/contracts/wits3/products/voice/voip_trunking.xml

The configuration described in these Application Notes was located in the Tekvizion Labs. The Verizon Business SIP Trunking service was accessed via a Verizon Lab VPN connection as described in Figure 1. Verizon Business provided the necessary service provisioning, for the Cisco Unified Communications Manager location.

For service provisioning, Verizon will require the customer IP address of the Data firewall in front of the Avaya Session Border Controller for Enterprise. Verizon provided the following information for the interoperability testing: the IP address and port used by the Verizon Server, and the numbers. This information was used to complete the configuration for Avaya Session Border Controller for Enterprise shown in Section 6 and the Cisco Unified Communications Manager shown in Section 5.

8. Verification

This section provides example verifications of the Avaya configuration with Verizon Business SIP Trunking service.

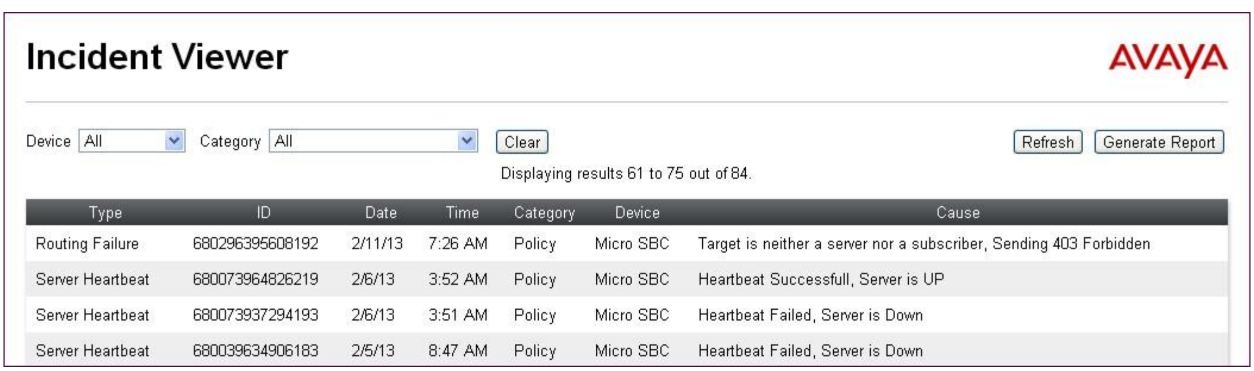
8.1. Avaya SBCE

This section provides verification steps that may be performed with the Avaya SBCE.

8.1.1. Incidents

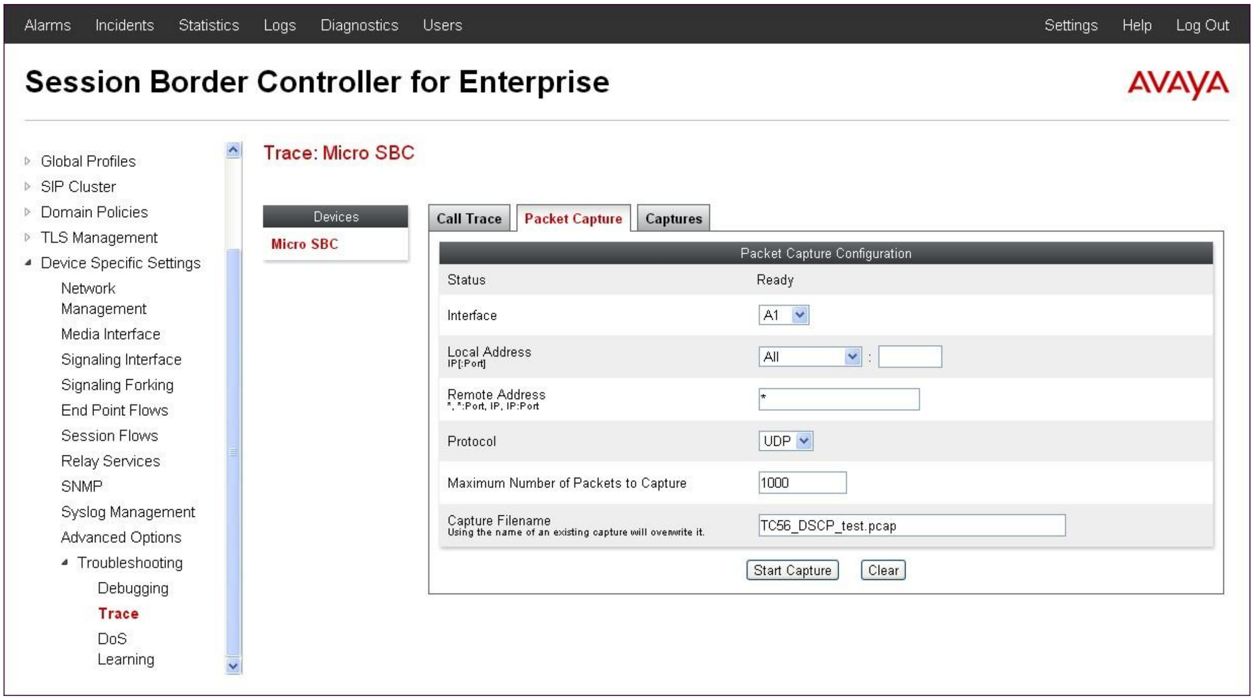
The Incident Viewer can be accessed from the Avaya SBCE Dashboard as highlighted in the screen shot below.

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.

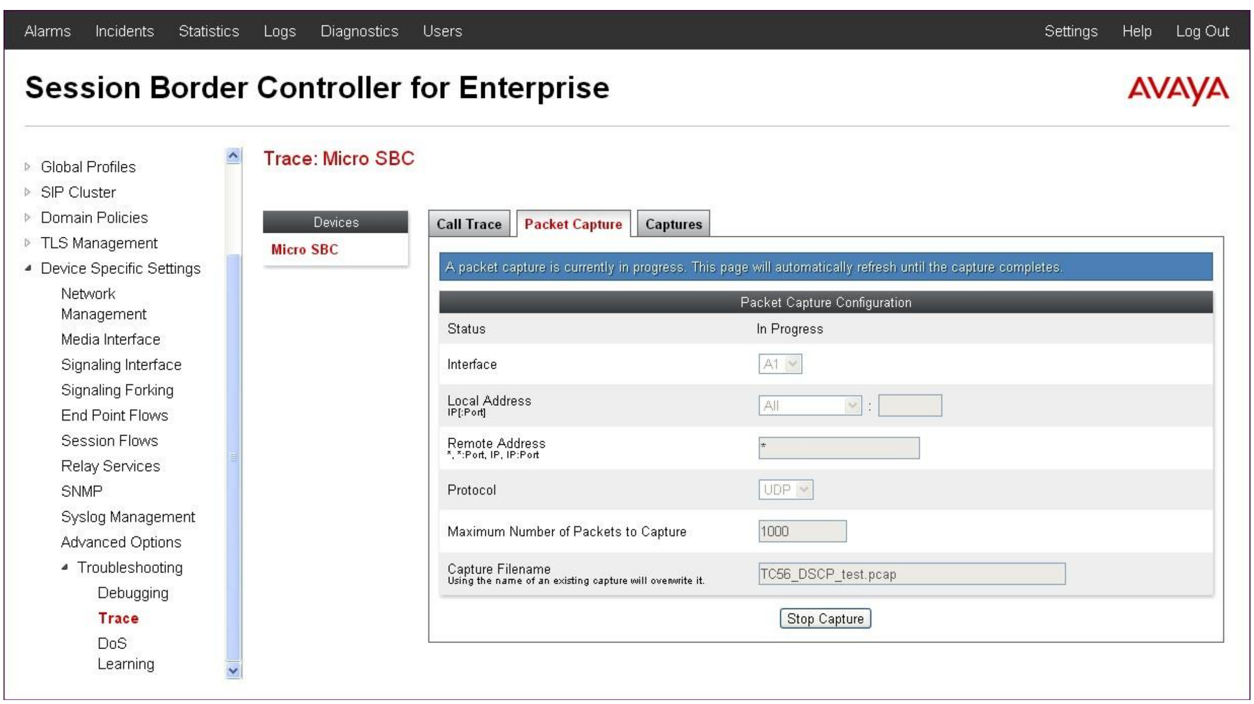


8.1.2. Tracing

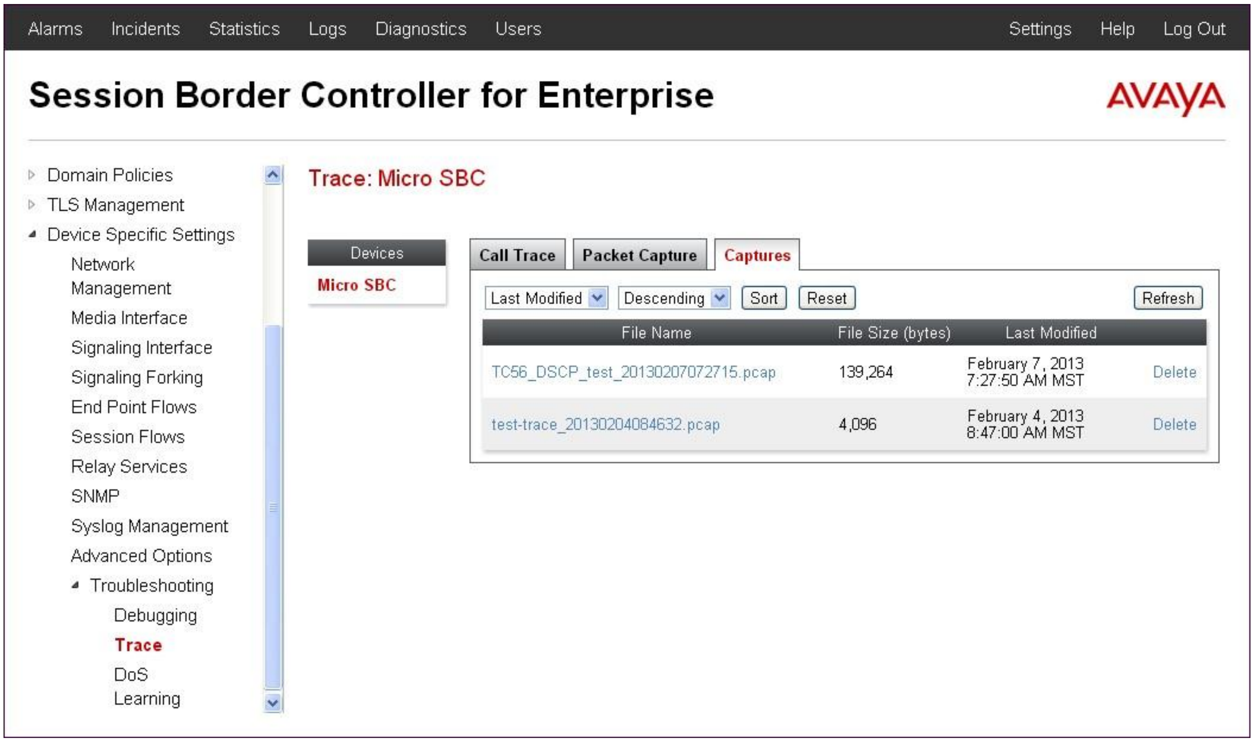
To take a call trace, navigate to **Device Specific Settings → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



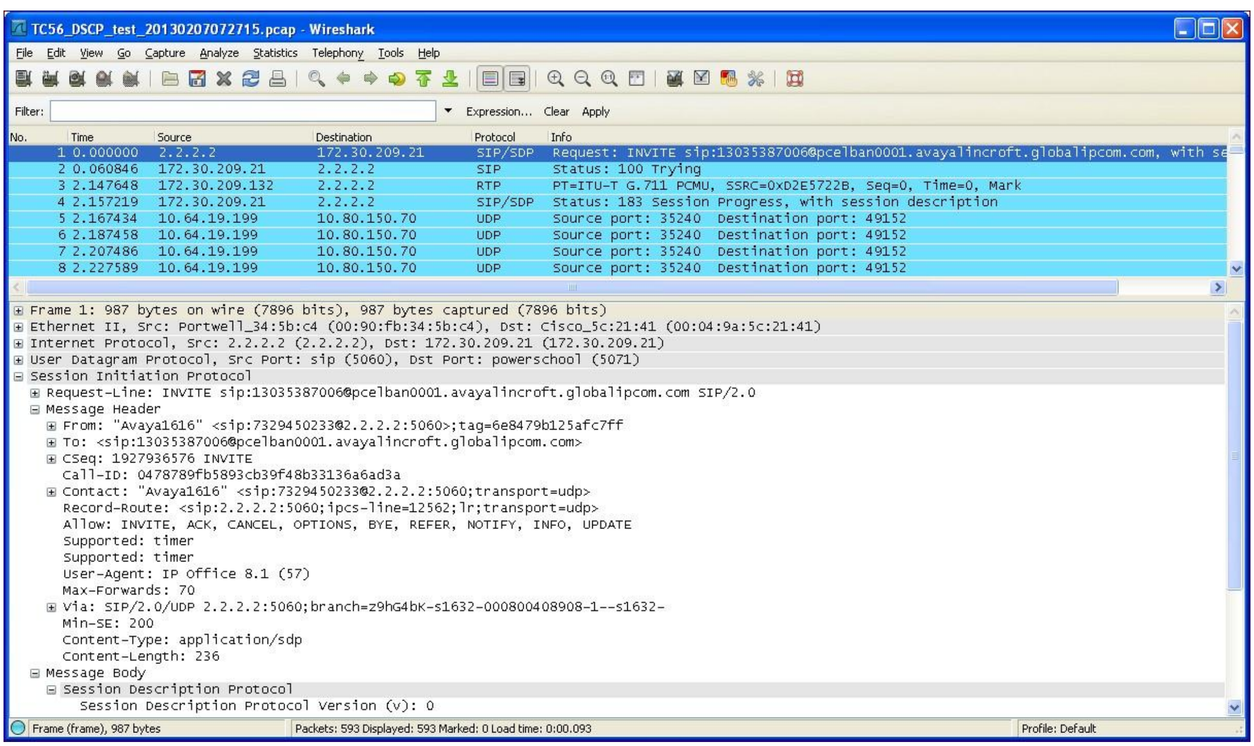
When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.



Select the **Captures** tab to view the files created during the packet capture.



The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like WireShark.



8.2. Cisco Unified Communications Manager

This section provides verification steps that may be performed with the Cisco Unified Communications Manager.

8.2.1. Real-Time Monitoring Tool

The Cisco Real-Time Monitoring Tool application is used to monitor and troubleshoot Cisco Unified Communications Manager. Use Real-Time Monitoring Tool application to verify the state of the SIP trunk. For more information about Real-Time Monitoring Tool consult reference [4].

9. Conclusion

These Application Notes demonstrated how Avaya Session Border Controller for Enterprise Release 6.2 and Cisco Unified Communications Manager Release 9.1/8.6 can be successfully combined with a Verizon Business SIP Trunk service connection to enable a business to receive and send calls. Utilizing this solution, Cisco Unified Communications Manager customers can leverage the operational efficiencies and cost savings associated with SIP trunking while gaining the advanced technical features provided through the marriage of best of breed technologies from Avaya and Verizon.

Cisco Unified Communications Manager Release 9.1/8.6 with Avaya Session Border Controller for Enterprise Release 6.2 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.

10. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at http://support.avaya.com

[1] *Installing Cisco Unified Communications Manager, Release 9.1(1)* , December 20, 2012

[2] *Cisco Unified Communications Manager Administration Guide, Release 9.1(1),* Text Part Number OL-27945-01, December 20 2012

[3] *Enterprise License Manager User Guide, Release 9.1(1),* Text Part Number OL-28579-01, June 18, 2013

[4] *Cisco Unified Real-Time Monitoring Tool Administration Guide*, Text Part Number OL-27838-01, December 20, 2012

[5] *Administering Avaya Session Border Controller*, Document Number 08-604063, Sept. 2012

The Application Notes referenced below correspond to the formal Interoperability testing by Tekvizion labs for Cisco Unified Communications Manager Release 9.1 with Verizon SIP Trunking and Avaya Service Session Border Controller for Enterprise 6.2.

[RFC-3261] RFC 3261 *SIP: Session Initiation Protocol* http://www.ietf.org/rfc/rfc3261.txt
[RFC-2833] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals* http://www.ietf.org/rfc/rfc2833.txt

Information in the following Verizon documents was also used for these Application Notes. Contact a Verizon Business Account Representative for additional information.

[VZ-Test-Plan] *Core Network Technology System Integration & Testing Voip Integration Testing Voip InteropLab*. Version 2.0. Document Number VIT.2010.03153.TPL.001 June 18, 2010