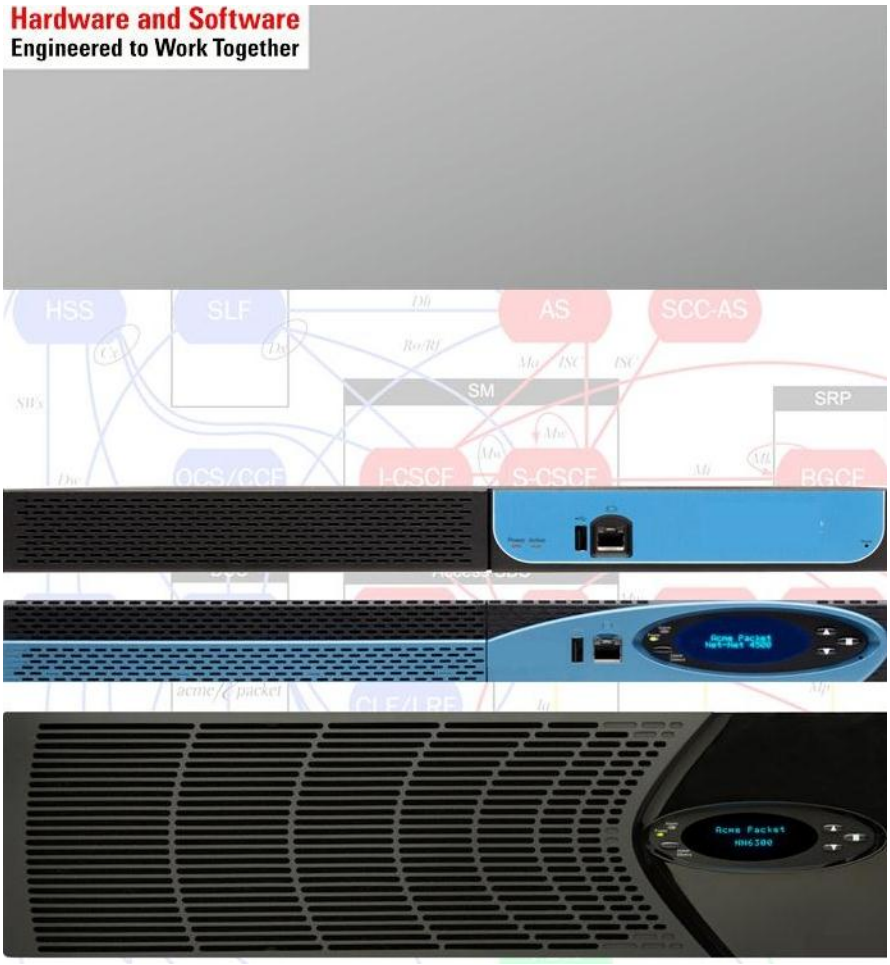


AT&T IP Flexible Reach with Enhanced Features Including MIS/PNT/AVPN Transports with Microsoft Lync 2013 & Acme Packet 3000-4000 Series SBC with Transcoding

A Technical Application Note

ORACLE

Microsoft Lync

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Abstract

This application note defines a SIP configuration model suitable for Oracle's Acme Packet 3000-4000 series session border controllers (SBCs) connecting Microsoft Lync 2013 from a customer premise to AT&T's IP Flexible Reach with Enhanced features service with MIS, PNT or AT&T Virtual Private Network (AVPN) transport. The reference configuration presented was tested in Oracle labs.

Introduction

This application note outlines the recommended configuration for the Acme Packet 3000-4000 series SBC (AKA Oracle Communications Session Border Controller), the industry leading Session Border Controllers, for connecting AT&T's IP Flexible Reach with Enhanced features service to Microsoft Lync customers. This document is applicable to Oracle's NNOS-C versions 6.3.7 stream of software only.

Intended Audience

This document is intended for use by Systems Engineers, Enterprise Customers and Partners. It assumes that the reader is familiar with basic operations of the Oracle Communications Session Border Controller.

Support

**The AT&T website is password protected. The ID and Password are provided to each customer when they place an order for IP Flexible Reach or IP Toll Free service.

Design goals

The reference configuration represents the most common SIP to SIP deployment models. Originating SIP traffic and terminating to a SIP provider via the Acme Packet series SBC. The configuration also supports bi-directional call-flows via Local-Policy routes.

This document will annotate each configuration with information on its general applicability. The intent is to:

- Minimize SIP to SIP interoperability issue's by standardizing field configurations
- Provide guidelines for new users for the Oracle Communications Session Border Controller
- Provide a configuration template, base-lining the SIP to SIP configuration (with accompanying Diagram)
- Flexibility: how resilient the configuration is and how adaptable the configuration is when turning up new SIP to SIP networks.
- Performance: minimize the use of unnecessary configuration objects

Limitations and Restrictions

The limitations and restrictions of this testing are as follows

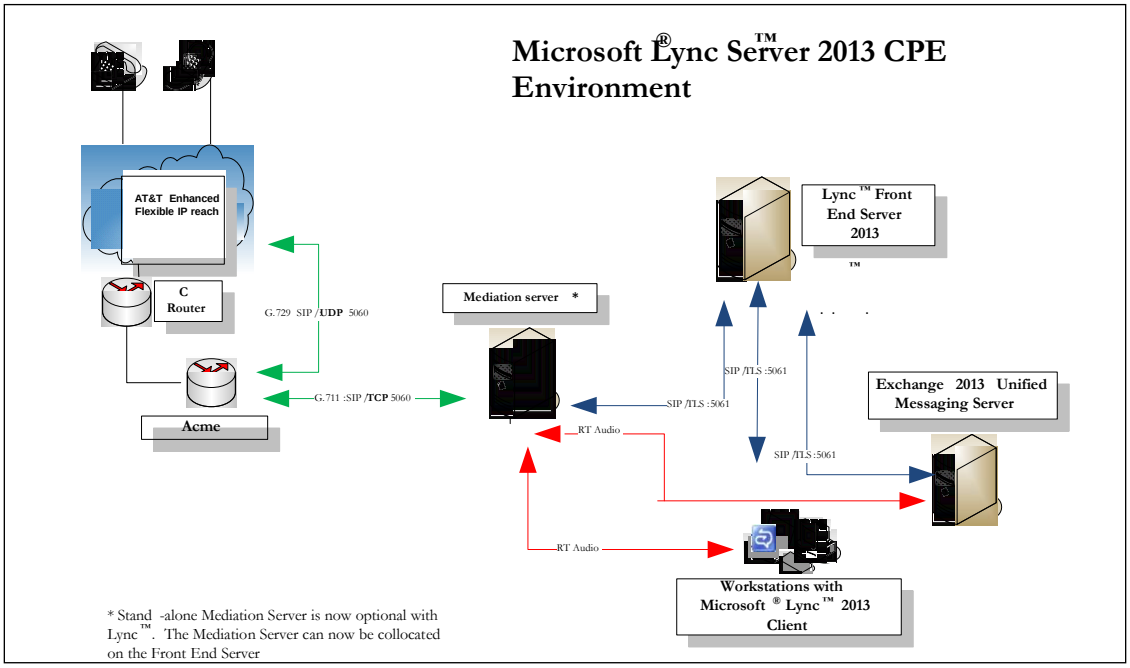
- DTMF does not work with ad hoc conference.
- The following AT&T IP Flexible Reach – Enhanced Features (IPFR-EF) features are not supported
    1. Network-based Call Forwarding – Busy and Call Forwarding – Not Reachable: Network based CFB and CFNR are not supported because Lync sends 183 sip messages before signaling non-reachable responses.
    2. Network-based Blind Call Transfer
       <Rueben please provide reason for no support on this feature>
- On ad hoc conference calls initiated by a Lync client and involving a hop-off endpoint (PSTN, IP Teleconference, IVR, etc.), Lync Mediation Server does not send a BYE when the Lync client(s) disconnect, resulting in a "hung call" with continuous RTP until the far end hangs up. This may result in long duration hung calls depending on endpoint time-outs or guard timers configured on the SBC.
- Call transfer and conference initiated by a Lync client are not supported on native IP calls to the AT&T IP Teleconferencing Service as DTMF is not supported.
- **With this configuration, RTCP reporting (RTCP sender and receiver reports) is not supported.** (Please refer to the section, Transcoding on page 56 for more information regarding the need for Transcoding and its configuration)
- **Emergency 911/E911 Services Limitations and Restrictions** - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.

While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when that E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

Reference Architecture

This section includes a reference architecture diagram, where the Acme Packet series SBC is integrated as an Enterprise CPE Trunking SBC, performing SIP between Microsoft Lync in the Enterprise and the AT&T Flexible Reach with Enhanced features service.

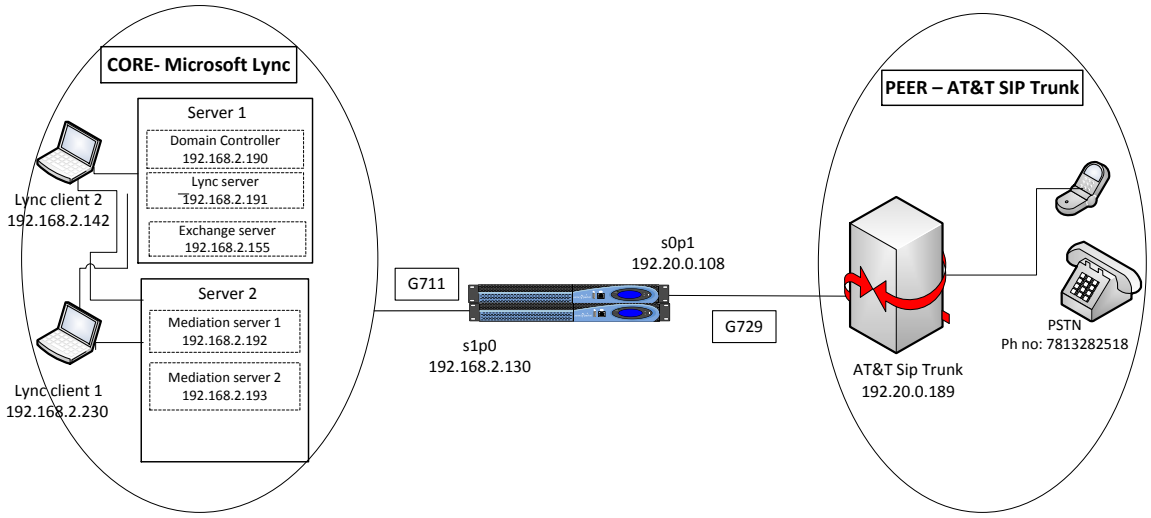
The MS mediation server peers with the AT&T IP Flexible Reach with Enhanced features service via the Acme Packet series SBC (as depicted below).



The Lync server Mediation server and the Acme Packet series SBC are the edge components that form the boundary of the SIP trunk. This document describes the configuration of the Lync server and the SBC and the results of the test plan.

Lab configuration:

The following diagram, similar to the Reference Architecture described earlier in this document, illustrates the lab environment created to facilitate certification testing:



Phase 1 - Lync 2013 configuration

The enterprise will have a fully functioning Lync Server infrastructure with Enterprise Voice deployed and a Mediation Server dedicated to this installation. If there is no Mediation Server present for this purpose, one will have to be deployed.

There are two parts for configuring Lync Server to operate with the Oracle Communications Session Border Controller:

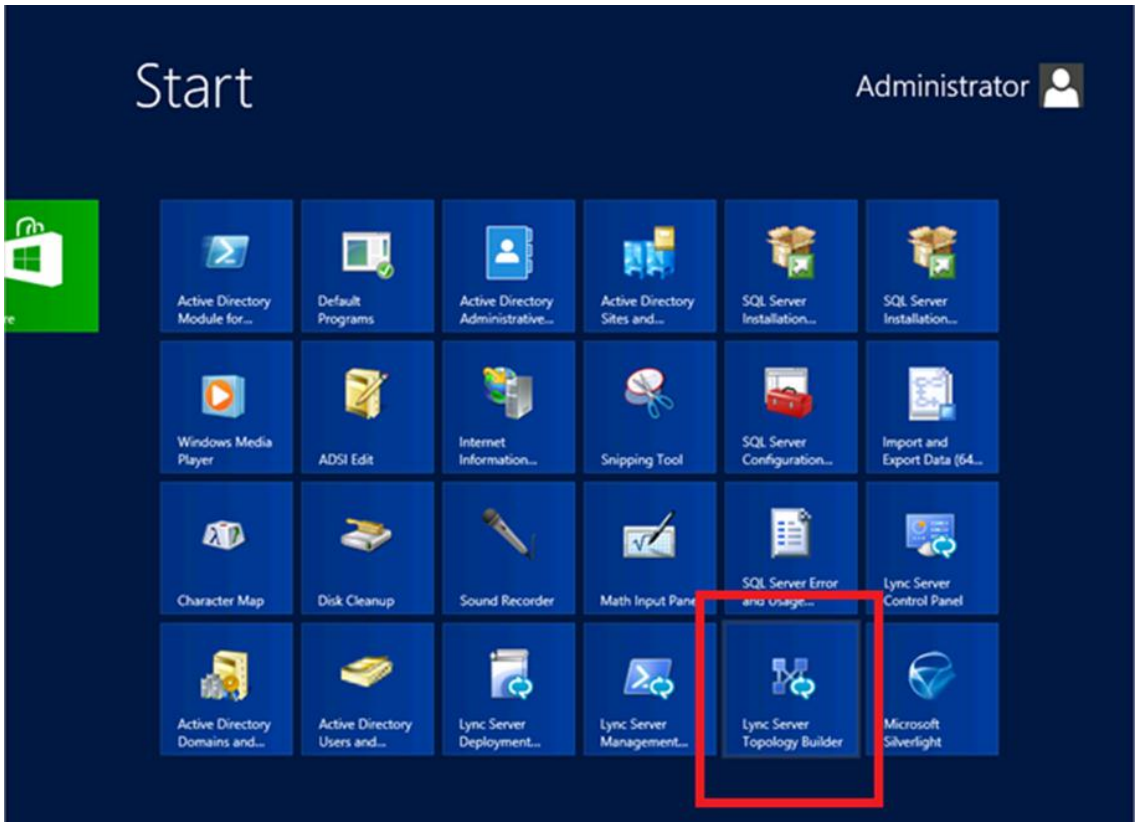
1. Adding the Oracle Communications Session Border Controller as a PSTN gateway to the Lync Server infrastructure; and
2. Creating a route within the Lync Server infrastructure to utilize the SIP trunk connected to the Oracle Communications Session Border Controller.

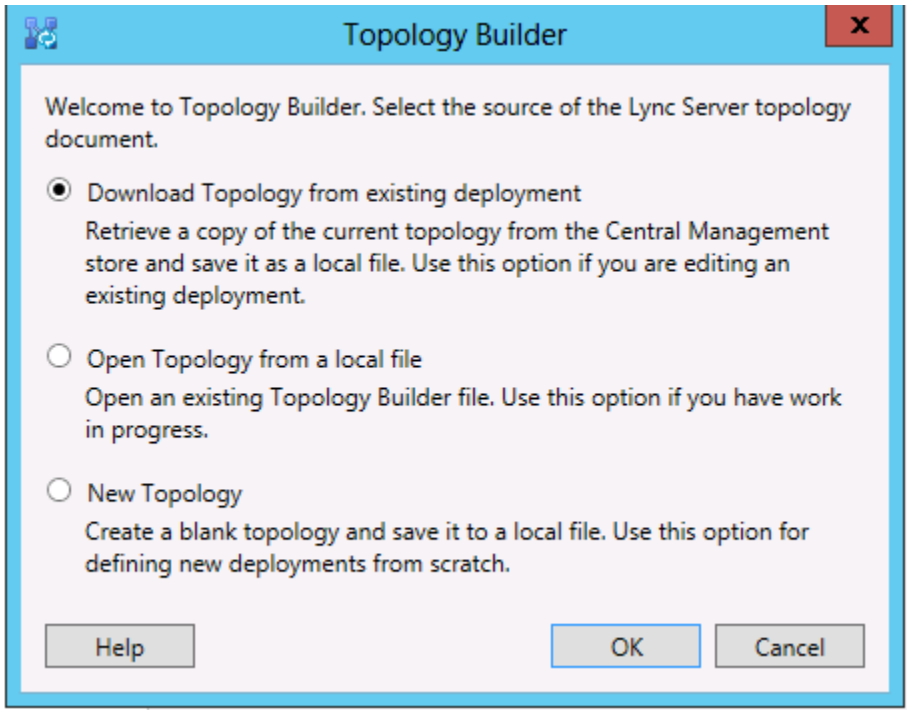
To add the PSTN gateway, we will need:

- IP addresses of the external facing NICs of the Mediation Servers
- IP address of the Oracle Communications Session Border Controller external facing port
- Rights to administer Lync Server Topology Builder
- Access to the Lync Server Topology Builder

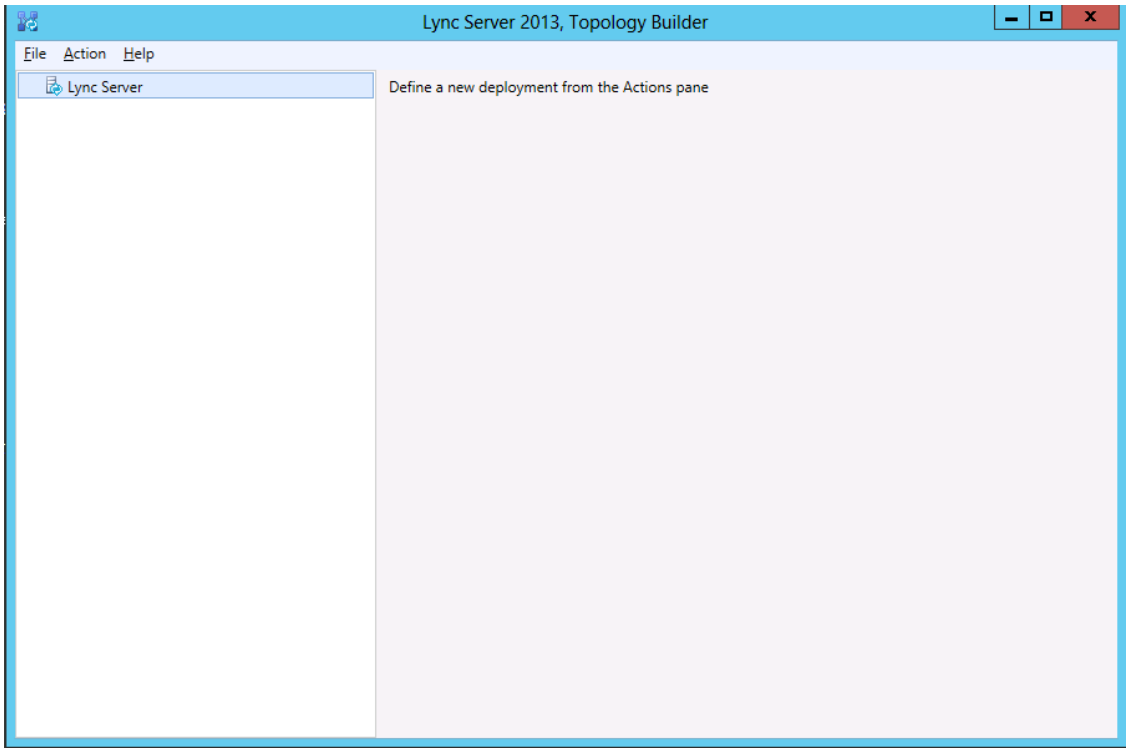
Steps to add the PSTN gateway

1. On the server where the Topology Builder is located start the console.
2. From the **Start** bar, select **Lync Server Topology Builder**

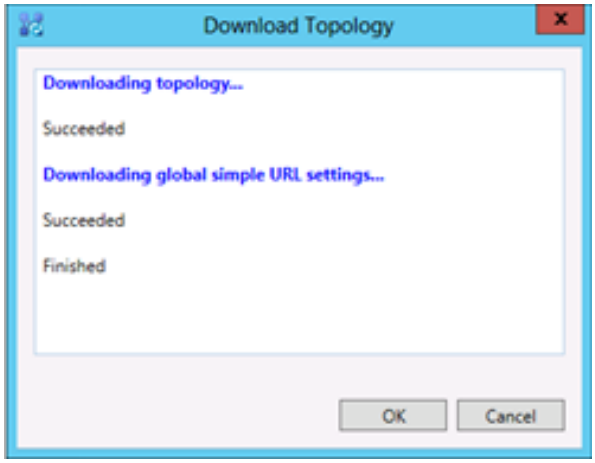

Start
Administrator
Active Directory Module for...
Default Programs
Active Directory Administrative...
Active Directory Sites and...
SQL Server Installation...
SQL Server Installation...
Windows Media Player
ADSI Edit
Internet Information...
Snipping Tool
SQL Server Configuration...
Import and Export Data (64...
Character Map
Disk Cleanup
Sound Recorder
Math Input Panel
SQL Server Error and Usage...
Lync Server Control Panel
Active Directory Domains and...
Active Directory Users and...
Lync Server Deployment...
Lync Server Management...
Lync Server Topology Builder
Microsoft Silverlight


Topology Builder
Welcome to Topology Builder. Select the source of the Lync Server topology document.
Download Topology from existing deployment
Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.
Open Topology from a local file
Open an existing Topology Builder file. Use this option if you have work in progress.
New Topology
Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.
Help
OK
Cancel

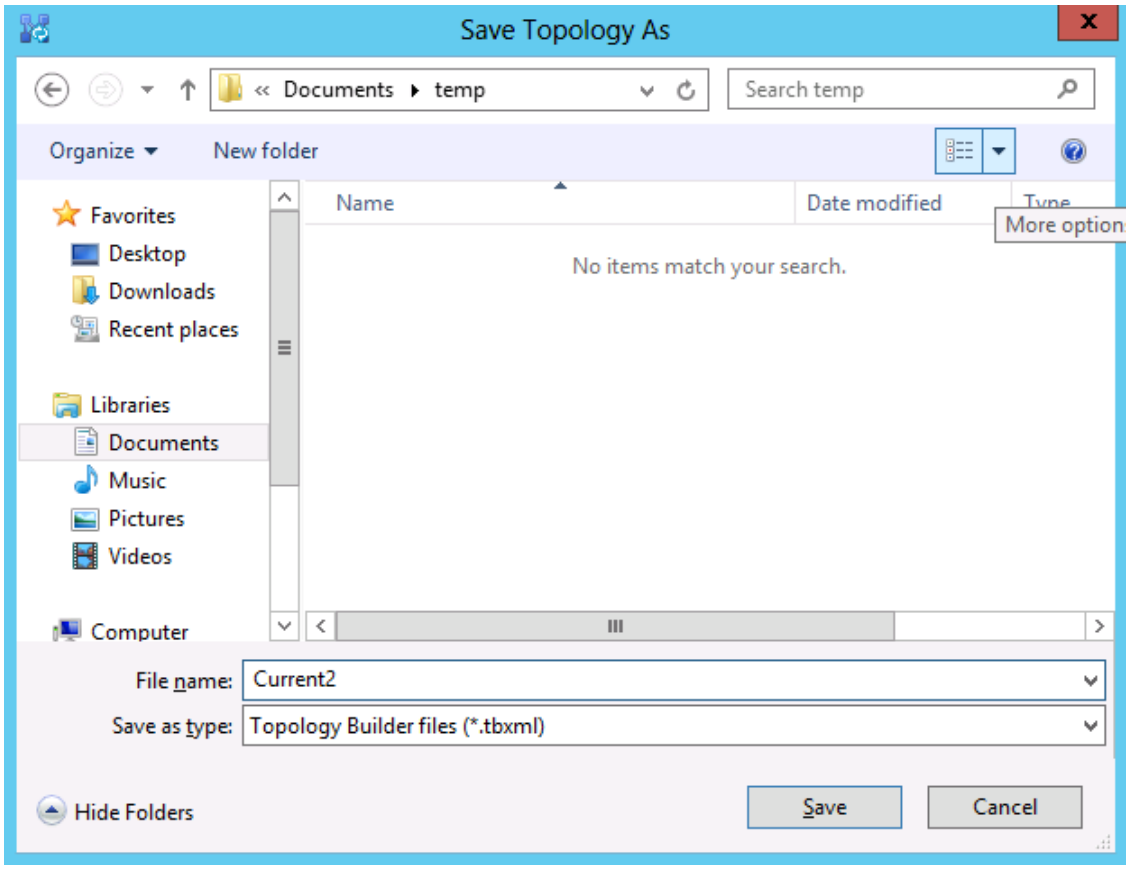
3. You will now be at the opening screen in the Topology builder.
4. Click on the **Cancel** button.



5. Click on Action and select **Download Topology**

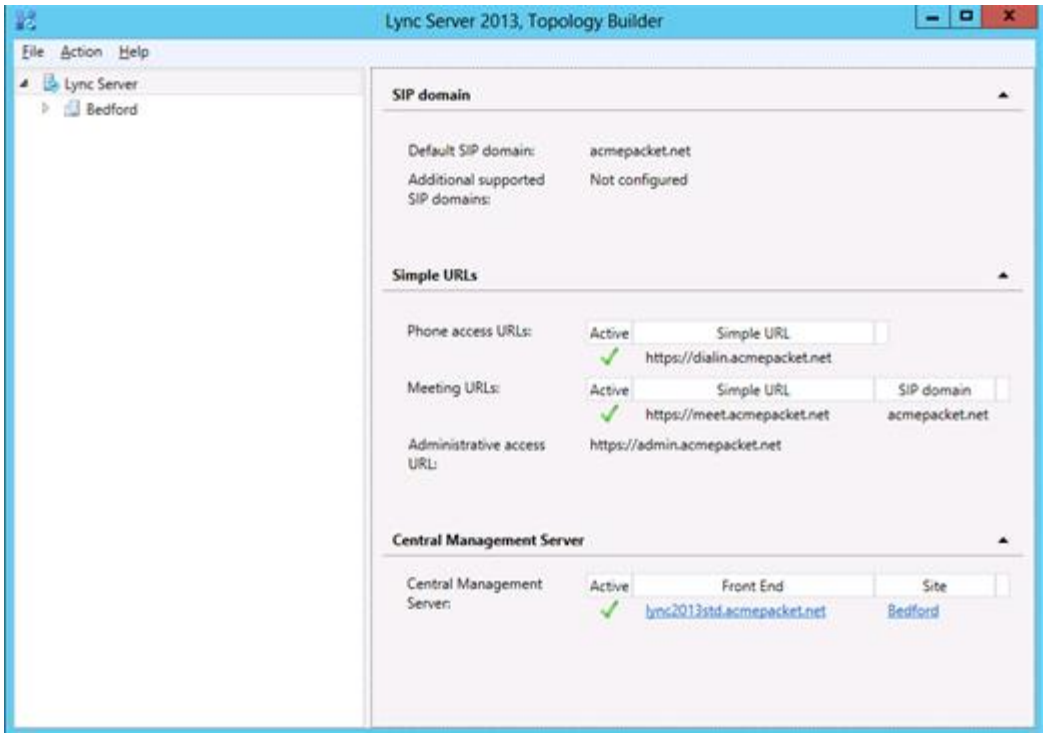


6. You will then see a screen showing that you have successfully imported the topology. Click the **Ok** button.

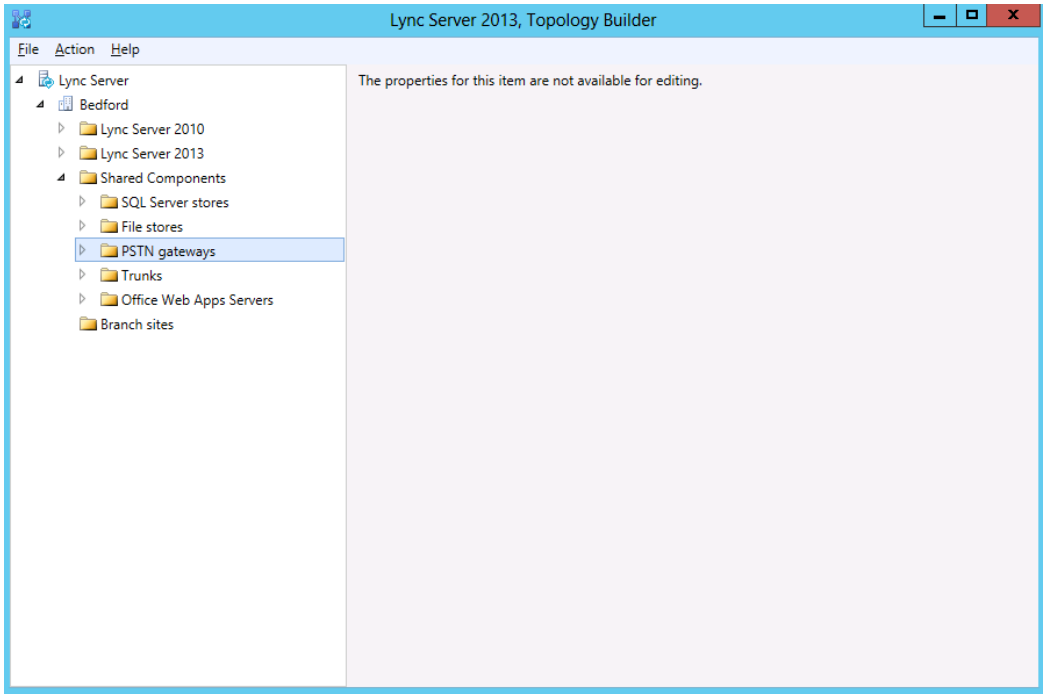


7. Next you will be prompted to save the topology which you have imported.
8. You should revision the name or number of the topology according to the standards used within the enterprise.
   Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make during this installation.
9. Click the **Save** button.

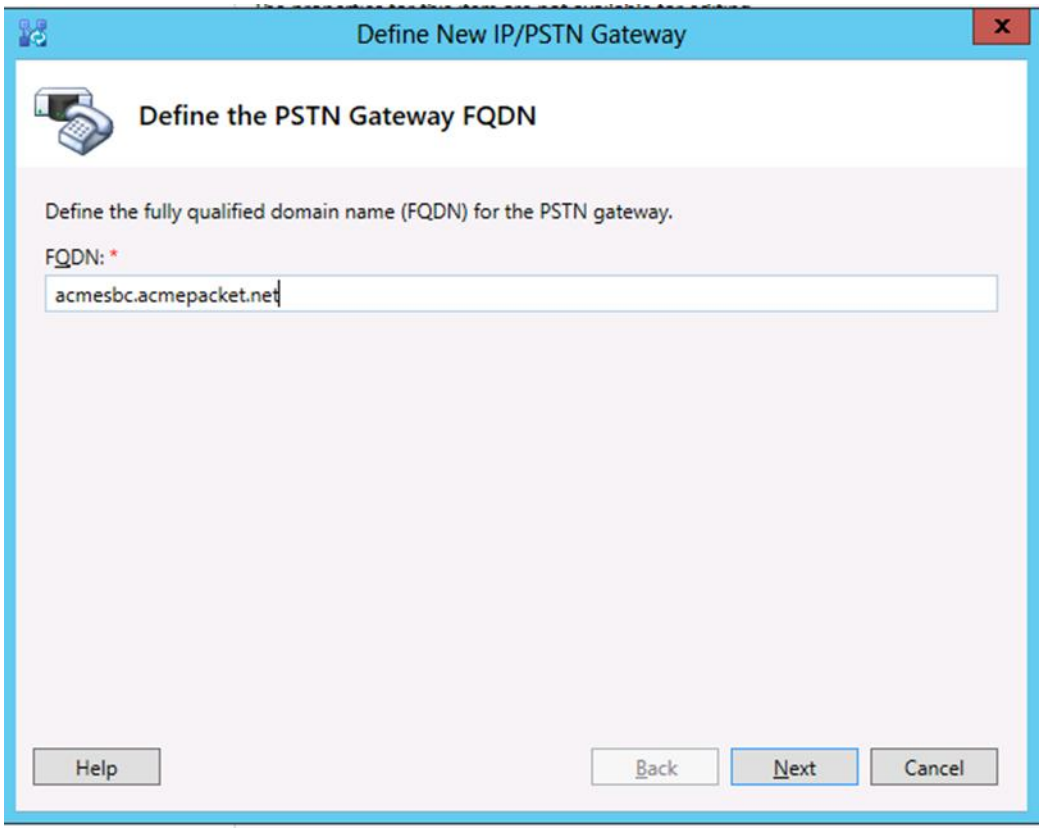
You will now see the topology builder screen with the enterprise's topology imported.

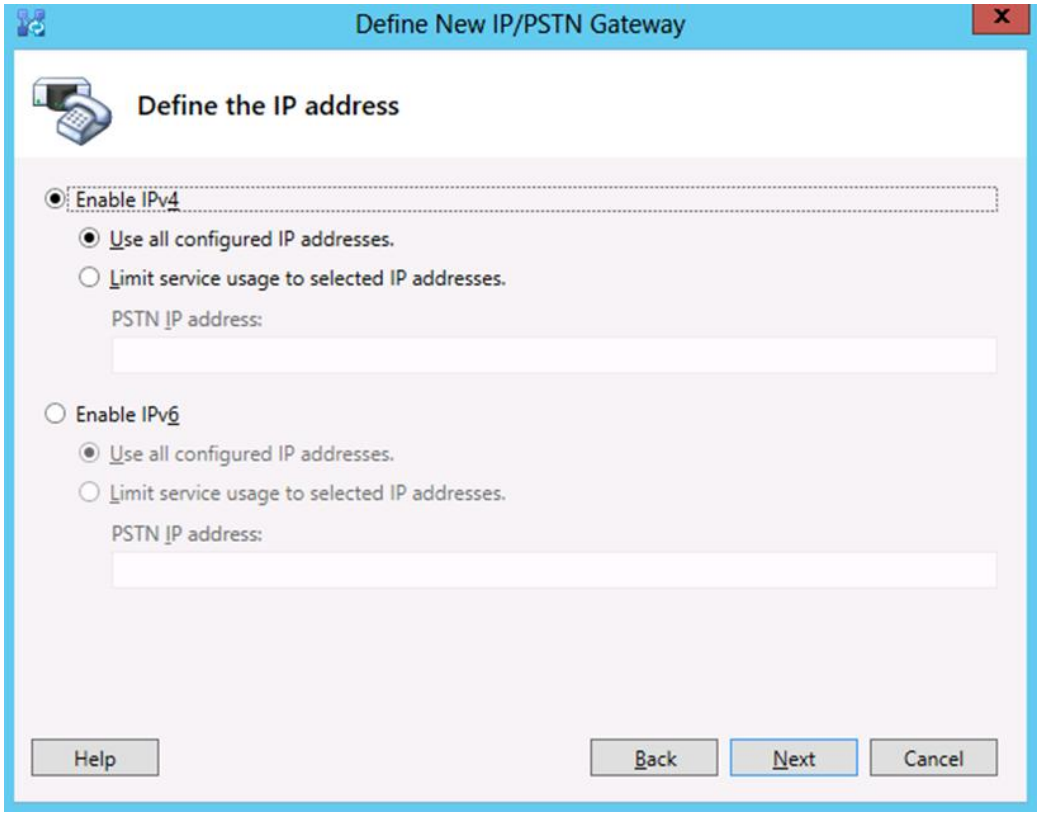


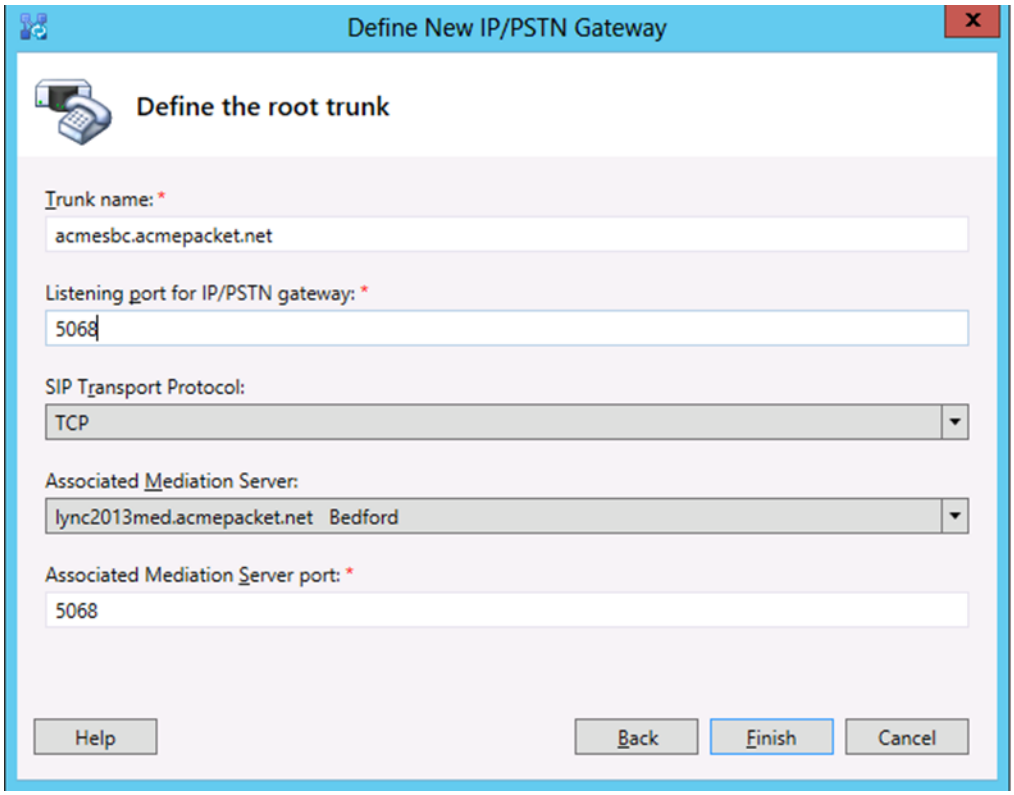
10. In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is **Bedford**. Then click on the **PSTN Gateways**.



11. Right click on PSTN Gateways and select New PSTN Gateway.

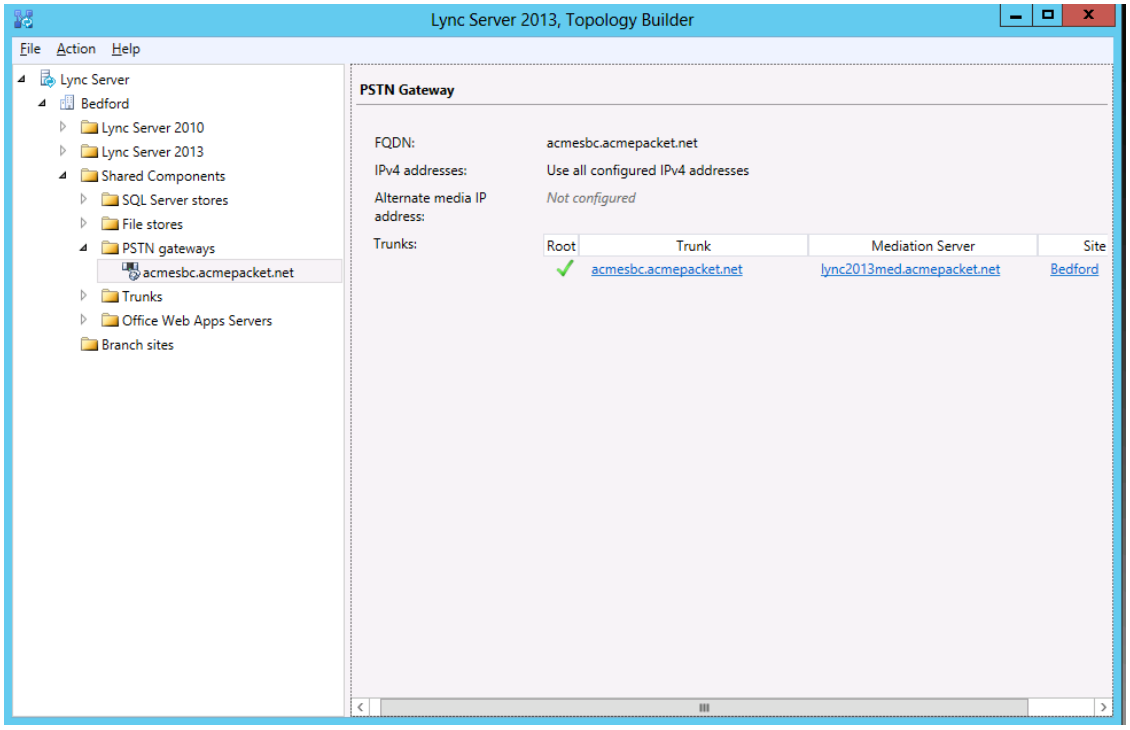

Define New IP/PSTN Gateway
Define the PSTN Gateway FQDN
Define the fully qualified domain name (FQDN) for the PSTN gateway.
FQDN: *
acmesbc.acmepacket.net
Help
Back
Next
Cancel


Define New IP/PSTN Gateway
Define the IP address
Enable IPv4
Use all configured IP addresses.
Limit service usage to selected IP addresses.
PSTN IP address:
Enable IPv6
Use all configured IP addresses.
Limit service usage to selected IP addresses.
PSTN IP address:
Help
Back
Next
Cancel



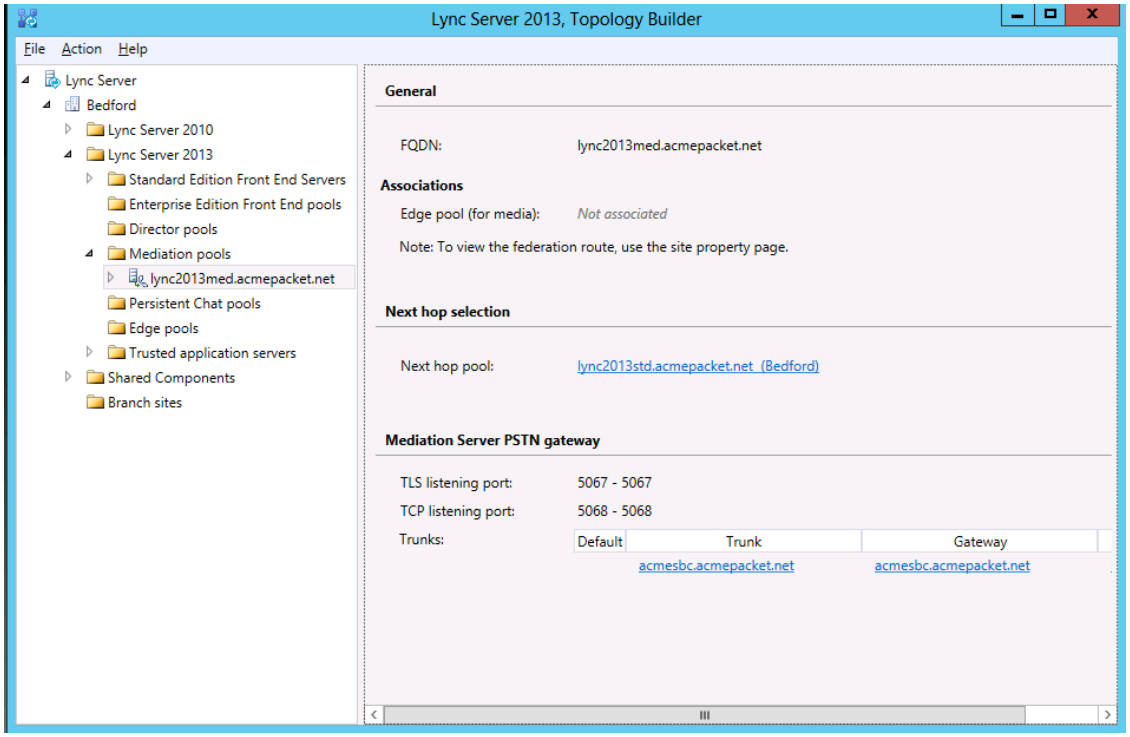
12. Enter the FQDN or the IP address that will be will be the outbound interface for the SIP Trunk on the Oracle Communications Session Border Controller. In our example the IP address is **acmesbc.acmepacket.net.**
13. Enter the **Listening Port**. In our example the listening port is **5068**.
14. Select the **"Sip Transport Protocol**". In our example it is **TCP**. Select this radio button and click **Ok**.

The PSTN Gateway for Lync Server, which is the outbound side of the Oracle Communications Session Border Controller has now been added.



Next we will add the newly created PSTN gateway entry to the Mediation Server.

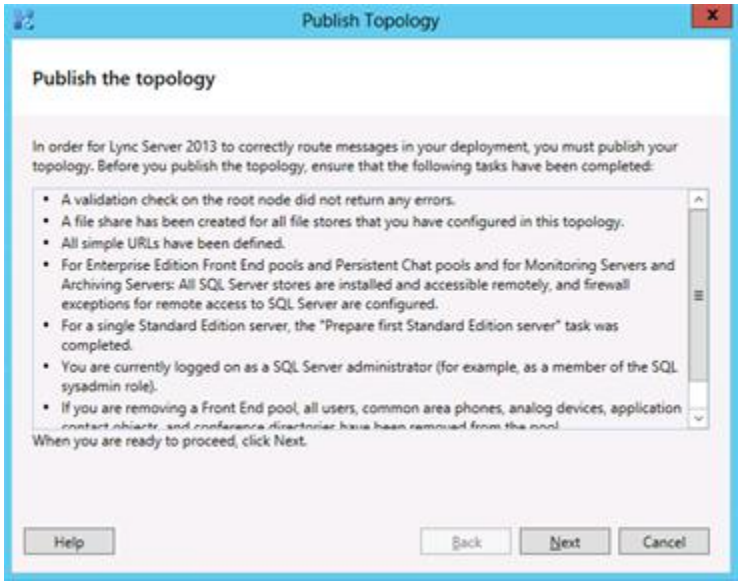
15. Expand the **Mediation Pool** list and click on the Mediation Server to be utilized. In our example the Mediation Server is **lync2013med.acmepacket.net.**



You will now be back at the Topology Builder screen and you can now see that your PSTN Gateway is associated with the Mediation Server

16. In the upper right hand corner of your screen under **Actions** select **Topology** then select **Publish**.

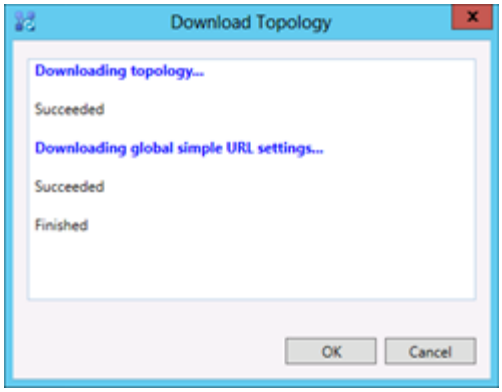
17. You will now see the **Publish Topology** window. Click on the **Next** button



You will now be at a window showing the databases associated with site.

18. Click **Next**.

When complete you should see a window from Topology Builder stating that your topology was successfully published. Click the **OK** button.



19. You will be at the Topology Builder main window, expand your site and double check that your PSTN entries are correct and that the appropriate Mediation Server has the PSTN gateway associated.

Configuring the Lync Server Route:

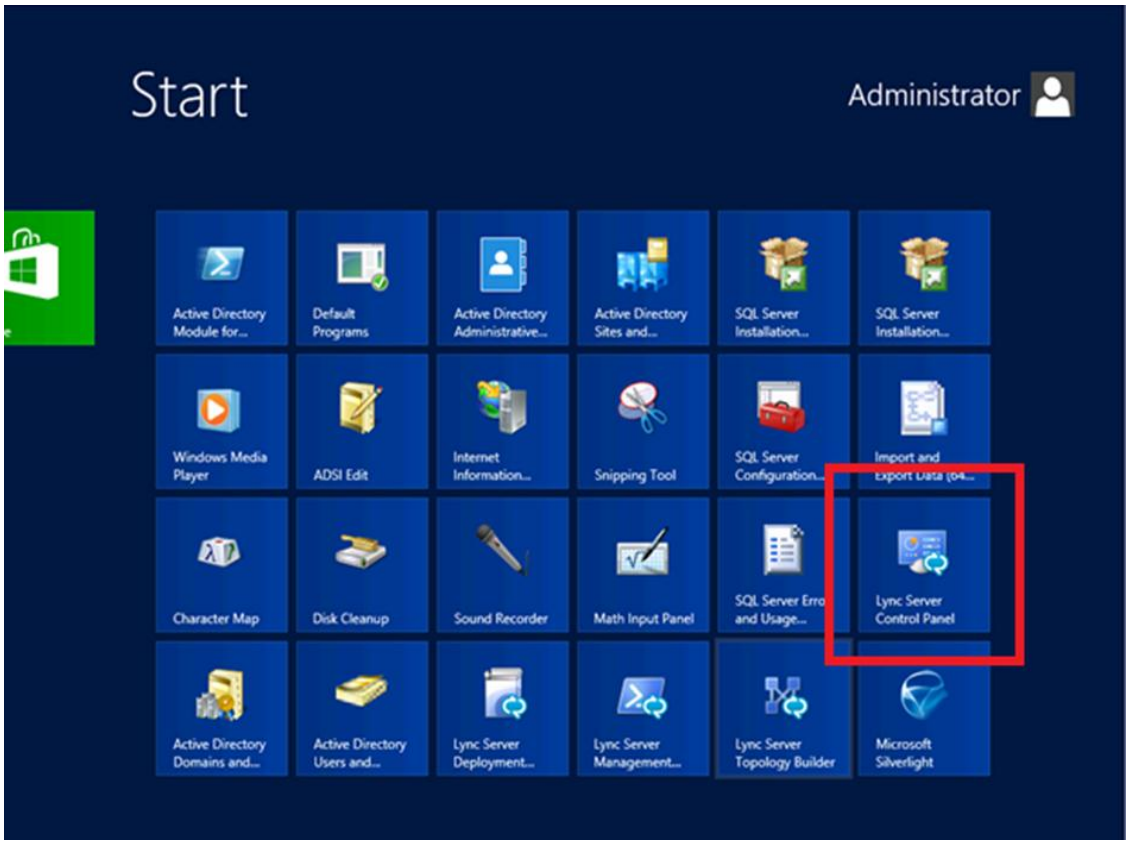
In order for the Lync Server Enterprise Voice clients to utilize the SIP trunking infrastructure that has been put in place, a route will need to be created to allow direction to this egress. Routes specify how Lync Server handles calls placed by enterprise voice users. When a user places a call, the server, if necessary, normalizes the phone number to the E.164 format and then attempts to match that phone number to a SIP Uniform Resource Identifier (URI). If the server is unable to make a match, it applies outgoing call routing logic based on the number. That logic is defined in the form of a separate voice route for each set of target phone numbers listed in the location profile for a locale. For this document we are only describing how to set up a route. Other aspects which apply to Lync Server Enterprise Voice deployments such as dial plans, voice policies, and PSTN usages are not covered.

To add the route we will need:

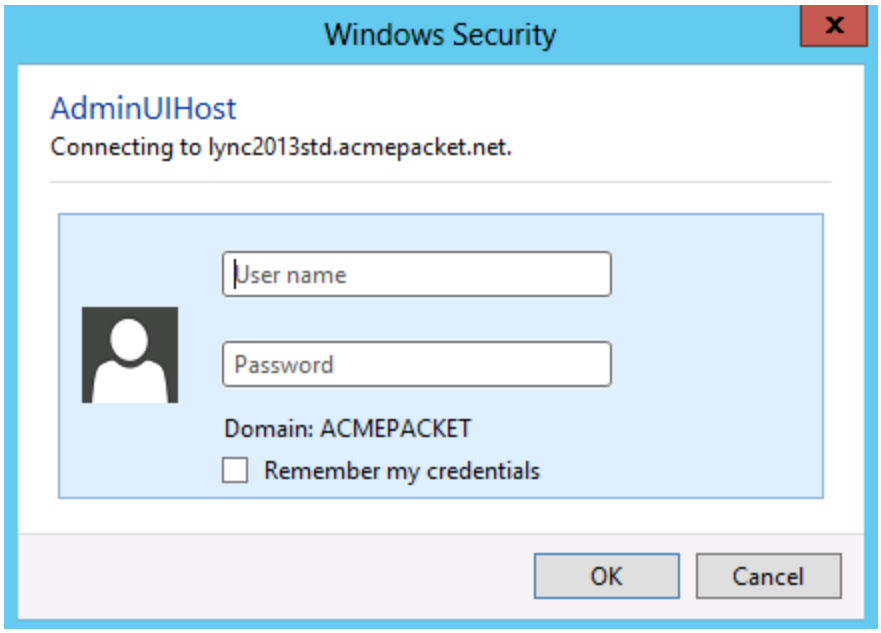
- Rights to administer Lync Server Control Panel
    - Membership in the CS Administrator Active Directory Group
- Access to the Lync Server Control Panel

Steps to add the Lync Server Route

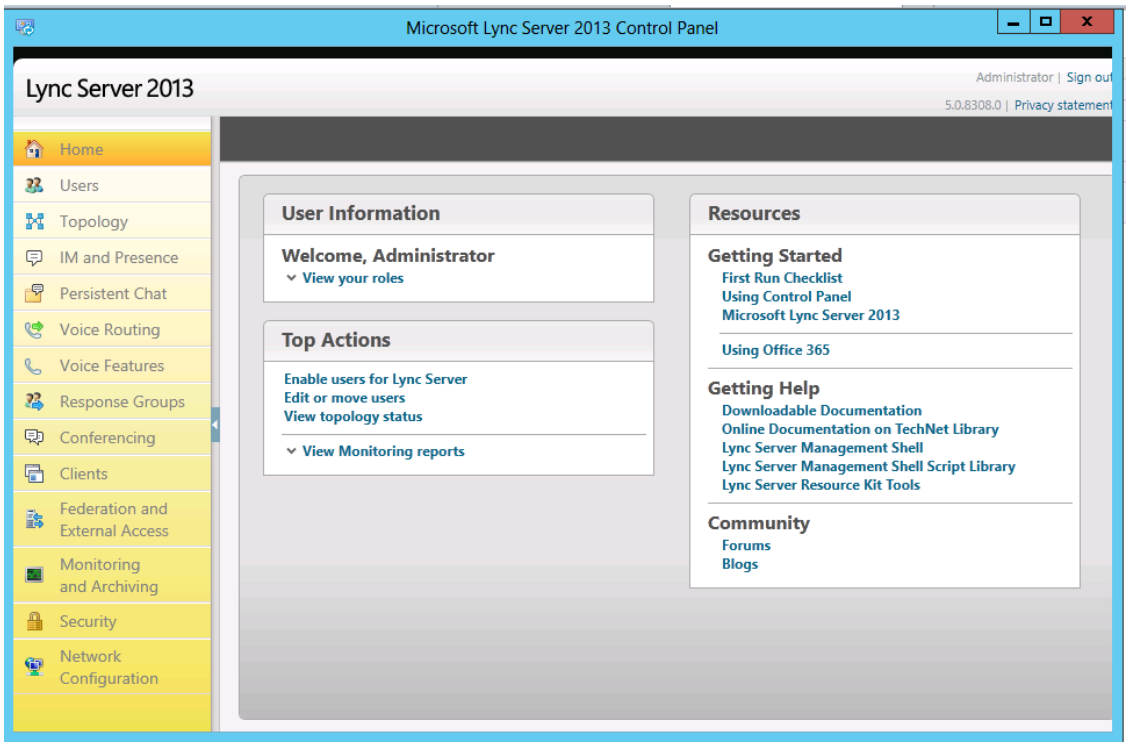
1. From the Start bar, select Lync Server Control Panel



You will be prompted for credential, enter your domain username and password.

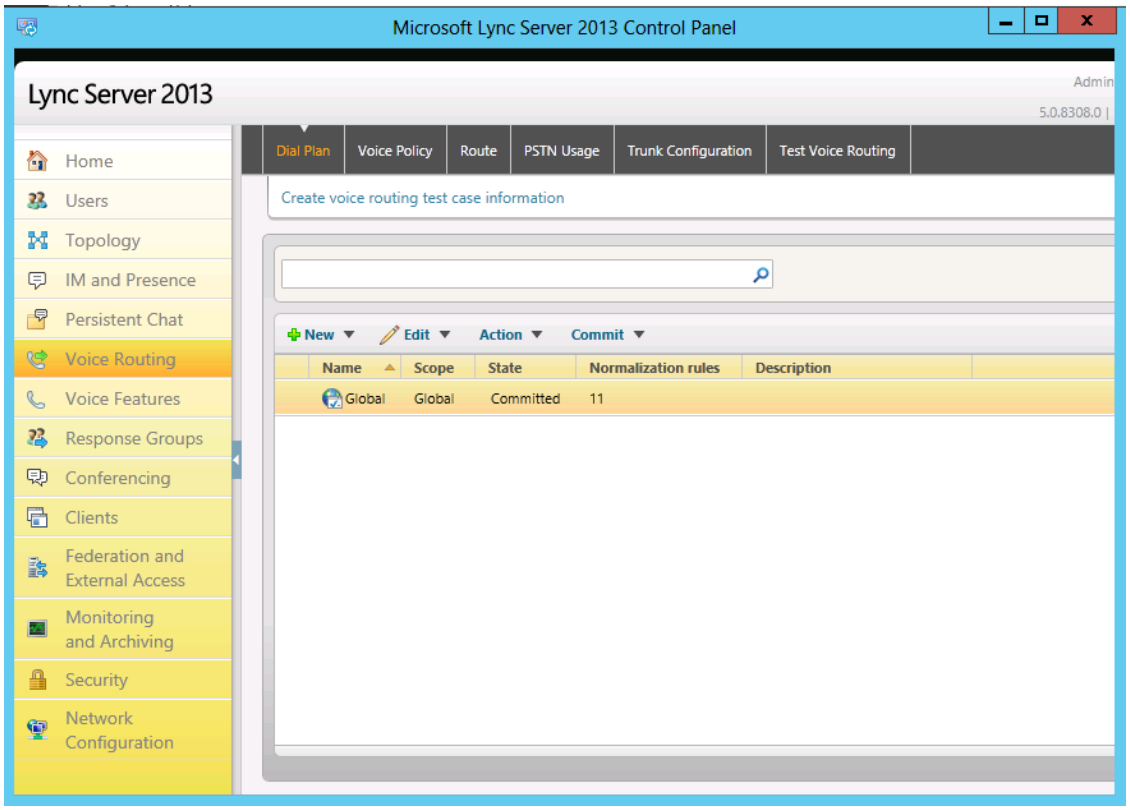


2. Once logged on, you will now be at the "Welcome Screen".



3. On the left hand side of the window, click on **Voice Routing**.
   You will now be in the Voice Routing Section of the Control Panel.

4. On the top rows of the tabs, select **Dial Plan**.



5. On the content area toolbar, click **+New**.

6. Next you build a Dial Plan and a translation rule for the phone numbers you want this route to handle. In this testing, we create a dial plan for US.

   US Dial-plan
   Match this pattern: ^(\d*)$
   Translation rule: $1

7. We will need to create additional normalization rules for the AT&T call forwarding. Call forwarding is activated/deactivated by access codes which differ by the call forwarding conditions.
   For example, to activate Call Forward Always (CFA) or Call Forward Unconditional (CFU), the user dials the CFA activation code, *72 followed by the call forward destination. The user then hears a recording informing that call forwarding has been activated. In order to deactivate CFA, the user dials *73. We will need to add normalization rules for activation/deactivation dial patterns.

   Below we show the normalization rules for CFU

CFU activation

Match this pattern: ^(*72\d*)$

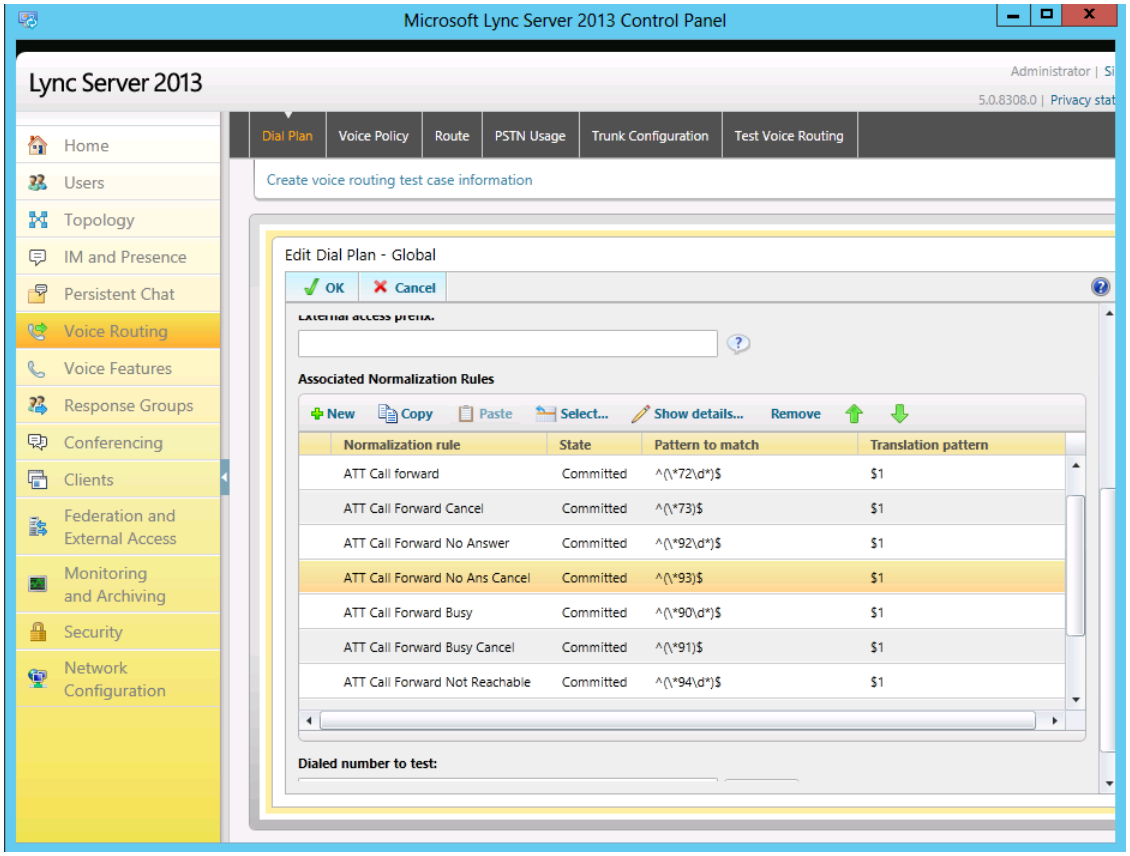
Translation rule: $1

CFU deactivation:

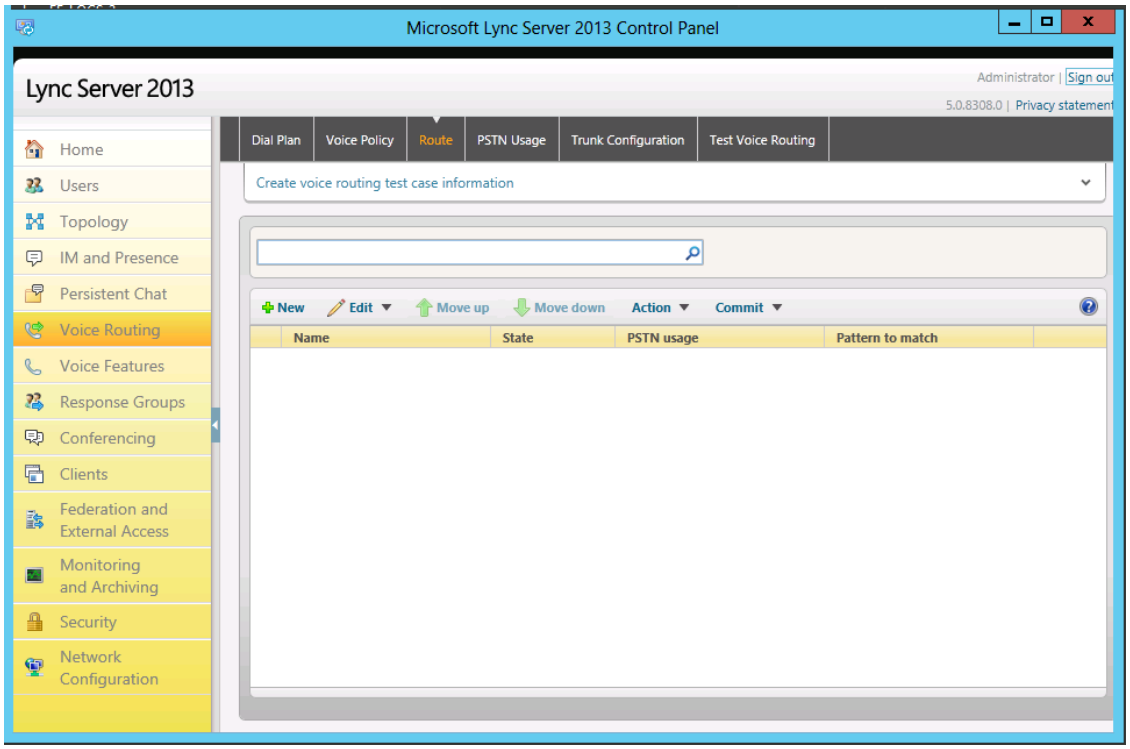
Match this pattern: ^(*73)$

Translation rule: $1

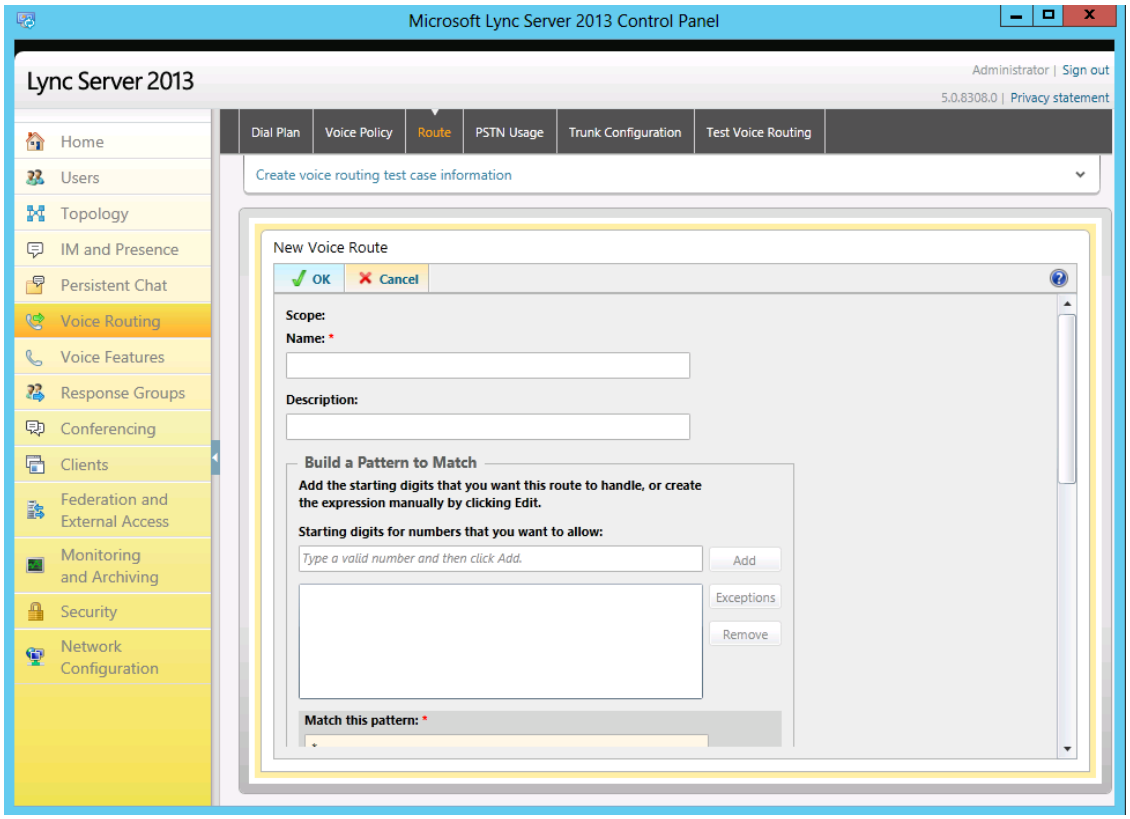
The rules for other call forwarding conditions are shown in the screenshot below.



8. On the top row of the tabs, select **Route**.

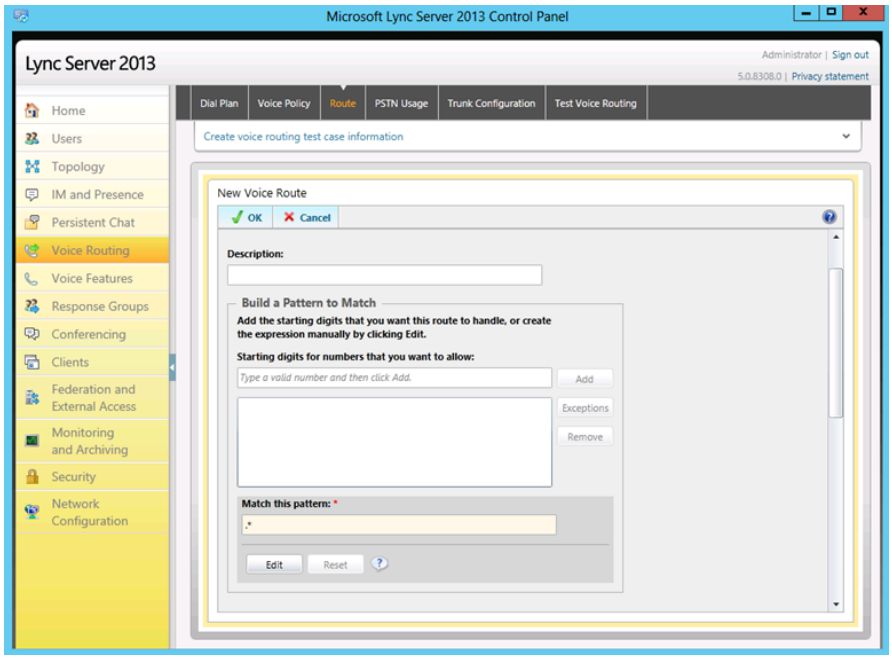


9. On the content area toolbar, click **+New**.

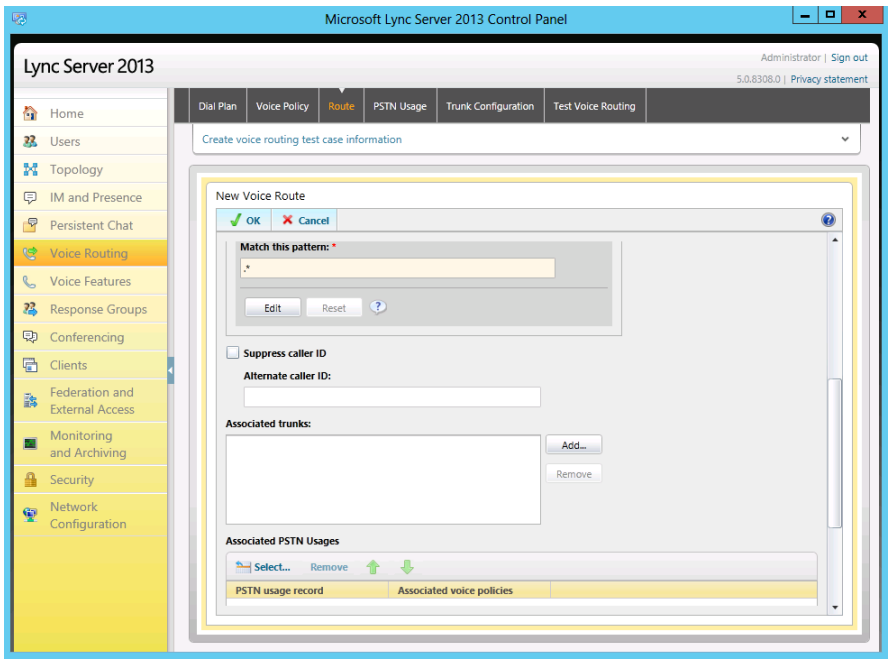


10. On the Create Voice Route page, in the Name field, enter the name you have selected for the Route. In our example, it is SBC.

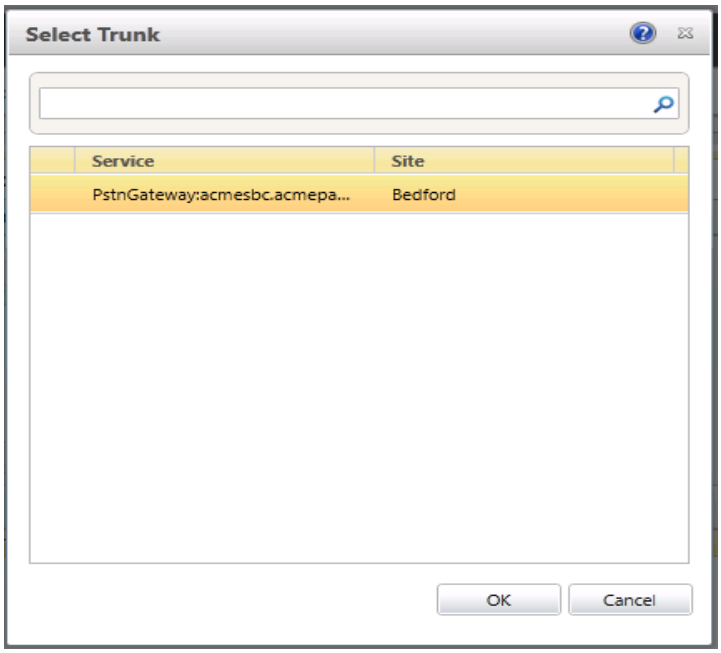
11. Next you build a Pattern Match for the phone numbers you want this route to handle. In our example we use ".*" since we were using a very simple dial plan for this route and wish to match any outgoing call.



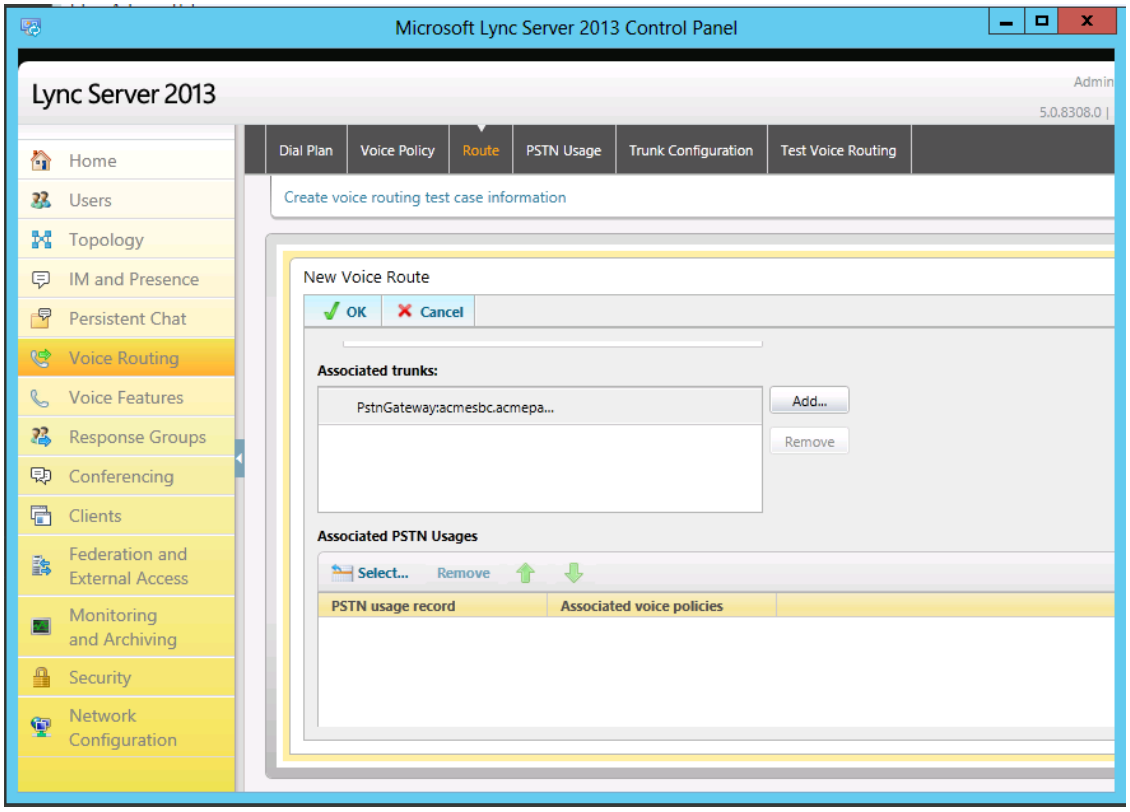
12. Next you want to associate the Voice Route with the PSTN gateway you have just created scroll down to Associated Trunks, click on the Add button.



You will now be at a window showing available PSTN Gateways to associate your Voice Route.



13. Click on the PSTN gateway that you just created and then click the **OK** button.

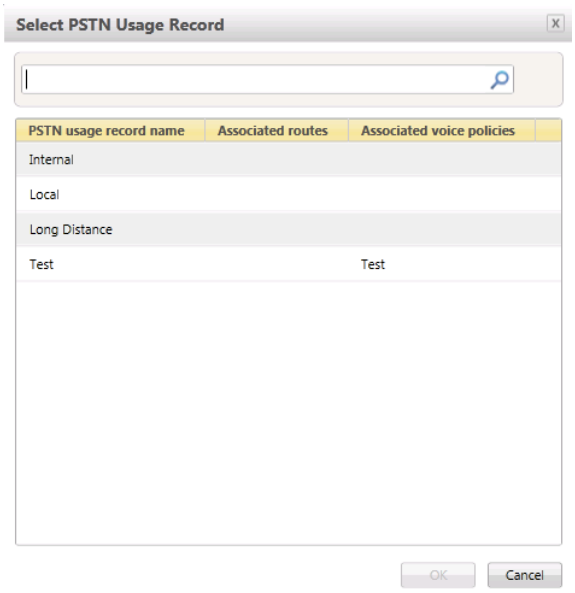


You can now see that you have associated your PSTN gateway with the route you created.

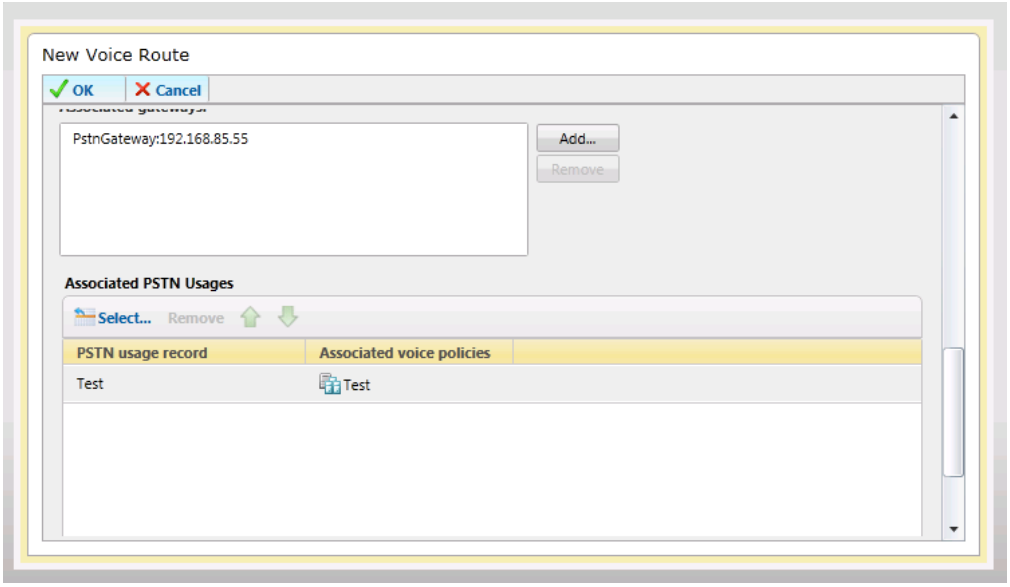
Note that the **Suppress Caller ID**: allows the manipulation of caller ID information for outbound calls, in order to mask employees' direct-dial extensions and replace them with the generic corporate or departmental numbers, this is not a necessary step for this installation, but may need to be addressed by customer policy.

An appropriate PSTN usage record will need to be assigned as well. In our example, we use one that was already created in the enterprise.

14. Click on the **Select** button under "Associated PSTN Usages".

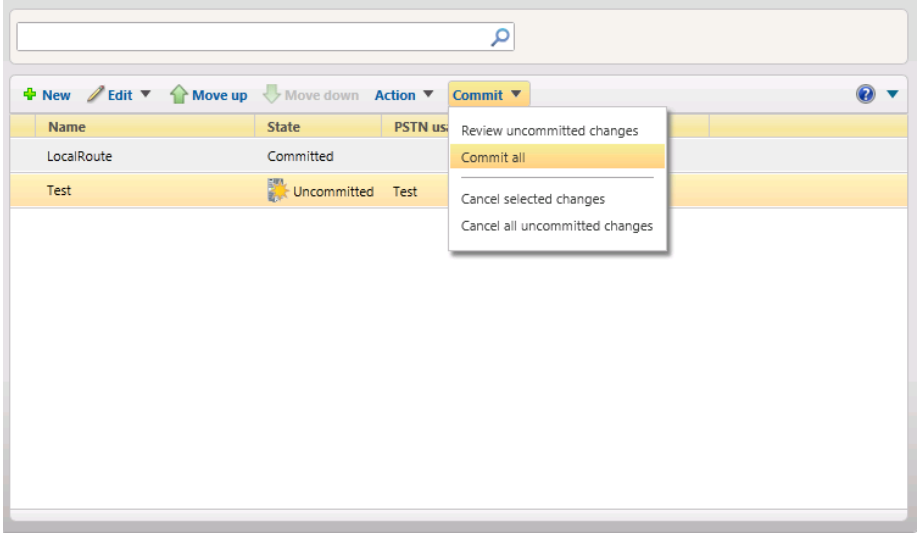


15. Select the appropriate PSTN Usage Record then click the **OK** button.

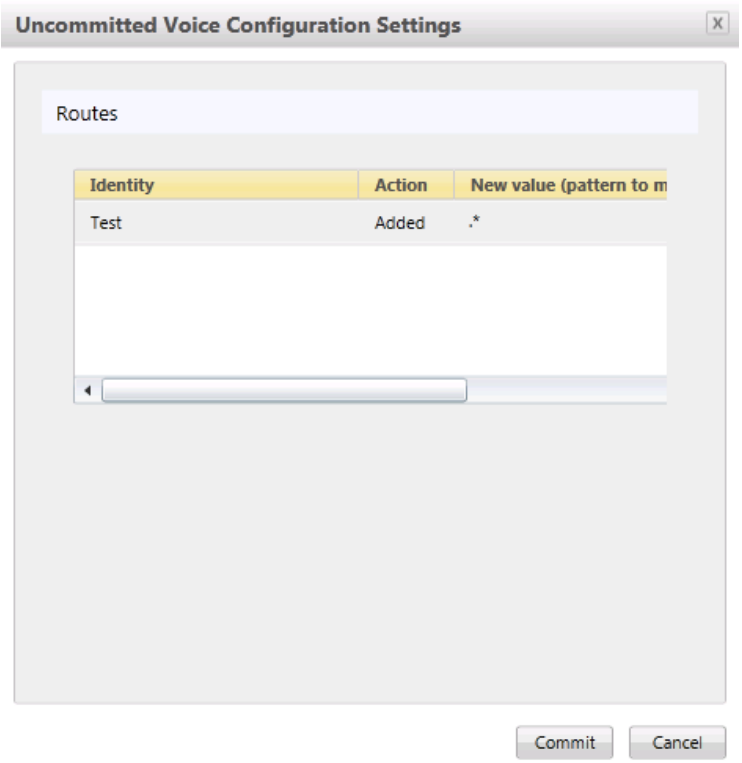


16. You will now see the Associated PSTN Gateway Usages which you have added. Click the **OK** button at the top New Voice Route screen.

17. Click the **Commit** drop-down menu, and then **Commit All**.



18. On the Uncommitted Voice Configuration Settings window, click **Commit**.



19. On the **Lync Server Control Panel** prompt, click OK.

20. If there are no errors, the new Voice Route has now been successfully created and the State will show as Committed.
21. Calls without RTP for 30 seconds are dropped by Lync. To resolve this issue, we need to disable the RTCPActiveCalls and RTCPCallsOnHold parameters by issuing the following command in Lync Server Management Shell. You can access it from **Start Lync Server Management Shell**
22. Set-CsTrunkConfiguration –RTCPActiveCalls $false –RTCPCallsOnHold $false

Additional Steps:

There are other aspects to a Lync Server Enterprise Voice deployment such as:

- Site, local, and global dial plans;
- Voice Policies;
- Assigning Voice Policies to users; and
- PSTN usage policies.

Refer to MSDN technet for relevant information

Phase II – Configure Oracle Communications Session Border Controller

In this section we describe the steps for configuring an Acme Packet series SBC for use with Lync Server in a SIP trunking scenario.

In Scope

The following Step-by-Step guide configuring the Acme Packet series SBC assumes that this is a newly deployed device dedicated to a single customer.

Note that Oracle offers several products and solutions that can interface with Lync Server. This document covers the setup for the Oracle Communications Session Border Controller platforms software SCX 6.3.7m1p1 or later. An Acme Packet 3800-series (NN3820) platform was used as the platform for developing this guide. If instructions are needed for other Oracle products, please contact your Oracle representative.

Out of Scope

- Configuration of Network management including SNMP and RADIUS;

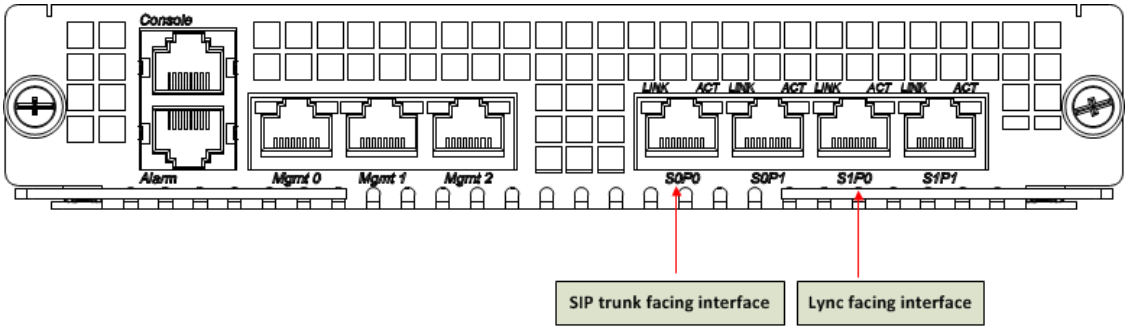
What you will need

- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTYor HyperTerm
- Passwords for the User and Superuser modes on the Oracle Enterprise Session Border Controller
- Signaling IP address and port of Lync Mediation Server

- Signaling and media IP addresses and ports to be used on the Oracle Enterprise Session Border Controller facing Lync and service provider SIP trunk
- Signaling IP address and port of the next hop network element in the service provider SIP trunk network
- IP address of the enterprise DNS server

Configuration

Once the Acme Packet series SBC is racked and the power cable connected, you are ready to set up physical network connectivity.



Plug the slot 0 port 0 (s0p0) interface into your SIP trunk provider (SIP trunk facing) network and the slot 0 port 1 (s1p0) interface into your Lync (Lync mediation server-facing) network as shown in the diagram above. Once connected, you are ready to power on and perform the following steps.

All commands are in bold, such as **configure terminal**; parameters in bold red such as **LYNC-ATT-IOT** are parameters which are specific to an individual deployment.

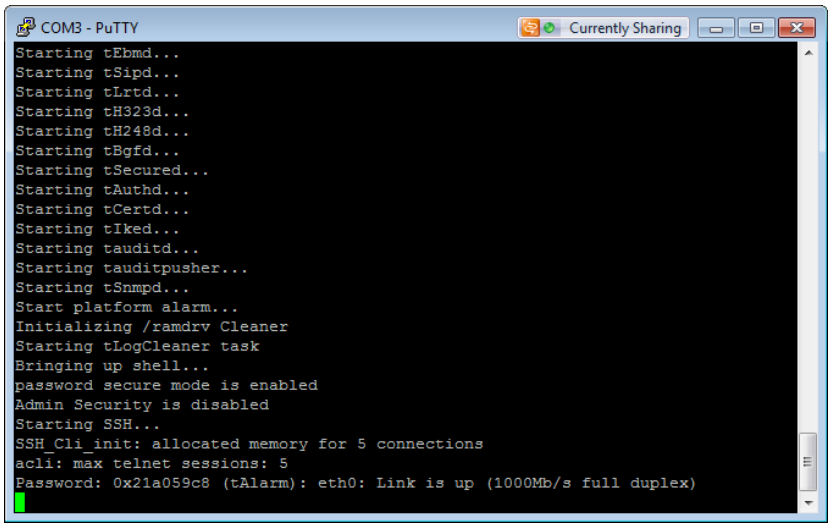
Note: The ACLI is case sensitive.

1. **Establish the serial connection to the Oracle Communications Session Border Controller.**

Confirm the Oracle Communications Session Border Controller is powered off and connect the serial console cable to the Oracle Communications Session Border Controller to a workstation running a terminal emulator application such as PuTTy. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Start the Oracle Communications Session Border Controller and confirm that you see the following output from the bootup sequence.

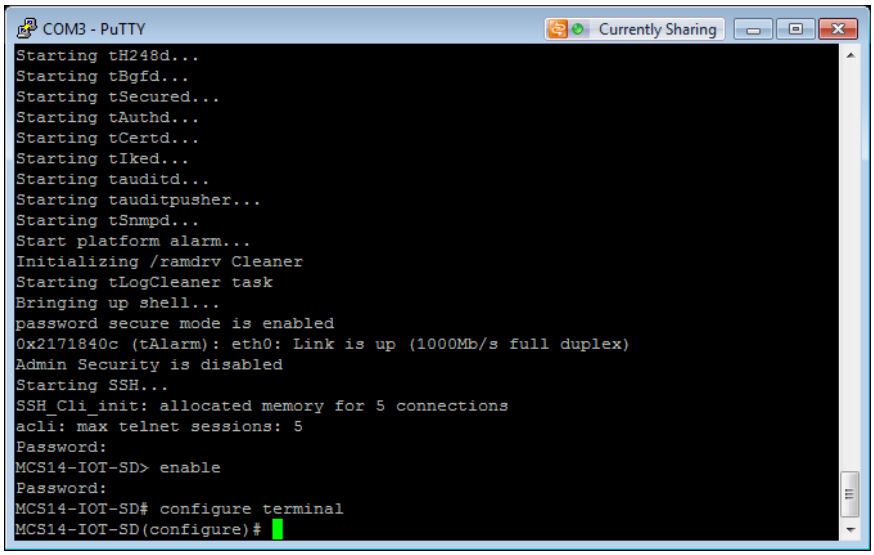


2. Login to the Oracle Communications Session Border Controller and enter the configuration mode

Enter the following commands to login to the Oracle Communications Session Border Controller and move to the configuration mode. Note that the default Oracle Communications Session Border Controller password is "acme" and the default super user password is "packet".

```
Password: acme
LYNC-ATT-IOT> enable
Password: packet
LYNC-ATT-IOT# configure terminal
LYNC-ATT-IOT (configure)#
```

You are now in the Global Configuration mode.



3. **Do the Initial Configuration – Assign the management Interface an IP address**

To assign an IP address, one has to configure the bootparams on the Oracle Communications Session Border Controller, by going to

Lync-ATT-IOT#configure terminal --- >bootparams

- Once you type "bootparam" you have to use "carriage return" key to navigate down
- A reboot is required if changes are made to the existing bootparams

```
MCS14-IOT-SD#(configure)bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device             : eth0
processor number        : 0
host name               : acmesystem
file name               : /code/images/nnECX637m1p1.tar--- >location where the software is
loaded on the SBC
inet on ethernet (e)    : 172.41.3.111:ffffff80 --- > This is the ip address of the
management interface of the SBC, type the IP address and mask in hex
inet on backplane (b)   :
host inet (h)           :
gateway inet (g)        : 172.41.0.1 --- > gateway address here
user (u)                : vxftp
ftp password (pw) (blank = use rsh)     : vxftp
flags (f)               :
target name (tn)        : Lync-ATT-IOT
startup script (s)      :
other (o)               :
```

4. Configure system element values

To configure system element values, use the `system-config` command under the system branch. Then enter values appropriate to your environment, including your default gateway IP address for your management Ethernet interface.

```
LYNC-ATT-IOT(configure)# system
LYNC-ATT-IOT(system)# system-config
LYNC-ATT-IOT(system-config)# hostname LYNC-ATT-IOT
LYNC-ATT-IOT(system-config)# description "Lync Server 2013 SIP Trunking"
LYNC-ATT-IOT(system-config)# location "Redmond, WA"
LYNC-ATT-IOT(system-config)# default-gateway 172.41.0.1
LYNC-ATT-IOT(system-config)# done
```

Once the **system-config** settings have completed and you enter **done**, the Oracle Communications Session Border Controller will output a complete listing of all current settings. This will apply throughout the rest of the configuration and is a function of the **done** command. Confirm the output reflects the values you just entered as well as any configuration defaults.

```
system-config
hostname
description                     Lync Server 2013 SIP Trunking
location                        Redmond, WA
mib-system-contact
mib-system-name
mib-system-location             Redmond, WA
snmp-enabled                    enabled
enable-snmp-auth-traps          disabled
enable-snmp-syslog-notify       disabled
enable-snmp-monitor-traps       disabled
enable-env-monitor-traps        disabled
snmp-syslog-his-table-length    1
snmp-syslog-level               WARNING
system-log-level                WARNING
process-log-level               NOTICE
```

```
process-log-ip-address          0.0.0.0
process-log-port                0
collect
sample-interval                 5
push-interval                   15
boot-state                      disabled
start-time                      now
end-time                        never
red-collect-state               disabled
red-max-trans                   1000
red-sync-start-time             5000
red-sync-comp-time              1000
push-success-trap-state         disabled
call-trace                      disabled
internal-trace                  disabled
log-filter                      all
default-gateway                 172.41.0.1
restart                         enabled
exceptions
telnet-timeout                  0
console-timeout                 0
remote-control                  enabled
cli-audit-trail                 enabled
link-redundancy-state           disabled
source-routing                  disabled
cli-more                        disabled
terminal-height                 24
debug-timeout                   0
trap-event-lifetime             0
default-v6-gateway              ::
ipv6-support                    disabled
```

5. Configure Physical Interface values

To configure physical Interface values, use the phy-interface command under the system branch. To enter the system branch from system-config, you issue the **exit** command then the **phy**-interface command.

You will first configure the slot 0, port 0 interface designated with the name s0p0. This will be the port plugged into your inside (connection to the PSTN gateway) interface.

```
LYNC-ATT-IOT(system-config)# exit
LYNC-ATT-IOT(system)# phy-interface
LYNC-ATT-IOT(phy-interface)# name M00
LYNC-ATT-IOT(phy-interface)# operation-type media
LYNC-ATT-IOT(phy-interface)# slot 0
LYNC-ATT-IOT(phy-interface)# port 0
LYNC-ATT-IOT(phy-interface)# done
```

Once the **phy-interface** settings have completed for slot 0 port 0 and you enter **done**, the Oracle Communications Session Border Controller will output a complete listing of all current settings. Confirm the output reflects the values you just entered.

```
phy-interface
name                            M00
operation-type                  Media
port                            0
slot                            0
virtual-mac
admin-state                     enabled
auto-negotiation                enabled
duplex-mode                     FULL
speed                           100
overload-protection             disabled
```

You will now configure the slot 1 port 0 phy-interface, specifying the appropriate values. This will be the port plugged into your outside (connection to the mediation server) interface.

```
LYNC-ATT-IOT(phy-interface)# name M10
LYNC-ATT-IOT(phy-interface)# operation-type media
LYNC-ATT-IOT(phy-interface)# slot 1
LYNC-ATT-IOT(phy-interface)# port 0
LYNC-ATT-IOT(phy-interface)# done

phy-interface
name                          M10
operation-type                Media
port                          0
slot                          1
virtual-mac
admin-state                   enabled
auto-negotiation              enabled
duplex-mode                   FULL
speed                         100
overload-protection           disabled
```

6. Configure Network Interface values

To configure Network Interface values, use the network-interface command under the system branch. To enter the system branch from phy-interface, you issue the **exit** command then the **network-interface** command.

You will first configure the IP characteristics for the M10 interface defined above.

```
LYNC-ATT-IOT(phy-interface)# exit
LYNC-ATT-IOT(system)# network-interface
LYNC-ATT-IOT(network-interface)# name s1p0
LYNC-ATT-IOT(network-interface)# description "Mediation Server-facing inside interface"
LYNC-ATT-IOT(network-interface)# ip-address 192.168.2.130
LYNC-ATT-IOT(network-interface)# netmask 255.255.255.0
LYNC-ATT-IOT(network-interface)# gateway 192.168.2.1
LYNC-ATT-IOT(network-interface)# pri-utility-addr 192.168.2.131
LYNC-ATT-IOT(network-interface)# sec-utility-addr 192.168.2.132
LYNC-ATT-IOT(network-interface)# add-hip-ip 192.168.2.130
LYNC-ATT-IOT(network-interface)# add-icmp-ip 192.168.2.130

LYNC-ATT-IOT(network-interface)# done

network-interface
        name                            s1p0
        sub-port-id                     0
        description                     Mediation Server-facing inside interface
        hostname                        acmesbc.acmepacket.net
        ip-address                      192.168.2.130
        pri-utility-addr                192.168.2.131
        sec-utility-addr                192.168.2.132
        netmask                         255.255.255.0
        gateway                         192.168.2.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain                    acmepacket.net
        dns-timeout                    11
```

```
        hip-ip-list                     192.168.2.130
        ftp-address
        icmp-address                    192.168.2.130
        snmp-address
        telnet-address
        ssh-address
```

You will now configure the slot 0 port 0 subport 0 network-interface, specifying the appropriate values.

```
LYNC-ATT-IOT(network-interface)# name s0p0
LYNC-ATT-IOT(network-interface)# description "VoIP gateway-facing inside interface"
LYNC-ATT-IOT(network-interface)# ip-address 192.20.0.108
LYNC-ATT-IOT(network-interface)# netmask 255.255.255.0
LYNC-ATT-IOT(network-interface)# gateway 192.20.0.1
LYNC-ATT-IOT(network-interface)# pri-utility-addr 192.20.0.109
LYNC-ATT-IOT(network-interface)# sec-utility-addr 192.20.0.110
LYNC-ATT-IOT(network-interface)# add-hip-ip 192.20.0.108
LYNC-ATT-IOT(network-interface)# add-icmp-ip 192.20.0.108
LYNC-ATT-IOT(network-interface)# done

network-interface
 name                           s0p0
 sub-port-id                    0
  description                    VoIP gateway-facing inside interface
        hostname
        ip-address                      192.20.0.108
        pri-utility-addr                192.20.0.109
        sec-utility-addr                192.20.0.110
        netmask                         255.255.255.0
        gateway                         192.20.0.108
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout
        hip-ip-list                     192.20.0.108
        ftp-address
        icmp-address                    192.20.0.108
        snmp-address
        telnet-address
        ssh-address
```

You will now configure the wancom1 and wancom2 for redundancy, specifying the appropriate values.

```
LYNC-ATT-IOT(network-interface)# name wancom1
LYNC-ATT-IOT(network-interface)# netmask 255.255.255.252
LYNC-ATT-IOT(network-interface)# pri-utility-addr 169.254.1.1
LYNC-ATT-IOT(network-interface)# sec-utility-addr 169.254.1.2

LYNC-ATT-IOT(network-interface)# done

network-interface
        name                            wancom1
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                169.254.1.1
        sec-utility-addr                169.254.1.2
        netmask                         255.255.255.252
```

```
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list
        ftp-address
        icmp-address
        snmp-address
        telnet-address
        ssh-address

LYNC-ATT-IOT(network-interface)# name wancom2
LYNC-ATT-IOT(network-interface)# netmask 255.255.255.252
LYNC-ATT-IOT(network-interface)# pri-utility-addr 169.254.2.1
LYNC-ATT-IOT(network-interface)# sec-utility-addr 169.254.2.2

LYNC-ATT-IOT(network-interface)# done

network-interface
        name                            wancom2
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                169.254.2.1
        sec-utility-addr                169.254.2.2
        netmask                         255.255.255.252
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list
        ftp-address
        icmp-address
        snmp-address
        telnet-address
        ssh-address
```

7. Configure Global SIP configuration

To configure the Global SIP values, use the sip-config command under the session-router branch. To enter the session-router branch from network-interface, you issue the exit command twice, followed by the sip-config command.

```
LYNC-ATT-IOT(network-interface)# exit
LYNC-ATT-IOT(system)# exit
LYNC-ATT-IOT(configure)# session-router
LYNC-ATT-IOT(session-router)# sip-config
LYNC-ATT-IOT(sip-config)# operation-mode dialog
LYNC-ATT-IOT(sip-config)#options +max-udp-length=0
LYNC-ATT-IOT(sip-config)# done

sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id
        egress-realm-id
        nat-mode                        None
        registrar-domain
        registrar-host
        registrar-port                  0
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        options                         max-udp-length=0
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
        extra-method-stats              disabled
        rph-feature                     disabled
        nsep-user-sessions-rate         0
        nsep-sa-sessions-rate           0
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        refer-src-routing               disabled
        add-ucid-header                 disabled
        proxy-sub-events
        pass-gruu-contact               disabled
        sag-lookup-on-redirect          disabled
        set-disconnect-time-on-bye      disabled
```

8. Configure Global Media configuration

To configure the Media values, use the media-manager command under the media-manager branch. To enter the media-manager branch from sip-config, you issue the **exit** command twice, followed by the **media-manager** command twice.

By issuing the select then done commands at this level, you will be creating the media-manager element, enabling the media management functions in the Oracle Communications Session Border Controller with the default values.

```
LYNC-ATT-IOT(sip-config)# exit
LYNC-ATT-IOT(session-router)# exit
LYNC-ATT-IOT(configure)# media-manager
LYNC-ATT-IOT(media-manager)# media-manager
LYNC-ATT-IOT(media-manager)# select
LYNC-ATT-IOT(media-manager-config)# done

media-manager
state                          enabled
latching                       enabled
flow-time-limit                86400
initial-guard-timer            300
subsq-guard-timer              300
tcp-flow-time-limit            86400
tcp-initial-guard-timer        300
tcp-subsq-guard-timer          300
tcp-number-of-ports-per-flow   2
hnt-rtcp                       disabled
algd-log-level                 NOTICE
mbcd-log-level                 NOTICE
red-flow-port                  1985
red-mgcp-port                  1986
red-max-trans                  10000
red-sync-start-time            5000
red-sync-comp-time             1000
media-policing                 enabled
max-signaling-bandwidth        10000000
max-untrusted-signaling        100
min-untrusted-signaling        30
app-signaling-bandwidth        0
tolerance-window               30
rtcp-rate-limit                0
trap-on-demote-to-deny         disabled
min-media-allocation           2000
min-trusted-allocation         4000
deny-allocation                64000
anonymous-sdp                  disabled
arp-msg-bandwidth              32000
fragment-msg-bandwidth         0
rfc2833-timestamp              disabled
default-2833-duration          100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event    disabled
media-supervision-traps        disabled
dnsalg-server-failover         disabled
```

9. Configure Realms configuration

To configure the realm values, use the realm-config command under the media-manager branch. To enter the media-manager branch from media-manager-config, you issue the **exit** command, followed by the **realm-config** command.

You will create two realms:

- The MS-Lync-Peer, which represents the mediation server-facing (inside) network; and
- The ATT, which represents the gateway-facing (outside) network.

```
LYNC-ATT-IOT(media-manager-config)# exit
LYNC-ATT-IOT(media-manager)# realm-config
```

```
LYNC-ATT-IOT(realm-config)# identifier MS-Lync-Peer
LYNC-ATT-IOT(realm-config)# description "Mediation Server-facing (Inside)"
LYNC-ATT-IOT(realm-config)# network-interfaces s1p0:0
LYNC-ATT-IOT(realm-config)# done

realm-config
        identifier                      MS-Lync-Peer
        description                     Mediation Server-facing(Inside)
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s1p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        cac-failure-threshold           0
        untrust-cac-failure-threshold   0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
```

```
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        codec-manip-in-network          disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
```

You will now configure the PSTN realm for SIP Trunk side of the SBC, specifying the appropriate values.

```
LYNC-ATT-IOT(realm-config)# identifier ATT
LYNC-ATT-IOT(realm-config)# description "Gateway (outside)"
LYNC-ATT-IOT(realm-config)# network-interfaces s0p0:0
LYNC-ATT-IOT(realm-config)#media-policy voip-default
LYNC-ATT-IOT(realm-config)# done

realm-config
        identifier                      ATT
        description                     Gateway (outside)
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy                    voip-default
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
```

```
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        cac-failure-threshold          0
        untrust-cac-failure-threshold  0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
        codec-policy
        codec-manip-in-realm           disabled
        codec-manip-in-network         disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
```

10. Configure SBC redundancy configuration

To configure the SBC redundancy configuration, use the `redundancy-config` command under the media-manager element.

```
LYNC-ATT-IOT(realm-config)# exit
LYNC-ATT-IOT(media-manager)# exit
LYNC-ATT-IOT(configure)# system
LYNC-ATT-IOT(system)# redundancy
LYNC-ATT-IOT(redundancy)# state enabled
LYNC-ATT-IOT(redundancy)# peer
LYNC-ATT-IOT(rdncy-peer)# name Lync-ATT-IOT
LYNC-ATT-IOT(rdncy-peer)# state enabled
LYNC-ATT-IOT(rdncy-peer)# type Primary
LYNC-ATT-IOT(rdncy-peer)# destination
LYNC-ATT-IOT(rdncy-peer-dest)# address 169.254.1.1:9090
LYNC-ATT-IOT(rdncy-peer-dest)# network-interface wancom1:0
LYNC-ATT-IOT(rdncy-peer-dest)# done
destination
    address                       169.254.1.1:9090
```

```
    network-interface              wancom1:0
LYNC-ATT-IOT(rdncy-peer-dest)# address 169.254.2.1:9090
LYNC-ATT-IOT(rdncy-peer-dest)# network-interface wancom2:0
LYNC-ATT-IOT(rdncy-peer-dest)# done
destination
    address                        169.254.2.1:9090
    network-interface              wancom2:0
LYNC-ATT-IOT(rdncy-peer-dest)# exit
LYNC-ATT-IOT(rdncy-peer)# done
peer
    name                           Lync-ATT-IOT
    state                          enabled
    type                           Primary
    destination
    address                        169.254.1.1:9090
          network-interface              wancom1:0
    destination
          address                        169.254.2.1:9090
          network-interface              wancom2:0
LYNC-ATT-IOT(rdncy-peer)# name SN1Secondary
LYNC-ATT-IOT(rdncy-peer)# state enabled
LYNC-ATT-IOT(rdncy-peer)# type Secondary
LYNC-ATT-IOT(rdncy-peer)# destination
LYNC-ATT-IOT(rdncy-peer-dest)# address 169.254.1.2:9090
LYNC-ATT-IOT(rdncy-peer-dest)# network-interface wancom1:0
LYNC-ATT-IOT(rdncy-peer-dest)# done
destination
    address                        169.254.1.2:9090
    network-interface              wancom1:0
LYNC-ATT-IOT(rdncy-peer-dest)# address 169.254.2.2:9090
LYNC-ATT-IOT(rdncy-peer-dest)# network-interface wancom2:0
LYNC-ATT-IOT(rdncy-peer-dest)# done
destination
    address                        169.254.2.2:9090
    network-interface              wancom2:0
LYNC-ATT-IOT(rdncy-peer-dest)# exit
LYNC-ATT-IOT(rdncy-peer)# done
peer
    name                           SN1Secondary
    state                          enabled
    type                           Secondary
    destination
    address                        169.254.1.2:9090
          network-interface              wancom1:0
    destination
          address                        169.254.2.2:9090
          network-interface              wancom2:0
LYNC-ATT-IOT(rdncy-peer)# exit
LYNC-ATT-IOT(redundancy)# done
redundancy-config
        state                          enabled
        log-level                      INFO
        health-threshold               75
        emergency-threshold            50
        port                           9090
        advertisement-time             500
        percent-drift                  210
        initial-time                   1250
        becoming-standby-time          180000
        becoming-active-time           100
        cfg-port                       1987
        cfg-max-trans                  10000
        cfg-sync-start-time            5000
        cfg-sync-comp-time             1000
        gateway-heartbeat-interval     10
        gateway-heartbeat-retry        3
```

```
        gateway-heartbeat-timeout       1
        gateway-heartbeat-health        1
        media-if-peercheck-time         0
        peer
                name                            SN1Secondary
                state                           enabled
                type                            Secondary
                destination
                        address                         169.254.1.2:9090
                        network-interface               wancom1:0
                destination
                        address                         169.254.2.2:9090
                        network-interface               wancom2:0
        peer
                name                            Lync-ATT-IOT
                state                           enabled
                type                            Primary
                destination
                        address                         169.254.1.1:9090
                        network-interface               wancom1:0
                destination
                        address                         169.254.2.1:9090
                        network-interface               wancom2:0
LYNC-ATT-IOT(redundancy)# exit
```

11. Configure SIP signaling configuration

To configure the SIP signaling values, use the sip-interface command under the session-router branch. To enter the session-router branch from realm-config, you issue the **exit** command twice, followed by the **sip-interface** command.

Here you will be configuring the IP addresses and TCP ports on which the Oracle Communications Session Border Controller will listen for and transmit SIP messages. These will be the same IP addresses as configured on the associated network-interface elements.

```
LYNC-ATT-IOT(realm-config)# exit
LYNC-ATT-IOT(media-manager)# exit
LYNC-ATT-IOT(configure)# session-router
LYNC-ATT-IOT(session-router)# sip-interface
LYNC-ATT-IOT(sip-interface)# realm ATT
LYNC-ATT-IOT(sip-interface)# description "SIP Trunk-facing (Outside)"
LYNC-ATT-IOT(sip-interface)# sip-ports
LYNC-ATT-IOT(sip-port)# address 192.20.0.108
LYNC-ATT-IOT(sip-port)# done

sip-port
address                         192.20.0.108
port                            5060
transport-protocol              UDP
tls-profile
allow-anonymous                 all
ims-aka-profile

LYNC-ATT-IOT(sip-port)# exit
LYNC-ATT-IOT(sip-interface)# done

sip-interface
        state                           enabled
        realm-id                        ATT
        description                     SIP Trunk-facing (Outside)
        sip-port
                address                         192.20.0.108
                port                            5060
                transport-protocol              UDP
```

```
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode  pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 101
        rfc2833-mode                    transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
```

You will now configure the mediation server-facing SIP interface.

```
LYNC-ATT-IOT(sip-interface)# realm-id MS-Lync-Peer
LYNC-ATT-IOT(sip-interface)# description "Mediation Server-Facing (Inside)"
LYNC-ATT-IOT(sip-interface)# sip-ports
```

```
LYNC-ATT-IOT(sip-port)# address 192.168.2.130
LYNC-ATT-IOT(sip-port)# transport-protocol TCP
LYNC-ATT-IOT(sip-port)# port 5068
LYNC-ATT-IOT(sip-port)# done
sip-port
address                         192.168.2.130
port                            5068
transport-protocol              TCP
tls-profile
allow-anonymous                 all
ims-aka-profile

LYNC-ATT-IOT(sip-port)# exit
LYNC-ATT-IOTLYNC-ATT-IOT(sip-interface)# done

sip-interface
        state                           enabled
        realm-id                        MS-Lync-Peer
        description                     Mediation Server-Facing(Inside)
        sip-port
                address                         192.168.2.130
                port                            5068
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
```

```
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
```

12. Configure next-hop signaling elements

To configure the next-hop signaling elements (i.e., the mediation server and PSTN gateway) you define **session-agents**. Use the session-agent command under the session-router branch. To enter the session-agent branch from sip-interface, you issue the **exit** command, followed by the **session-agent** command.

Here you will be configuring the IP addresses and TCP ports to which the Oracle Communications Session Border Controller will send and from which it will expect to receive SIP messages for your next-hop signaling elements.

Lync Server 2013 Gateway specification outlines the need for the SBC to have capability to do DNS load balancing among a pool of mediation servers. This is currently supported by the Oracle Communications Session Border Controller via A or SRV records, however not necessarily in a round-robin manner. In this document and testing, the SBC load balances between two mediation servers that are defined in a group (session-group) with round-robin algorithm configured. It is assumed that when using this kind of a configuration at any point another mediation server is added to the pool of servers, it will need to be explicitly configured on the SBC and added to the session-group which will be the responsibility of the enterprise network administrator.

We will first configure the PSTN gateway.

```
LYNC-ATT-IOTLYNC-ATT-IOT(sip-interface)# exit
LYNC-ATT-IOT(session-router)#session-agent
LYNC-ATT-IOT(session-agent)# hostname 10.10.10.10
LYNC-ATT-IOT(session-agent)# port 5060
LYNC-ATT-IOT(session-agent)# realm-id ATT
LYNC-ATT-IOT(session-agent)#ping-method OPTIONS;hops=0
LYNC-ATT-IOT(session-agent)#ping-interval 30
LYNC-ATT-IOT(session-agent)# done

session-agent
        hostname                       10.10.10.10
        ip-address
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       ATT
        egress-realm-id
```

```
        description
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                             OPTIONS;hops=0
        ping-interval                   30
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
```

You will now define the mediation server. For the sake of simplicity, two mediation servers are defined and assigned to a group called 'MediationServerGroup. The SBC then load balances among these mediation servers.

```
LYNC-ATT-IOT(session-agent)# exit
LYNC-ATT-IOT(session-router)# session-group
Lync-ATT-IOT(session-group)# group-name MediationServerGroup
Lync-ATT-IOT(session-group)#description "Group for Mediation servers 1 and 2"
Lync-ATT-IOT(session-group)# strategy RoundRobin
Lync-ATT-IOT(session-group)# dest lync2013med1.acmepacket.net
Lync-ATT-IOT(session-group)# dest +lync2013med2.acmepacket.net
Lync-ATT-IOT(session-group)# done
session-group
        group-name                      MediationServerGroup
        description                     Group for Mediation servers 1 &2
        state                           enabled
        app-protocol                    SIP
        strategy                        RoundRobin
        dest
                                        lync2013med1.acmepacket.net
                                        lync2013med2.acmepacket.net
        trunk-group
        sag-recursion                   disabled
        stop-sag-recurse                401,407
```

Defining Mediation Server 1

```
LYNC-ATT-IOT(session-group)exit
LYNC-ATT-IOT(session-router)session-agent
LYNC-ATT-IOT(session-agent)# hostname lync2013med1.acmepacket.net
LYNC-ATT-IOT(session-agent)# ip-address 192.168.2.192
LYNC-ATT-IOT(session-agent)# port 5068
LYNC-ATT-IOT(session-agent)# app-protocol sip
LYNC-ATT-IOT(session-agent)# transport-method statictcp
LYNC-ATT-IOT(session-agent)# realm-id MS-Lync-Peer
LYNC-ATT-IOT(session-agent)# ping-method OPTIONS;hops=0
LYNC-ATT-IOT(session-agent)#ping-interval 30
Lync-ATT-IOT(session-agent)# refer-call-transfer enabled
LYNC-ATT-IOT(session-agent)# done

session-agent
        hostname                        lync2013med1.acmepacket.net
        ip-address                      192.168.2.192
        port                            5068
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                StaticTCP
        realm-id                        MS-Lync-Peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
```

```
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             enabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
```

Defining Mediation Server 2

```
LYNC-ATT-IOT(session-agent)# hostname lync2013med2.acmepacket.net
LYNC-ATT-IOT(session-agent)# ip-address 192.168.2.193
LYNC-ATT-IOT(session-agent)# port 5068
LYNC-ATT-IOT(session-agent)# app-protocol sip
LYNC-ATT-IOT(session-agent)# transport-method statictcp
LYNC-ATT-IOT(session-agent)# realm-id MS-Lync-Peer
LYNC-ATT-IOT(session-agent)# ping-method OPTIONS;hops=0
LYNC-ATT-IOT(session-agent)#ping-interval 30
Lync-ATT-IOT(session-agent)# refer-call-transfer enabled
LYNC-ATT-IOT(session-agent)# done

session-agent
        hostname                        lync2013med2.acmepacket.net
        ip-address                      192.168.2.193
```

```
        port                            5066
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                StaticTCP
        realm-id                        MS-Lync-Peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             enabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
```

```
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
```

Note: The parameter refer-call-transfer is enabled only if refer termination is required on the SBC. Additional configuration is required to enable this feature. Please refer to the Appendix for the configuration.

13. Configure SIP routing

To configure the SIP routing, use the **local-policy** command under the session-router branch. To enter the session-router branch from session-agent, you issue the **exit** command, followed by the **local-policy** command.

We will first configure the route from the gateway to the mediation server.

```
LYNC-ATT-IOT(session-agent)# exit
LYNC-ATT-IOT(session-router)# local-policy
LYNC-ATT-IOT(local-policy)# from-address *
LYNC-ATT-IOT(local-policy)# to-address *
LYNC-ATT-IOT(local-policy)# source-realm ATT
LYNC-ATT-IOT(local-policy)# policy-attributes
LYNC-ATT-IOT(local-policy-attributes)#next-hop SAG:MediationServerGroup
LYNC-ATT-IOT(local-policy-attributes)# realm MS-Lync-Peer
LYNC-ATT-IOT(local-policy-attributes)# app-protocol sip
LYNC-ATT-IOT(local-policy-attributes)# done


LYNC-ATT-IOT(local-policy-attributes)# exit
LYNC-ATT-IOT(local-policy)# done
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        ATT
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@10.0.222.38
        last-modified-date              2011-12-22 20:48:39
        policy-attribute
                next-hop                        SAG:MediationServerGroup
                realm                           MS-Lync-Peer
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
```

```
                eloc-str-lkup                   disabled
                eloc-str-match
```

We will now configure the route from the mediation server to the gateway.

```
LYNC-ATT-IOT(local-policy)# from-address *
LYNC-ATT-IOT(local-policy)# to-address *
LYNC-ATT-IOT(local-policy)# source-realm MS-Lync-Peer
LYNC-ATT-IOT(local-policy)# policy-attributes
LYNC-ATT-IOT(local-policy-attributes)# next-hop 10.10.10.10
LYNC-ATT-IOT(local-policy-attributes)# realm ATT
LYNC-ATT-IOT(local-policy-attributes)# app-protocol sip
LYNC-ATT-IOT(local-policy-attributes)# done

LYNC-ATT-IOT(local-policy-attributes)# exit
LYNC-ATT-IOT(local-policy)# done

local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        MS-Lync-Peer
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@172.41.0.11
        last-modified-date              2012-03-06 11:43:03
        policy-attribute
                next-hop                    10.10.10.10
                realm                          ATT
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol
                state                          enabled
                methods
                media-profiles
                lookup                         single
                next-key
                eloc-str-lkup                  disabled
                eloc-str-match
```

14. Configure media handling

To configure the media handling, use the **steering-pool** command under the media-manager branch. To enter the steering-pool branch from local-policy, you issue the **exit** command twice, followed by the **media-manager** then the **steering-pool** command.

You will use the same IP address for the steering pool as the one used for the SIP interface. Note that the port ranges provide a means of limiting the number of concurrent media sessions within a given realm. For example, assigning 100 ports to a realm would limit it to 50 concurrent bidirectional calls, where two ports are assigned (one per unidirectional media stream).

```
LYNC-ATT-IOT(local-policy)# exit
LYNC-ATT-IOT(session-router)# exit
LYNC-ATT-IOT(configure)# media-manager
```

```
LYNC-ATT-IOT(media-manager)# steering-pool
LYNC-ATT-IOT(steering-pool)# ip-address 192.168.2.130
LYNC-ATT-IOT(steering-pool)# start-port 30000
LYNC-ATT-IOT(steering-pool)# end-port 40000
LYNC-ATT-IOT(steering-pool)# realm-id MS-Lync-Peer
LYNC-ATT-IOT(steering-pool)# network-interface s1p0:0
LYNC-ATT-IOT(steering-pool)# done
steering-pool
        ip-address                      192.168.1.130
        start-port                      30000
        end-port                        40000
        realm-id                        MS-Lync-Peer
        network-interface               s1p0:0
```

You will now configure the media handling for the ATT realm.

```
LYNC-ATT-IOT(steering-pool)# ip-address 192.20.0.108
LYNC-ATT-IOT(steering-pool)# start-port 40000
LYNC-ATT-IOT(steering-pool)# end-port 50000
LYNC-ATT-IOT(steering-pool)# realm-id ATT
LYNC-ATT-IOT(steering-pool)# network-interface s0p0:0
LYNC-ATT-IOT(steering-pool)# done
steering-pool
        ip-address                      192.20.0.108
        start-port                      20000
        end-port                        30000
        realm-id                        ATT
        network-interface               s0p0:0
```

15. Transcoding

Transcoding requires a transcoding module to be installed in the SBC. In order to check if the module is present in your SBC, use command "show prom-info phy" and you should see the following output **"ID: 4 Port GiGE w/QoS & DSP".** The transcoding module requires a minimum bootloader version compiled on "06/21/2011". Using command "show version boot" should confirm the compilation date. Transcoding was required in this testing as majority of AT&T customers prefer to use G729. Microsoft Lync requires a minimum codec of G711 and AT&T SIP uses G.729 as a preferred codec, in order for a call to function between MS Lync and AT&T SIP trunk transcoding of the RTP stream is a must. Since their customers support G711 and G729 and G729 annexb, the codec policy must be configured to allow the three codecs mentioned above. The codec order preference required on the calls to AT&T is G729 annexb=no followed by G711mulaw.

For configuring transcoding, the codec-policy needs to be configured on the SBC and then applied on the respective realms. Before configuring the codec-policy, we need to create a media-profile to insert annexb=no in the sdp for G729 codec and then call it by the codecs in codec-policy.

```
LYNC-ATT-IOT(configure)# session-router
LYNC-ATT-IOT(session-router)# media-profile
Lync-ATT-IOT(media-profile)# name G729
Lync-ATT-IOT(media-profile)# subname vadoff
Lync-ATT-IOT(media-profile)# media-type audio
Lync-ATT-IOT(media-profile)# payload-type 18
Lync-ATT-IOT(media-profile)# transport RTP/AVP
Lync-ATT-IOT(media-profile)# parameters annexb=no
Lync-ATT-IOT(media-profile)# done

media-profile
        name                            G729
        subname                         vadoff
        media-type                      audio
        payload-type                    18
```

```
        transport                       RTP/AVP
        req-bandwidth                   0
        frames-per-packet               0
        parameters                      annexb=no
        average-rate-limit              0
        peak-rate-limit                 0
        max-burst-size                  0
        sdp-rate-limit-headroom         0
        sdp-bandwidth                   disabled
        police-rate                     0
        standard-pkt-rate               0
        last-modified-by                admin@console
        last-modified-date              2012-01-24 14:51:19

Lync-ATT-IOT(media-profile)# exit
LYNC-ATT-IOT(session-router)# exit
LYNC-ATT-IOT(configure)# media-manager
LYNC-ATT-IOT(media-manager)# codec-policy
LYNC-ATT-IOT(codec-policy)# name AllowG711
LYNC-ATT-IOT(codec-policy)# allow-codecs (PCMU PCMA telephone-event)
LYNC-ATT-IOT(codec-policy)# add-codecs-on-egress (PCMU PCMA telephone-event)
LYNC-ATT-IOT(codec-policy)# order-codecs (PCMU PCMA telephone-event)
LYNC-ATT-IOT(codec-policy)# dtmf-in-audio disabled
LYNC-ATT-IOT(codec-policy)# done

codec-policy
        name                            AllowG711
        allow-codecs                    PCMU PCMA telephone-event
        add-codecs-on-egress            PCMU PCMA telephone-event
        order-codecs                    PCMU PCMA telephone-event
        force-ptime                     disabled
        packetization-time              20
        dtmf-in-audio                   disabled

LYNC-ATT-IOT(codec-policy)# name ATT
LYNC-ATT-IOT(codec-policy)# allow-codecs (G729::vadoff G729 telephone-event RED:no CN:no
PCMU)
LYNC-ATT-IOT(codec-policy)# add-codecs-on-egress (G729::vadoff PCMU telephone-event)
LYNC-ATT-IOT(codec-policy)# order-codecs (G729::vadoff PCMU telephone-event)
LYNC-ATT-IOT(codec-policy)# dtmf-in-audio disabled
LYNC-ATT-IOT(codec-policy)# done

codec-policy
        name                            ATT
        allow-codecs                    G729::vadoff G729 telephone-event RED:no CN:no PCMU
        add-codecs-on-egress            G729::vadoff PCMU telephone-event
        order-codecs                    G729::vadoff PCMU telephone-event
        force-ptime                     disabled
        packetization-time              20
        dtmf-in-audio                   disabled
LYNC-ATT-IOT(codec-policy)# exit
LYNC-ATT-IOT(media-manager)# realm-config
LYNC-ATT-IOT(realm-config)# sel
identifier:
1: ATT s0p0:0           0.0.0.0
2: MS-Lync-Peer s1p0:0          0.0.0.0
selection: 1
LYNC-ATT-IOT(realm-config)#codec-policy ATT
LYNC-ATT-IOT(realm-config)# done
realm-config
        identifier                      ATT
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     enabled
```

```
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy                    voip-default
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        cac-failure-threshold           0
        untrust-cac-failure-threshold   0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy                    ATT
        codec-manip-in-realm            disabled
        codec-manip-in-network          disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
```

```
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@172.41.0.11
        last-modified-date              2012-03-06 13:31:20


LYNC-ATT-IOT(realm-config)# sel
identifier:
1: ATT s0p0:0           0.0.0.0
2: MS-Lync-Peer s1p0:0          0.0.0.0
selection: 2
LYNC-ATT-IOT(realm-config)#codec-policy AllowG711
LYNC-ATT-IOT(realm-config)#done

realm-config
        identifier                      MS-Lync-Peer
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s1p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        cac-failure-threshold           0
        untrust-cac-failure-threshold   0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
```

```
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy                    AllowG711
        codec-manip-in-realm            disabled
        codec-manip-in-network          disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@console
        last-modified-date              2012-02-02 16:36:03
```

Note: RTCP reporting is not support with transcoding. When transcoding feature is disabled, RTCP reporting is available.

16. SIP PRACK interworking and Media Handling

SIP PRACK Interworking

In order to establish an early media session for outbound calls, Lync Server 2013 gateway specification mandates the PSTN gateways to offer a reliable provisional response and for inbound calls offer INVITEs with a supported header The SBC can interwork and provide RFC 3262 PRACK interworking towards Lync and it is a mandatory configuration in all Oracle Communications Session Border Controller – Microsoft Lync deployments. For this, the following need to be configured:

- Configure option 100rel-interworking on the sip-interface facing mediation server
- Configure a sip-feature to pass the 100rel in supported and require headers
- Configure a manipulation to add a Require:100rel header in incoming SIP INVITE from mediation server and delete the Supported:100rel header

```
LYNC-ATT-IOT(session-router)# sip-interface
Lync-ATT-IOT(sip-interface)# sel
<realm-id>:
1: MS-Lync-Peer  192.168.2.130:5068
2: ATT 192.20.0.108:5060
```

```
selection: 1
LYNC-ATT-IOT(sip-interface)#options 100rel-interworking
```

Configure Sip-feature to pass Supported and Require headers in SIP messages

```
LYNC-ATT-IOT(session-router)#sip-feature
LYNC-ATT-IOT(sip-feature)#name 100rel
LYNC-ATT-IOT(sip-feature)#realm pstn
LYNC-ATT-IOT(sip-feature)# support-mode-inbound Pass
LYNC-ATT-IOT(sip-feature)# require-mode-inbound Pass
LYNC-ATT-IOT(sip-feature)# proxy-require-mode-inbound Pass
LYNC-ATT-IOT(sip-feature)# support-mode-outbound Pass
LYNC-ATT-IOT(sip-feature)# require-mode-outbound Pass
LYNC-ATT-IOT(sip-feature)# proxy-require-mode-outbound Pass
LYNC-ATT-IOT(sip-feature)#done

sip-feature
      name                          100rel
      realm                         pstn
      support-mode-inbound          Pass
      require-mode-inbound          Pass
      proxy-require-mode-inbound    Pass
      support-mode-outbound         Pass
      require-mode-outbound         Pass
      proxy-require-mode-outbound   Pass
```

The manipulation to add Require:100rel header will be configured in the next section.

Media Bypass handling

In order for Media Bypass to work, both Client and gateway (SBC) need to use the same RTP format, either SRTP (by default) or RTP. In default configuration of MS Lync, Lync client is required to use media encryption, so Media Bypass is mainly when media is encrypted (SRTP) and exchanged between Lync client and PSTN gateway (Oracle Enterprise Session Border Controller).

Media Bypass from Acme Packet series SBC's perspective is routing RTP traffic to an endpoint/Lync client on a private routable network directly (instead of RTP going through the mediation server). To enable the SBC to handle the media bypass feature in Lync, you will need to set restricted-latching to sdp in the core realm (facing mediation server). Select the core realm from the media-manager --- > realm-config configuration branch.

Note: This setting is recommended irrespective of the media bypass setting.

```
Lync-ATT-IOT(realm-config)#restricted-latching sdp
Lync-ATT-IOT(realm-config)#done
realm-config
        identifier                      MS-Lync-Peer
        description                     Mediation Server-facing(Outside)
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s1p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
```

```
        max-priority-bandwidth         0
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        cac-failure-threshold          0
        untrust-cac-failure-threshold  0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
        codec-policy
        codec-manip-in-realm           disabled
        codec-manip-in-network         disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
```

Recently, in some accounts where MS Lync and the Acme Packet series SBC are deployed for enterprise voice and SIP trunk termination to an enterprise, there have been complaints of the PSTN caller hearing a silence when a call is placed from PSTN to a Lync user on the enterprise especially when Media Bypass is enabled on MS Lync

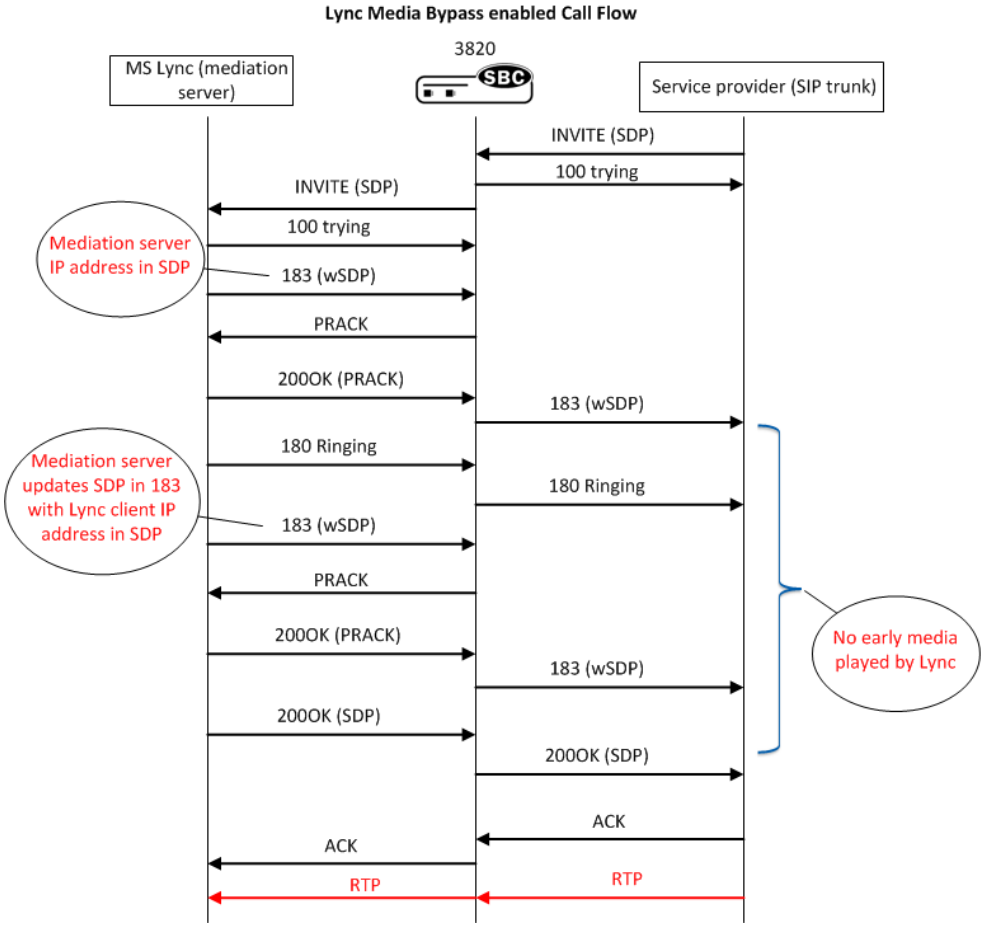
The configuration note below aims to explain this scenario briefly, steps taken to rectify this issue and proposed workaround by Oracle. The workaround is an interim solution while a permanent solution is being researched and developed by Oracle Communications Session Border Controller Engineering

Media Bypass

As explained earlier in the document, in order for Media Bypass to work, both Client and gateway (SBC) need to use the same RTP format, either SRTP (by default) or RTP. In default configuration of MS Lync, Lync client is required to use media encryption, so Media Bypass is mainly when media is encrypted (SRTP) and exchanged between Lync client and PSTN gateway (E-SBC).

Signaling between mediation server and SBC is a little different (Two 183s with SDP coming from mediation server) when media bypass is enabled on Lync.

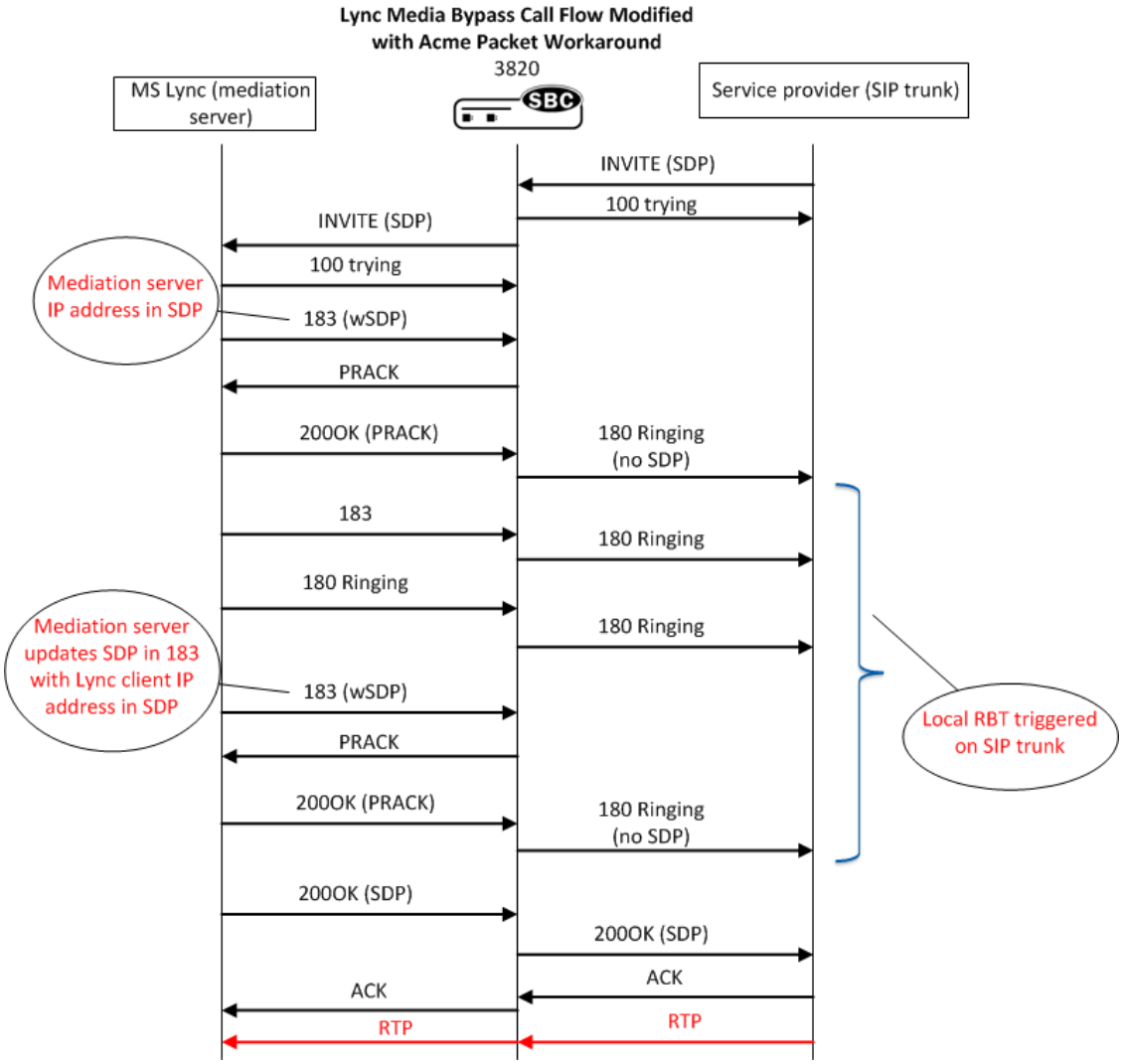
The following is the call flow:



Note: that after signaling 183 with SDP, Lync never plays any early media and expects gateway (E-SBD) to signal appropriately to the SIP Trunk provider to follow RFC 3960 and play local RBT. The second 183w SDP coming from Mediation server which is forwarded to the SIP trunk and stops the local RBT which was started after 180 Ringing was sent; hence PSTN caller would hear a silence before Lync client answers call.

Oracle Work Around

The interim solution is to present 180 ringing (convert all 183s on Lync side to 180 ringing towards SIP trunk and strip the SDP) to trigger RBT in ISUP. The call flow is modified with the help of Oracle's robust Sip Manipulation and Sip Response Map features to the following:



The following header rules needs to be included in the manipulation that is applied on the realm or sip-interface facing Lync to modify the signaling traffic sent from Lync.

```
        header-rule
                name                            delsupported
                header-name                     Supported
                action                          delete
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
        header-rule
                name                            addrequireinINVITE
                header-name                     Require
                action                          add
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value                       100rel
        header-rule
                name                            formod183
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value                       Stripsdp183 (the manipulation Stripsdp183 is
mentioned below)
```

```
sip-manipulation
        name                            Stripsdp183
        description                     For incoming 183 from Lync, strip SDP
        split-headers
        join-headers
        header-rule
                name                            check183
                header-name                     @status-line
                action                          store
                comparison-type                 pattern-rule
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            is183
                        parameter-name
                        type                            status-code
                        action                          store
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     183
                        new-value
        header-rule
                name                            delSDP
                header-name                     Content-Type
                action                          manipulate
                comparison-type                 case-insensitive
                msg-type                        any
                methods
                match-value                     $check183.$is183
                new-value
                element-rule
                        name                            del183SDP
```

```
                    parameter-name                  application/sdp
                    type                            mime
                    action                          delete-element
                    match-val-type                  any
                    comparison-type                 boolean
                    match-value
                    new-value
      header-rule
              name                            delContentType
              header-name                     Content-Type
              action                          manipulate
              comparison-type                 boolean
              msg-type                        any
              methods
              match-value                     $check183.$is183
              new-value
              element-rule
                      name                            delCT
                      parameter-name                  *
                      type                            header-param
                      action                          delete-header
                      match-val-type                  any
                      comparison-type                 case-sensitive
                      match-value
                      new-value
```

The following sip response map needs to be configured and applied on the sip interface facing ATT.

```
response-map
        last-modified-by                admin@10.0.221.18
        last-modified-date              2012-06-04 11:14:17
        name                            change183to180
        entries
                                        183 -> 180 (Ringing)
```

```
      sip-interface
              state                           enabled
              realm-id                        ATT
              description
              sip-port
                      address                         192.20.0.108
                      port                            5060
                      transport-protocol              UDP
                      tls-profile
                      multi-home-addrs
                      allow-anonymous                 agents-only
                      ims-aka-profile
                    ....
                  response-map                  change183to180
```

17. Configure Sip-manipulations and translation rules

In order to cater to AT&T's and Lync's call flow standards, we need to configure certain header manipulation rules (HMR). The sip-manipulation element can be found under the session-router element.

Lync typically sends mediation server FQDN in the Contact header with no username in the SIP URI which when the SBC forwards, is not acceptable by SIP trunk providers. The SBC's Sip manipulation feature updates the Contact header to include the username appropriately.

A manipulation, ChangeContact, will need to be configured to change the format of the CONTACT header which will then be referenced in the manipulation that is finally applied to the realm or sip-interface facing AT&T.

The manipulation consists of two header rules – StoreFromnumber and ChangeContact. The StoreFromnumber header rule stores the uri-user-only element in the From header which is then added as the uri-user in the Contact header in the ChangeContact header rule.

```
sip-manipulation
        name                            ChangeContact
        description
        split-headers
        join-headers
        header-rule
                name                            StoreFromnumber
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            StoreFromnumber_er
                        parameter-name
                        type                              uri-user-only
                        action                            store
                        match-val-type                    any
                        comparison-type                   case-sensitive
                        match-value
                        new-value
        header-rule
                name                            ChangeContact
                header-name                     Contact
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                              ChangeContact_er
                        parameter-name
                        type                              uri-user
                        action                            add
                        match-val-type                    any
                        comparison-type                   case-sensitive
                        match-value
                        new-value
$StoreFromnumber.$StoreFromnumber_er.$0
```

The manipulation ChangeContact is nested along with other header rules in the manipulation Privacy. The header rules From_Header, To_Header, PAI_Header, PPI_Header, RPI_Header, Refer_header and ReferredTo replace the ip address to hide the network topology. The header rule - Changesendonlytosendrecv is required to enable the end user hear MOH in call hold/resume scenarios. This header rule changes the a=sendonly attribute on the INVITE for hold from Lync to a=sendrecv towards AT&T. The rule manipContentType is added to deletes the lines - a=label:Audio and b=CT:1000 from SDP. In order to allow call forwarding to 8YY numbers, AT&T requires that the History-info header be deleted and a Diversion header be added. To implement this signaling, we configure the header rules – HistRegex, AddDiversion, delHist and normDiv.

```
        sip-manipulation
        name                            Privacy
        description
        split-headers
```

```
        join-headers
        header-rule
                name                            From_Header
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            From_header
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            To_Header
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            To_header
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP

        header-rule
                name                            Changesendonlytosendrecv
                header-name                     Content-Type
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            sendonlytosendrecv
                        parameter-name                  application/sdp
                        type                            mime
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     a=sendonly
                        new-value                       a=sendrecv

        header-rule
                name                            PAI_Header
                header-name                     P-Asserted-Identity
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
```

```
                element-rule
                        name                            PAI_Local_IP
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            PPI_Header
                header-name                     P-Preferred-Identity
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            PPI_Local_IP
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            RPI_Header
                header-name                     Remote-Party-ID
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            RPI_header
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP

        header-rule
                name                            Contact
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value                       ChangeContact
        header-rule
                name                            Refer_header
                header-name                     Referred-By
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            referredbyhdr
```

```
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       $LOCAL_IP
        header-rule
                name                            ReferredTo
                header-name                     Refer-To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            refertohdr
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP
        header-rule
                name                            manipContentType
                header-name                     Content-Type
                action                          manipulate
                comparison-type                 pattern-rule
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            deleteB
                        parameter-name                  application/sdp
                        type                            mime
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     b=CT:.*(\n|\r\n)
                        new-value
                element-rule
                        name                            deleteLABEL
                        parameter-name                  application/sdp
                        type                            mime
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     a=label:Audio(\n|\r\n)
                        new-value
        header-rule
                name                            HistRegex
                header-name                     History-Info
                action                          store
                comparison-type                 pattern-rule
                msg-type                        request
                methods                         INVITE
                match-value                     ()
                new-value
                element-rule
                        name                            GetUser
                        parameter-name
                        type                            uri-user
                        action                          store
```

```
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value
                        new-value
                element-rule
                        name                            GetHost
                        parameter-name
                        type                            uri-host
                        action                          store
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value
                        new-value
        header-rule
                name                            AddDiversion
                header-name                     Diversion
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $HistRegex
                new-value
<sip:+$HistRegex[0].$GetUser.$0+@+$HistRegex[0].$GetHost.$0+>
        header-rule
                name                            delHist
                header-name                     History-Info
                action                          delete
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
        header-rule
                name                            normDIv
                header-name                     diversion
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            normDivelem
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
```

The sip-manipulation then needs to be applied on the realm or sip-interface or session-agent towards the ATT trunk side. We apply it on the sip-interface here:

```
LYNC-ATT-IOT(session-router)# sip-interface
Lync-ATT-IOT(sip-interface)# sel
<realm-id>:
1: MS-Lync-Peer  192.168.2.130:5068
2: ATT 192.20.0.108:5060

selection: 2
Lync-ATT-IOT(sip-interface)# out-manipulationid Privacy
Lync-ATT-IOT(sip-interface)# done
```

In order to complete the calls successfully per AT&T's signaling specifications, we need to configure manipulation rules on the realm facing Lync. The manipulations are mentioned below.

The sip-manipulation NATting ensure topology hiding.

```
sip-manipulation
        name                            NATting
        description
        split-headers
        join-headers
        header-rule
                name                            From
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            From_header
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            To
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                            To
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_IP
```

For simultaneous ringing, the following manipulation is configured

```
sip-manipulation
        name                            ATT-Simulring
        description                     HMR for simul ring towards Lync
        split-headers
        join-headers
        header-rule
                name                            getTo
                header-name                     To
                action                          store
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            getTag
                        parameter-name                  tag
```

```
                type                            header-param
                action                          store
                match-val-type                  any
                comparison-type                 pattern-rule
                match-value
                new-value
        header-rule
                name                            checkHoldSdp
                header-name                     Content-Type
                action                          store
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     !$getTo.$getTag
                new-value
                element-rule
                        name                            checkIP
                        parameter-name                  application/sdp
                        type                            mime
                        action                          store
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value                     \Rc=IN IP4 0\.0\.0\.0\b
                          new-value
        header-rule
                name                            fixSdptest
                header-name                     Content-Type
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $checkHoldSdp.$checkIP
                new-value
                element-rule
                        name                            replaceIP
                        parameter-name                  application/sdp
                        type                            mime
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     \Rc=IN IP4 (0\.0\.0\.0)\b[[:1:]]
                        new-value                       $LOCAL_IP
        header-rule
                name                            checkmodinactive
                header-name                     Content-Type
                action                          store
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     !$getTo.$getTag
                new-value
                element-rule
                        name                            checkstate
                        parameter-name                  application/sdp
                        type                            mime
                        action                          store
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     \Ra=inactive\b
                        new-value
        header-rule
                name                            fixinactive
                header-name                     Content-Type
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
```

```
                methods                         INVITE
                match-value                     $checkmodinactive.$checkstate
                new-value
                element-rule
                        name                            replaceAttribute
                        parameter-name                  application/sdp
                        type                            mime
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     \Ra=inactive\b
                        new-value
```

The manipulations NATting and ATT-Simulring need to be applied to manipulate the signaling sent to devices in the realm MS-Lync-Peer. Hence the following nested sip-manipulation Lyncprivacy is configured.

```
sip-manipulation
        name                            Lyncprivacy
        description                     NAT plus recvonly to inactive
        split-headers
        join-headers
        header-rule
                name                            doNATforlync
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value                       NATting
        header-rule
                name                            manipPPreferredIdentity
                header-name                     P-Preferred-Identity
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value
                element-rule
                        name                      PPreferredIdentityURIHost
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            simulring
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value                       ATT-Simulring
```

This manipulation is applied on the sip-interface or realm facing Lync.

```
LYNC-ATT-IOT(session-router)# sip-interface
Lync-ATT-IOT(sip-interface)# sel
<realm-id>:
1: MS-Lync-Peer  192.168.2.130:5068
Note:2: ATT 192.20.0.108:5060

selection: 1
Lync-ATT-IOT(sip-interface)# out-manipulationid Lyncprivacy
Lync-ATT-IOT(sip-interface)# done
```

During call transfer to a PSTN party, the transfer completes but the calling party does not hear a ring back tone during the process of transfer. The INVITE Lync sends to the SBC to initiate the transfer contains the SDP attribute, a=inactive which is forwarded to the trunk and as a result of which the SBC cannot play the ring back tone to the original PSTN caller (while call is being transferred). A sendonly attribute is required for MoH and transfer scenarios for the calling party to be able to hear ringback or MoH when it is kept on hold. The SBC is able to signal appropriately towards the SIP trunk by changing the a=inactive SDP attribute in the INVITE to sendonly towards PSTN. This attribute needs to be changed to a=sendrecv when it is sent to AT&T so that the ringback tone or the MOH can be heard.

Sip manipulations are configured to make the necessary changes. The manipulation Changeinactosendonly is configured to change the SDP attribute from a=inactive to a=sendonly in the INVITEs sent to the calling party for transfer.

```
sip-manipulation
        name                            Changeinactosendonly
        description                     Change inactive to sendonly for pstn tran
        split-headers
        join-headers
        header-rule
                name                            changeSDP
                header-name                     Content-Type
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            inacttosendonly
                        parameter-name                  application/sdp
                        type                            mime
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     a=inactive
                        new-value                       a=sendonly
```

Note:

To change the a=sendonly to a=sendrecv before sending the INVITE to AT&T, we have a header rule `Changesendonlytosendrecv` included in the manipulation Privacy that is applied on the sip-interface facing AT&T.

A nested sip manipulation Forearlymedia is configured to include the header rules mentioned in the section "SIP PRACK interworking and Media Handling" and the manipulation Changeinactosendonly

```
sip-manipulation
        name                            Forearlymedia
        description
        split-headers
        join-headers
        header-rule
                name                            delsupported
                header-name                     Supported
                action                          delete
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
        header-rule
                name                            addrequireinINVITE
                header-name                     Require
                action                          add
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value                       100rel
  header-rule
                name                            mod183
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value                       Stripsdp183
        header-rule
                name                            inactosendonly
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        request
                methods
                match-value
                new-value                       Changeinactosendonly
```

The sip-interface or realm facing Lync is configured with this manipulation as the in-manipulationid.

```
LYNC-ATT-IOT(session-router)# sip-interface
Lync-ATT-IOT(sip-interface)# sel
<realm-id>:
1: MS-Lync-Peer  192.168.2.130:5068
Note:2: ATT 192.20.0.108:5060

selection: 1
Lync-ATT-IOT(sip-interface)# in-manipulationid Forearlymedia
Lync-ATT-IOT(sip-interface)# done
```

18. Verify configuration integrity

You will verify your configuration referential integrity before saving and activating it with the **verify-config** command. This command is available from Superuser Mode. To enter the Superuser Mode from steering-pool, you issue the **exit** command three times.

```
LYNC-ATT-IOT(session-agent)# exit
LYNC-ATT-IOT(session-router)# exit
LYNC-ATT-IOT(configure)# exit
LYNC-ATT-IOT# verify-config
------------------------------------------------------------------------

Verification successful! No errors nor warnings in the configuration
```

19. Save and activate your configuration

You will now save your configuration with the save-config command. This will make it persistent through reboots, but it will not take effect until after you issue the activate-config command.

```
LYNC-ATT-IOT# save-config
checking configuration
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.

LYNC-ATT-IOT# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43, VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45, VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

The SBC configuration is complete.

Test Results

Once the Lync Server 2013 and the Oracle Communications Session Border Controller have been configured, the final phase is to test connectivity and the SIP trunk interface. A comprehensive test plan was executed which included some of the test cases mentioned below

- Basic inbound/outbound calls to/from Lync
- Call hold and resume with Music On Hold
- Attended and unattended call transfers
- Conferencing – both ad-hoc and using AT&T IP Teleconferencing Service
- Network based call forwarding scenarios
- Network based Simultaneous and Sequential ringing features
- Calls to confirm privacy of the calling number if required

Troubleshooting Tools

If you find that there are issues with call setup, signaling, etc. or have problems with the test cases, there are a few tools available for Windows Server, Lync Server, and the Oracle Enterprise Session Border Controller like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting some minor issues you may encounter.

Microsoft Network Monitor (NetMon)

NetMon is a network protocol analyzer which is freely downloadable from Microsoft. It can be found at www.microsoft.com/downloads. NetMon could be installed on the Lync Server mediation server, the Lync Server Standard Edition server, or Enterprise Edition front end server.

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org. Wireshark could be installed on the Lync Server mediation server, the Lync Server Standard Edition server, or MCS Enterprise Edition front end server.

Event Viewer

There are several locations in the event viewer where you can find valuable information to aid in troubleshooting issues with your deployment.

With the requirement that there is a completely functioning Lync Server with Enterprise Voice deployment in place, there are a few areas in which one would use the Event Viewer for troubleshooting:

- The Enterprise Voice client
- The Lync Front End server
- Lync Mediation server

Oracle Enterprise Session Border Controller

The Oracle Enterprise Session Border Controller provides a rich set of statistical counters available from the ACLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces.

Resetting the statistical counters, enabling logging and restarting the log files.

At the Oracle Enterprise Session Border Controller Console:

```
ACME1A# reset sipd
ACME1A# notify sipd siplog
ACME1A# notify sipd debug
enabled SIP Debugging
ACME1A# notify all rotate-logs
```

Examining the log files.

Note: You will FTP to the management interface of the Oracle Communications Session Border Controller with the username user and user mode password (the default is **"acme"**).

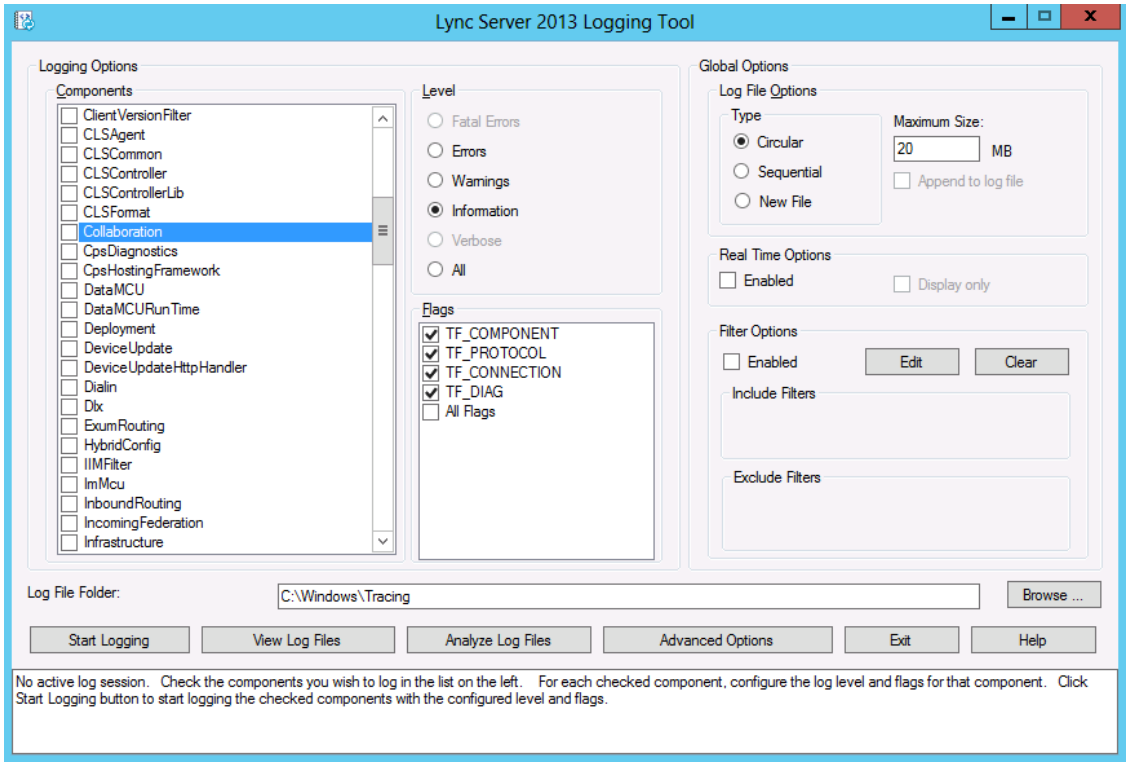
```
C:\Documents and Settings>ftp 192.168.5.24
Connected to 192.168.85.55.
220 ACME1A FTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
331 Password required for user.
Password: acme
230 User user logged in.
ftp> cd /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
```

```
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353 bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (204681 bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

You may now examine the log files with the text editor of your choice.

Lync Server Logging Tool

The Lync Server 2013 Logging Tool provides internal traces and messaging between different Lync Server 2013 elements like Front-end, Mediation server, Lync Clients, etc. File name is OCSReskit.msi. Once installed, it can be accessed from any one of the Lync Server servers by running Start/Microsoft Lync Server 2013/Lync Server Logging Tool.



Normative References

Acme Packet 4000 S-C6.2.0 ACLI Configuration Guide, 400-0061-62, Dec 2010.

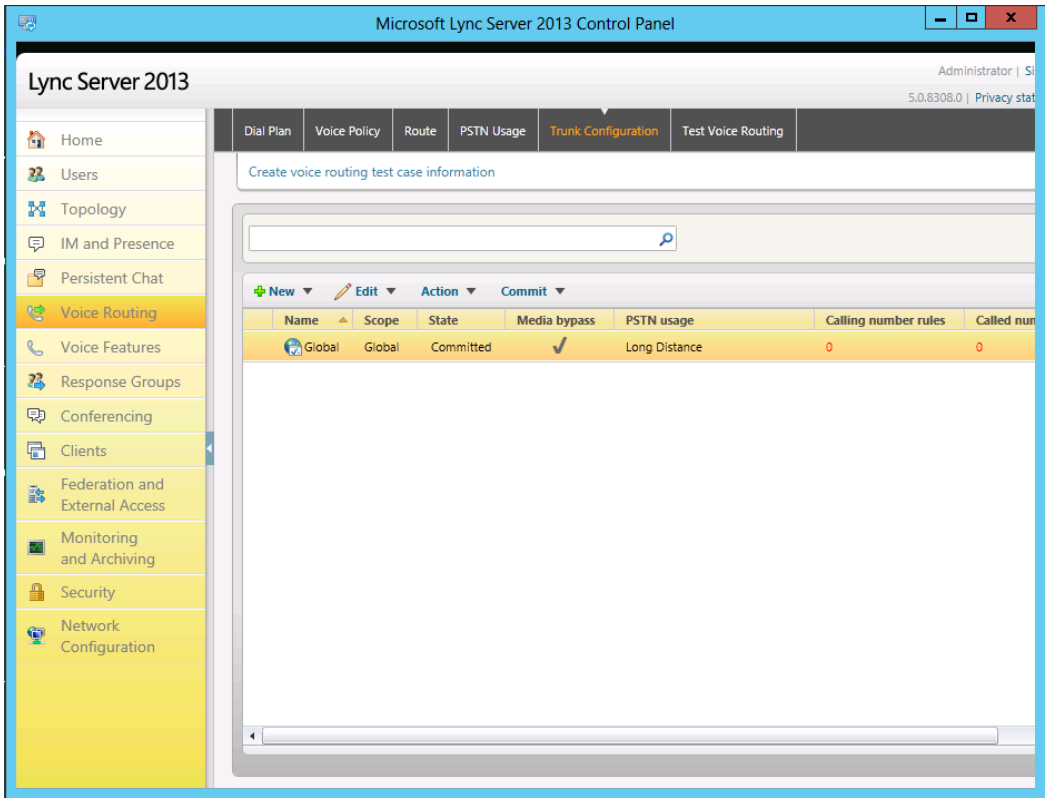
Appendix

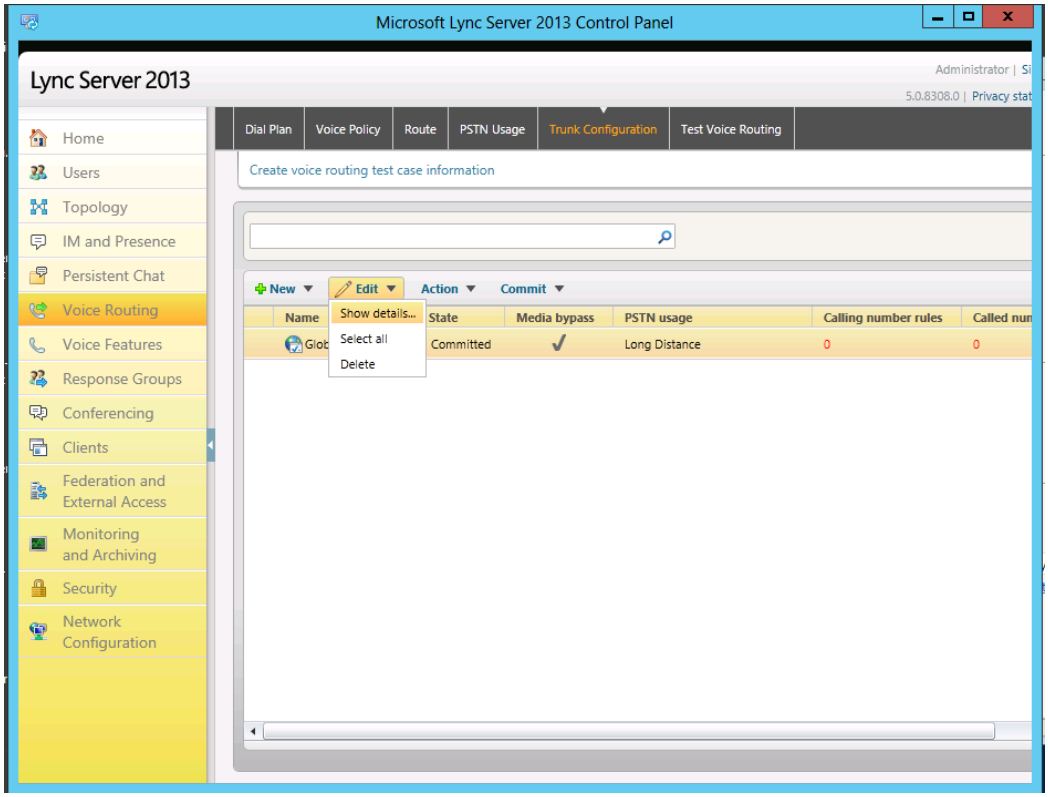
Call Transfer Scenario with REFER enabled

For the deployments that support REFER for call transfers, additional configuration needs to be implemented. This appendix includes the steps to enable REFER on Lync and SBC configuration to support the REFER based transfers.

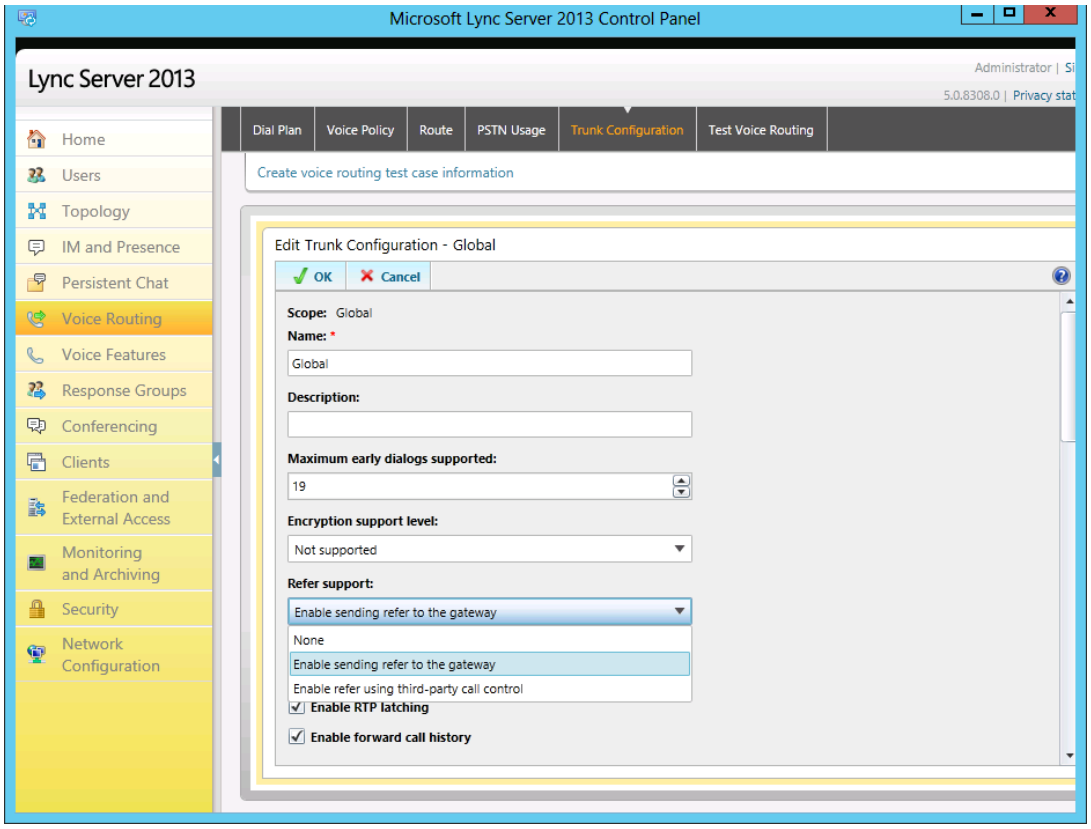
Lync Configuration:

This configuration is done in the Trunk Configuration section of the Lync Server Control Panel.





Click on Edit and select Show details



In the Edit Trunk Configuration window, select **Enable Sending refer to the gateway** under **Refer support.** Click OK and then commit the configuration.

Refer support has been enabled on Lync.

Configuring Refer handling on the SBC

In the realm facing Lync, the parameter refer-call-transfer needs to enabled.

```
Lync-ATT-IOT(realm-config)# refer-call-transfer enabled
Lync-ATT-IOT(realm-config)# done
realm-config
        identifier                      MS-Lync-Peer
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s1p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
```

```
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        cac-failure-threshold           0
        untrust-cac-failure-threshold   0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             enabled
        refer-notify-provisional        none
        dyn-refer-term                  disabled
        codec-policy                    Lync
        codec-manip-in-realm            disabled
        codec-manip-in-network          enabled
        constraint-name
        call-recording-server-id
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
```

Lync Server 2013 authorizes transfers of all Lync initiated calls whether it is Lync to Lync or Lync to PSTN. Oracle Communications Session Border Controller provides REFER handling by terminating the REFER from Lync and generating an INVITE for the referred party back towards the Lync Mediation server. Lync then processes the INVITE, authorizes the call transfer and sends either a new

INVITE (for calls transferred to PSTN) to the SBC or transfers call internally to the transferred Lync client

To handle the call transfer and refer scenarios – when Lync client 1 refers/transfers the call to Lync Client 2 or to a party on the PSTN, we will need two routes to route to the two mediation servers depending on the referred party.

```
local-policy
from-address                  *
      to-address                          lync2013med2.acmepacket.net
      source-realm                      ATT
      description                     for referred party OP1-0704.st02.loc
      activate-time                    N/A
      deactivate-time                  N/A
      state                            enabled
      policy-priority                  none
      last-modified-by                 admin@10.176.33.30
      last-modified-date               2011-06-22 14:46:32
      policy-attribute
              next-hop                         lync2013med2.acmepacket.net
              realm                            MS-Lync-Peer
              action                           replace-uri
              terminate-recursion              disabled
              carrier
              start-time                       0000
              end-time                         2400
              days-of-week                     U-S
              cost                             0
              app-protocol                     SIP
              state                            enabled
              methods
              media-profiles
              lookup                           single
              next-key
              eloc-str-lkup                    disabled
              eloc-str-match


local-policy
from-address                  *
      to-address                          lync2013med1.acmepacket.net
      source-realm                      ATT
      description                     for referred party OP1-0704.st02.loc
      activate-time                    N/A
      deactivate-time                  N/A
      state                            enabled
      policy-priority                  none
      last-modified-by                 admin@10.176.33.30
      last-modified-date               2011-06-22 14:47:35
      policy-attribute
              next-hop                         lync2013med1.acmepacket.net
              realm                            MS-Lync-Peer

              action                           replace-uri
            terminate-recursion              disabled
              carrier
              start-time                       0000
              end-time                         2400
              days-of-week                     U-S
              cost                             0
              app-protocol                     SIP
              state                            enabled
              methods
              media-profiles
```

```
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

Oracle ATT – Microsoft Lync
February 2014

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together