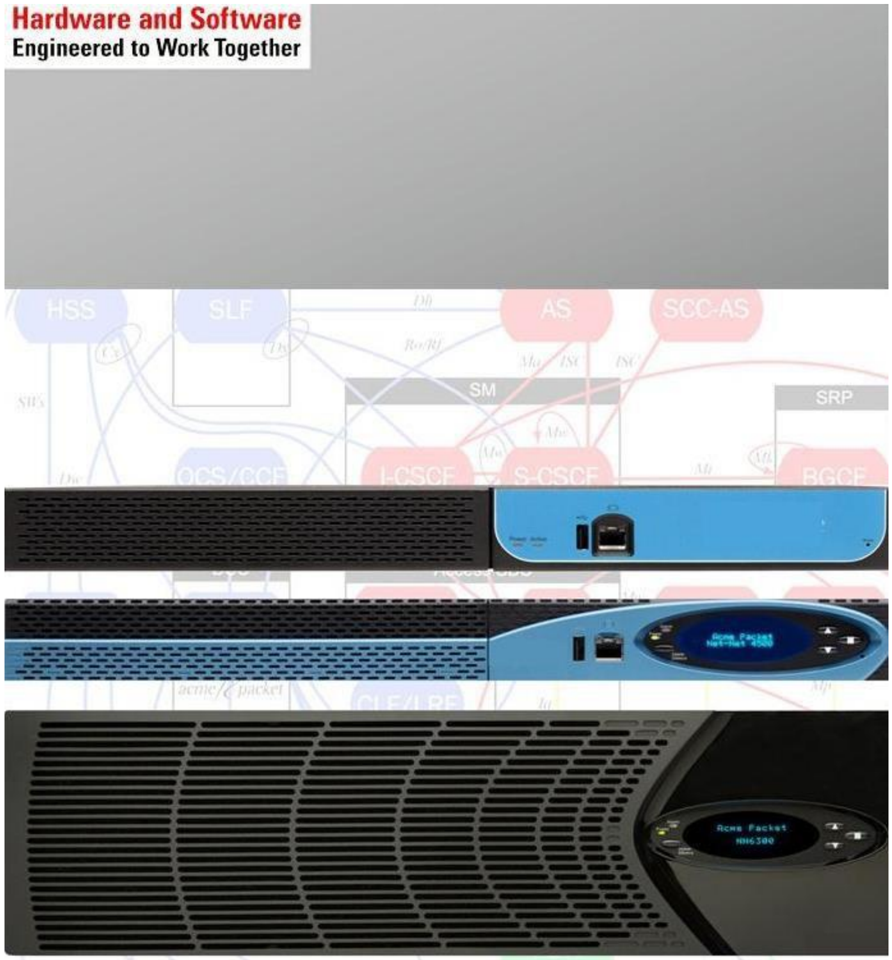


Oracle Enterprise Session Border Controller- Acme Packet 3820 and Microsoft Lync 2013 for Enterprise SIP Trunking

Technical Application Note

Table of Contents

Document Overview

Microsoft Lync Server 2013 offers the ability to connect to Internet telephony service providers (ITSP) using an IP-based SIP trunk. This reduces the cost and complexity of extending an enterprise's telephony system outside its network borders. Microsoft recommends an E-SBC to provide interoperability and service assurance when connecting the Lync environment to a SIP trunk service. Acme Packet Net-Net Enterprise Session Director (Net-Net ESD) Session Border Controllers (SBCs) play an important role in SIP trunking as they are used by many ITSPs and enterprises as part of their SIP trunking infrastructure. Acme Packet solutions can also be used for enterprise Session Management applications involving Lync. In Session Management applications, the same methods described in this guide for interfacing with the Lync environment via SIP trunking apply.

This step-by-step deployment guide has been prepared as a means of ensuring that SIP trunking between Lync Server and Acme Packet SBCs is configured in the optimal manner. This guide can be used to support the SIP trunking reference topologies that are documented by Microsoft and Acme Packet in this TechNet article:

"Lync Server 2010 & OCS 2007 R2 Support for Acme Packet Session Border Controllers" http://blogs.technet.com/b/nexthop/archive/2011/02/21/support-for-acme-packet-session-border-controllers-in-lync-server-and-2010-communications-server-2007-r2.aspx.

The Net-Net ESD is fully qualified by Microsoft under its Unified Communications Open Interoperability Program. It should be noted that while this deployment guide focuses on the optimal configurations for the Acme Packet Net-Net ESD SBC in a Lync Server environment, the same SBC configuration model can also be used for Microsoft OCS 2007 R2 environments. In addition, it should be noted that the Net-Net SD configuration provided in this guide focuses strictly on the Lync Server associated parameters. Many Net-Net ESD users may have additional configuration requirements that are specific to other applications. These configuration items are not covered in this guide. Please contact your Acme Packet representative for any additional information required. Additionally, the screenshots pertaining to Lync Server 2013 configuration and setup are taken to give an overview of how the setup is built and may or may not correspond to the actual configuration described elsewhere in the document.

For additional information on Lync Server, please visit the URL below:

http://www.microsoft.com/lync

For additional information on Acme Packet SBCs and Lync Server, please visit the URL below:

http://www.acmepacket.com/lync

Note: This document is to be used with Acme Packet Session Director and Enterprise Session Director platforms operating the C-series software. This includes the Net-Net 3820, 4500, and Enterprise Session Director Server Edition. For deployments involving other Acme Packet products, please contact your Acme Packet representative.

Inroduction

Audience

This is a technical document intended for engineers with the purpose of configuring both the Net-Net ESD SBC and the Lync Server 2013. There will be steps that require navigating Microsoft Windows Server as well as the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Requirements

- Fully functioning Lync Server deployment, including Active Directory and DNS
- A dedicated Mediation Server for the SIP trunking connection
- Acme Packet Net-Net SD running software SCx6.2.0m6p1 or later

Architecture

The following reference architecture shows a logical view of the connectivity between Lync Server and the Net-Net SD.

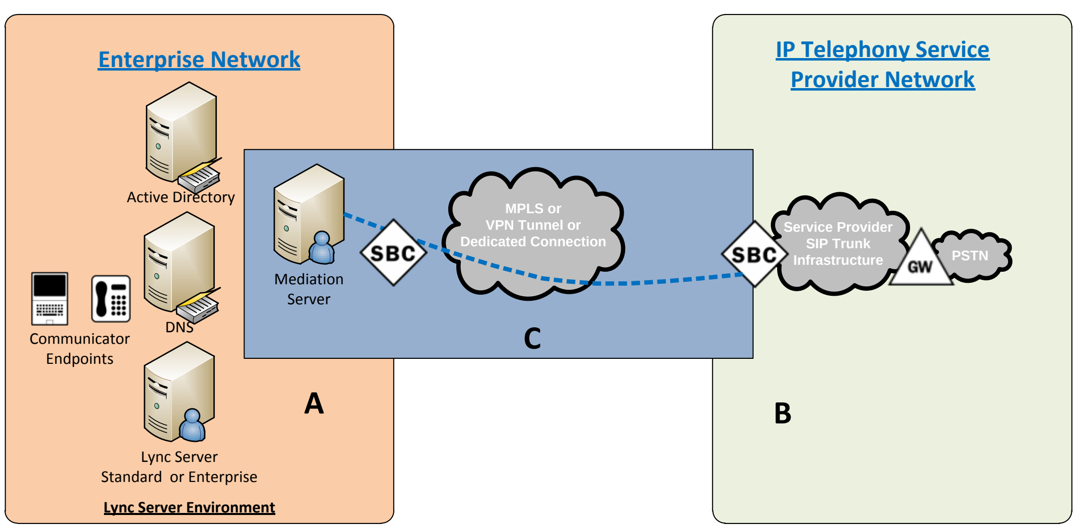


Figure 1 – Logical Reference Architecture

Area A represents the customer's on-premise infrastructure, which includes the Active Directory, DNS and Lync Server systems. Area B represents the service provider infrastructure which provides PSTN service via the SIP trunk. Area C represents the integration of these two environments over an IP network. This could be, through a VPN tunnel over the Internet, an MPLS managed network, or even a dedicated physical connection. The Lync Server Mediation Server and the Net-Net SD are the edge components that form the boundary of the SIP trunk. The configuration, validation and troubleshooting of the areas B and C is the focus of this document and will be described in three phases:

- Phase 1 – Configure Lync Server 2013 (define topology, pool, mediation server, add PSTN gateway and routes)
  - Phase 2 – Configure the Session Director (configure interfaces, routing, TLS/encryption)
  - Phase 3 – Test connectivity

Phase I – Configure Lync Server 2013

There are two parts for configuring Lync Server to operate with the Net-Net SD:

- Adding the Net-Net ESD as a PSTN gateway to the Lync Server infrastructure and
- Creating a route within the Lync Server infrastructure to utilize the SIP trunk connected to the Net-Net ESD

Requirements

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.

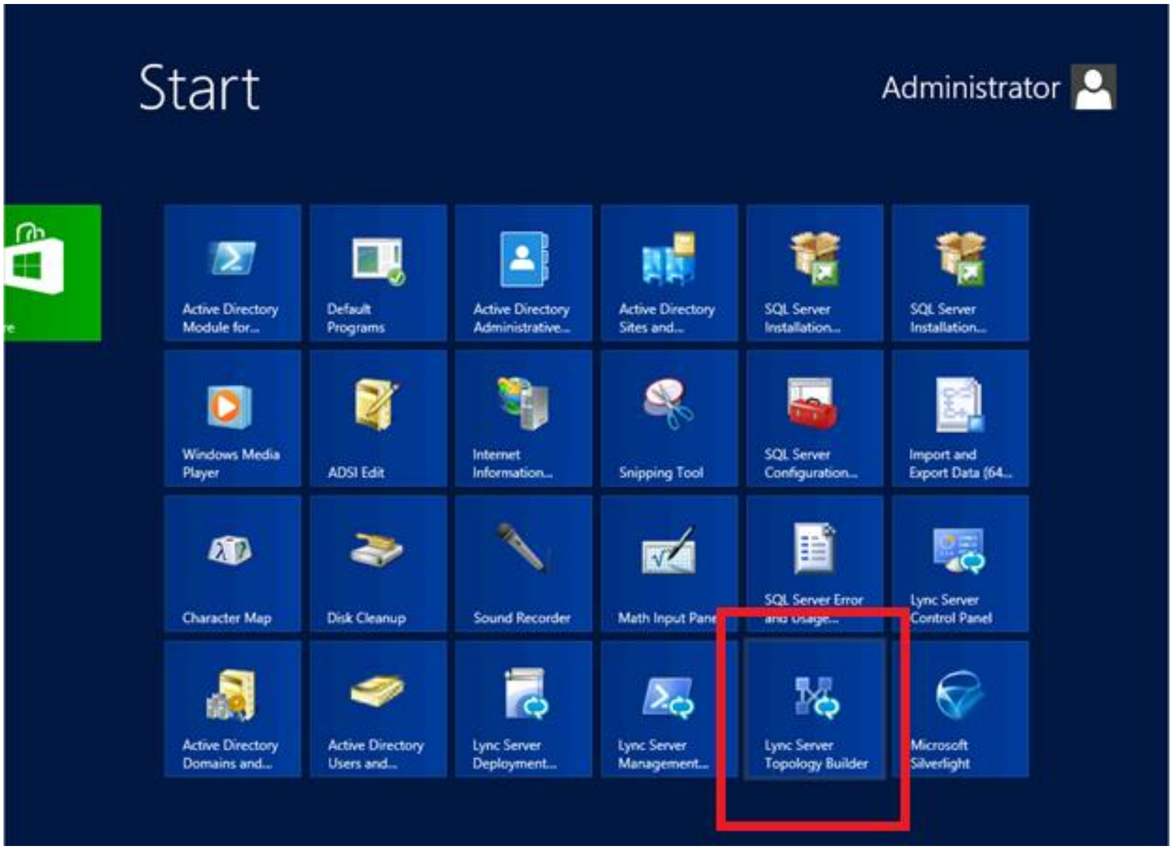
Adding the PSTN Gateway

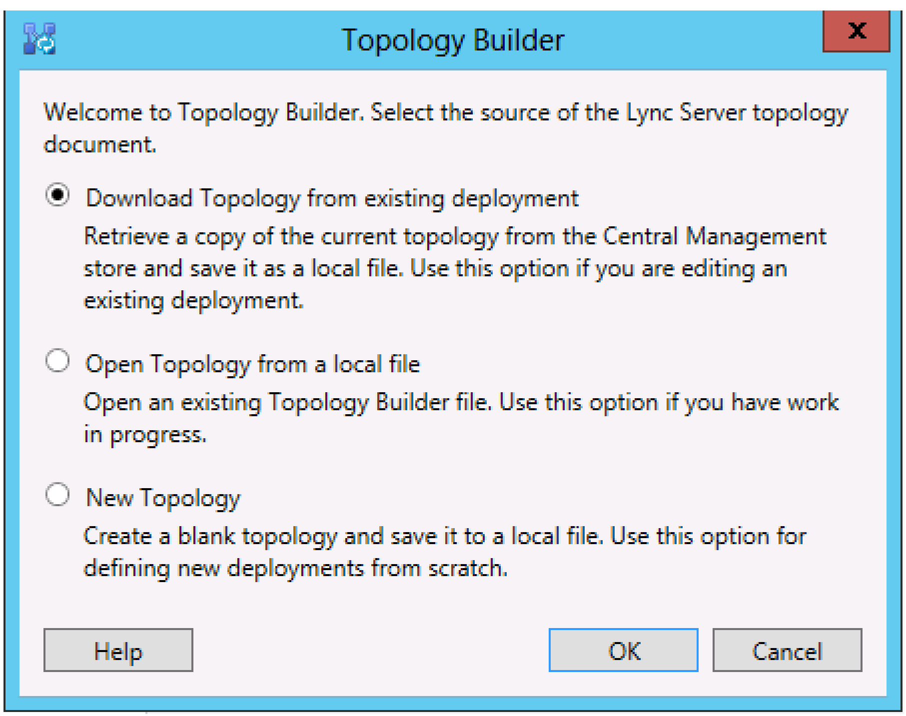
What you will need:

- IP address of Mediation Server external facing NIC
- IP address to be used for the Net-Net SD external facing port
- Rights to administer Lync Server Topology Builder
- Access to the Lync Server Topology Builder

Steps to add the PSTN gateway

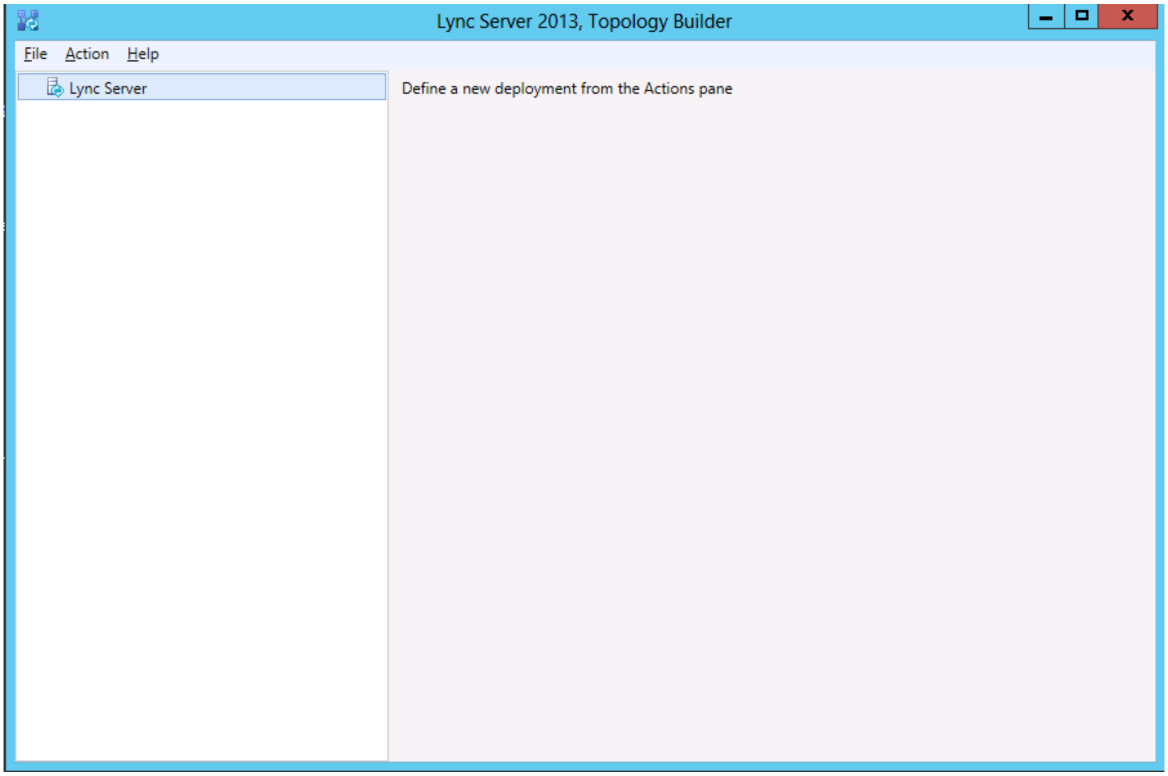
1. On the server where the Topology Builder is located start the console.
2. From the Charms Bar **Start**, select **Lync Server Topology Builder**

3. 

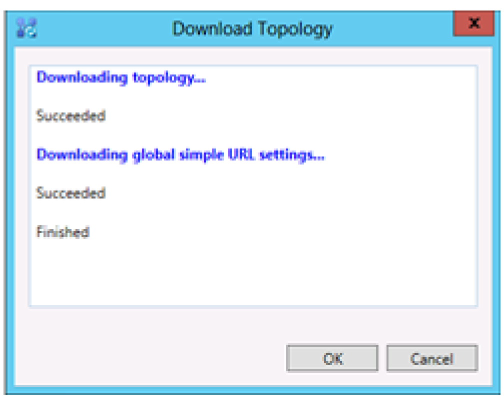


You will now be at the opening screen in the Topology Builder.

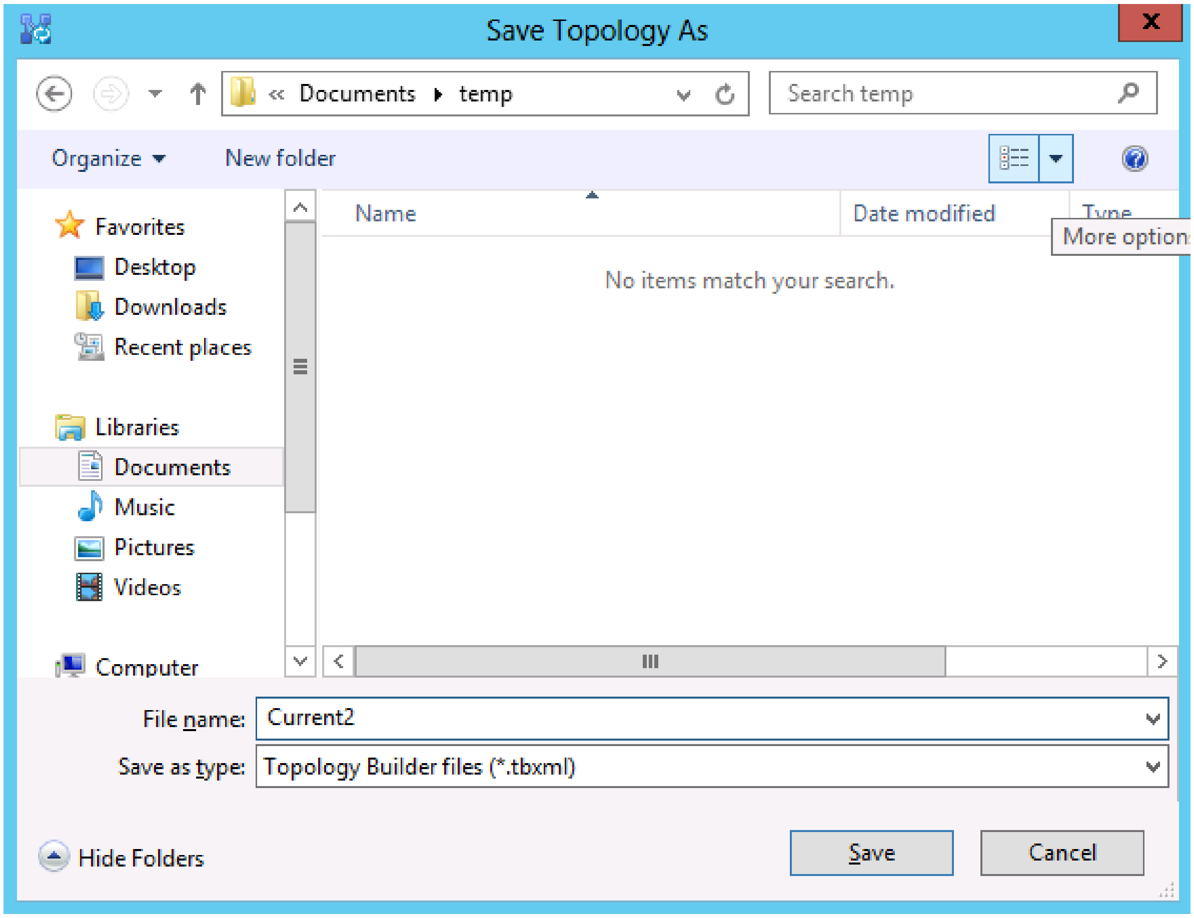
4. Click on the **Cancel** button.



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

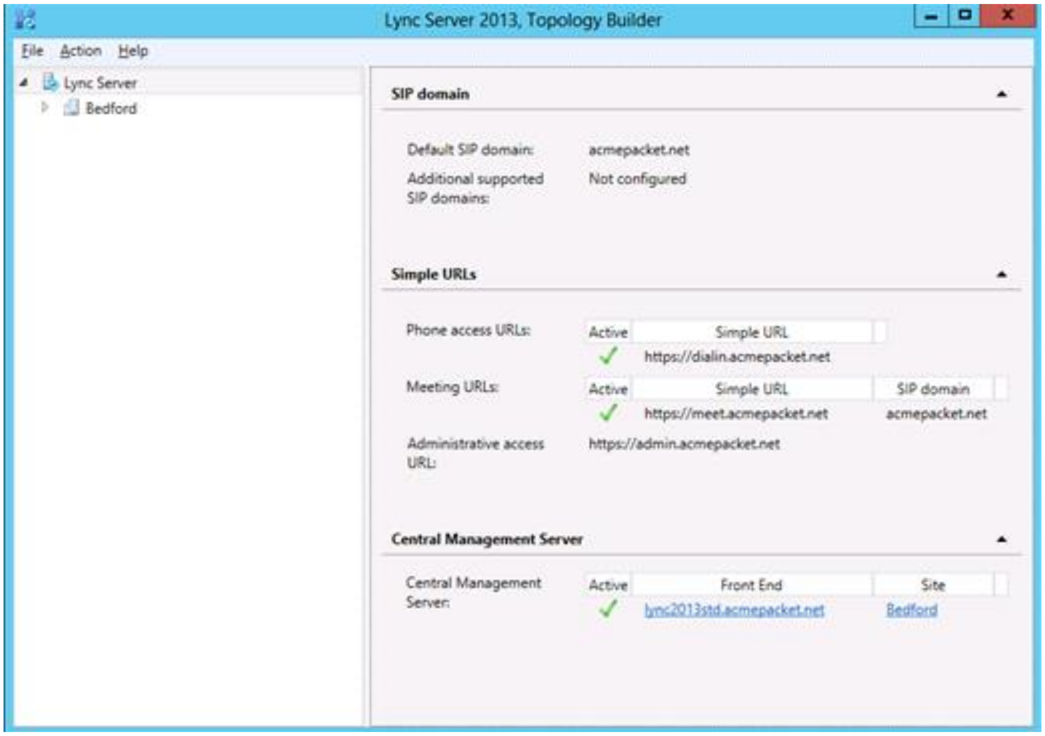


6. You will then see a screen showing that you have successfully imported the topology. Click the **Ok** button.

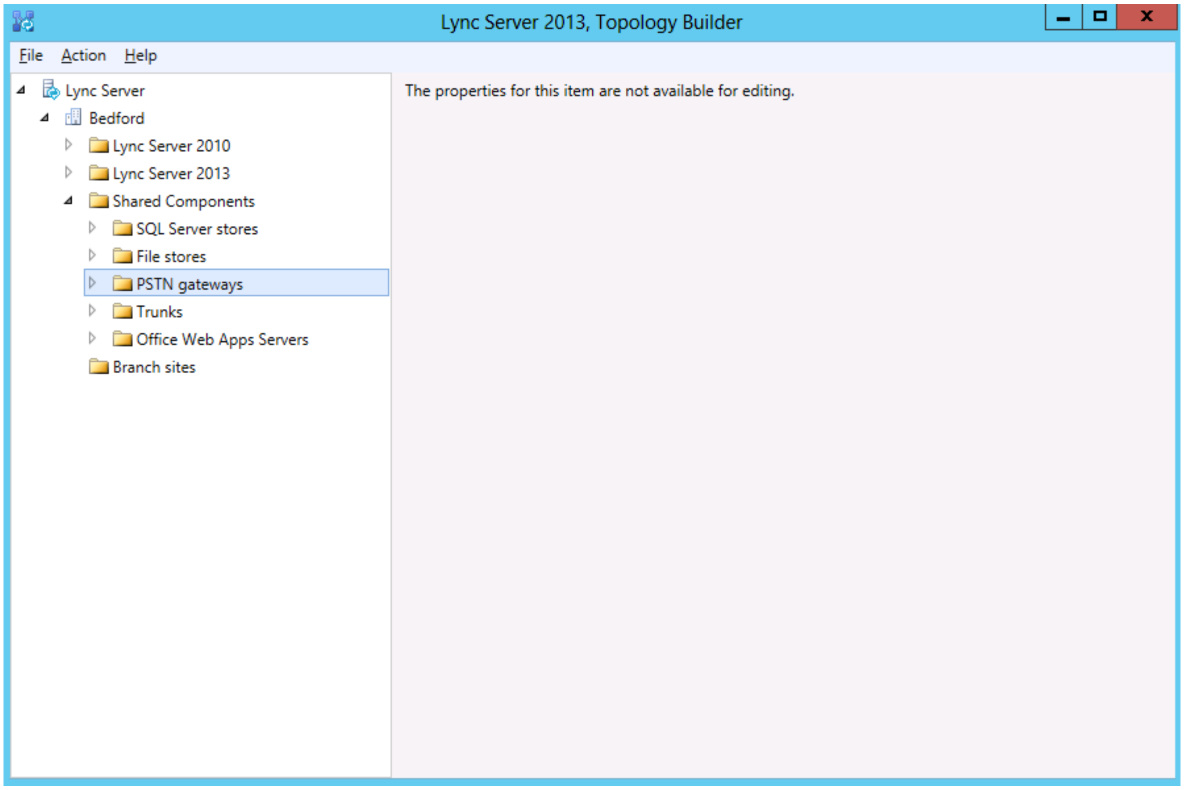


7. Next you will be prompted to save the topology which you have imported.
8. You should revision the name or number of the topology according to the standards used within the enterprise.
   Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make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

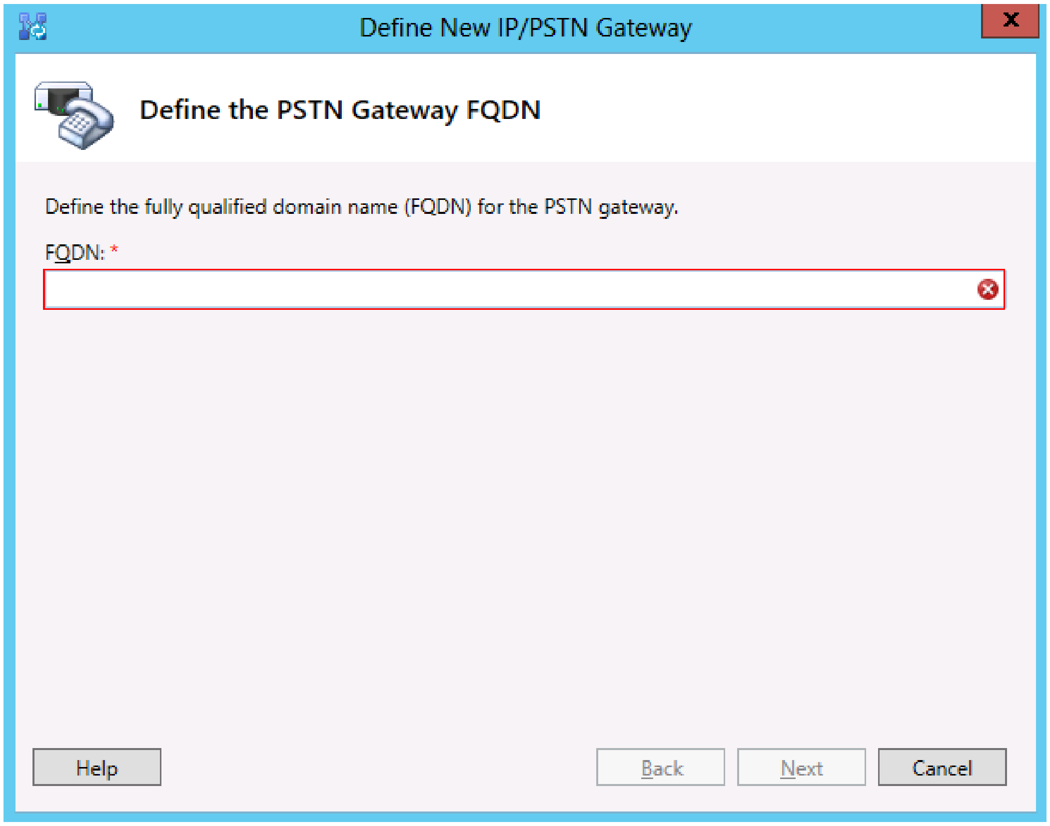
You will now see the topology builder screen with the enterprise's topology imported.

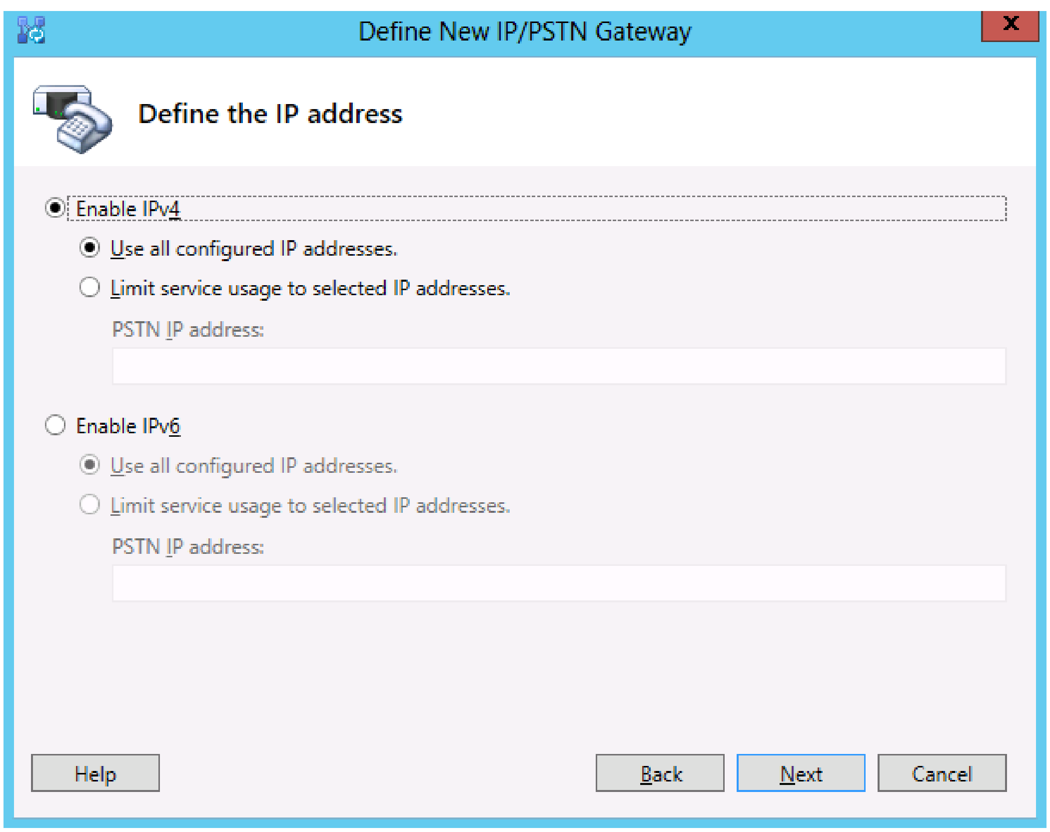

Lync Server 2013, Topology Builder
File Action Help
Lync Server
Bedford
SIP domain
Default SIP domain: acmepacket.net
Additional supported SIP domains: Not configured
Simple URLs
Phone access URLs:
Active Simple URL
https://dialin.acmepacket.net
Meeting URLs:
Active Simple URL SIP domain
https://meet.acmepacket.net acmepacket.net
Administrative access URL: https://admin.acmepacket.net
Central Management Server
Central Management Server:
Active Front End Site
lync2013std.acmepacket.net Bedford

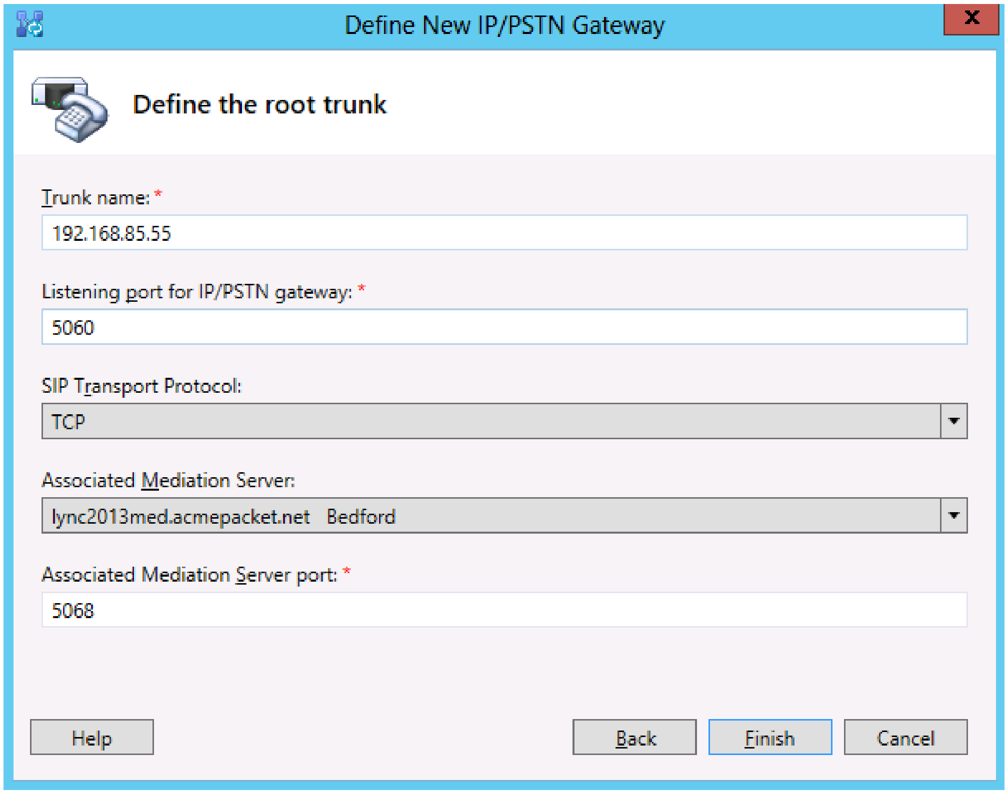
10. In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is **Test**. Then click on the **PSTN Gateways**.



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

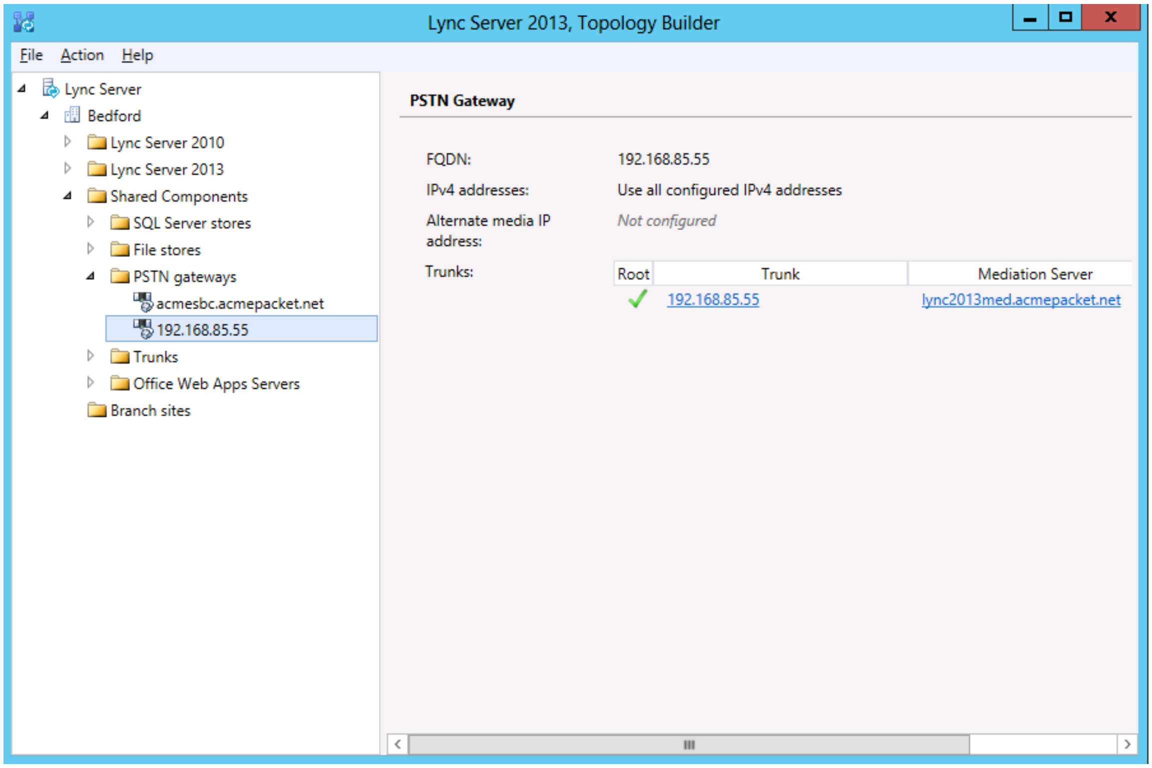

Define New IP/PSTN Gateway
Define the PSTN Gateway FQDN
Define the fully qualified domain name (FQDN) for the PSTN gateway.
FQDN: *
Help
Back
Next
Cancel


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



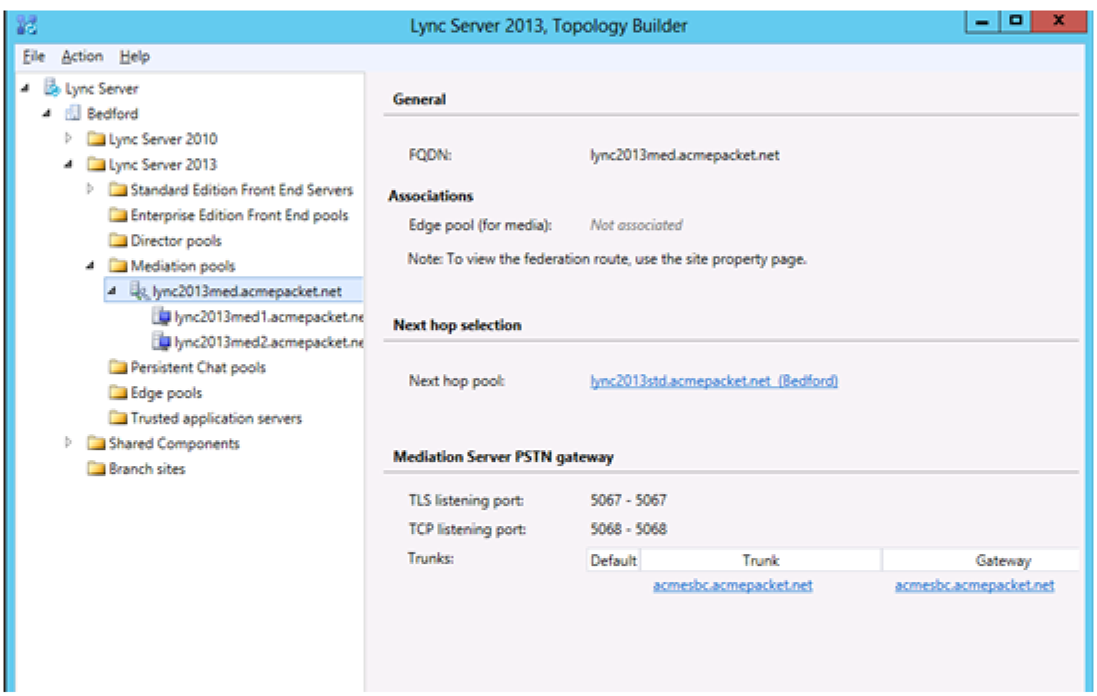
12. Enter the FQDN or the IP address that will be will be the outbound interface for the SIP Trunk on the Net-Net SD. In our example the IP address is **192.168.85.55**.
13. Enter the **Listening Port**. In our example the listening port is **5060**.
14. Select the **"Sip Transport Protocol**". In our example it is **TCP**. Select this radio button and click **Ok**.

The PSTN Gateway for Lync Server, which is the outbound side of the Net-Net SD has now been added.



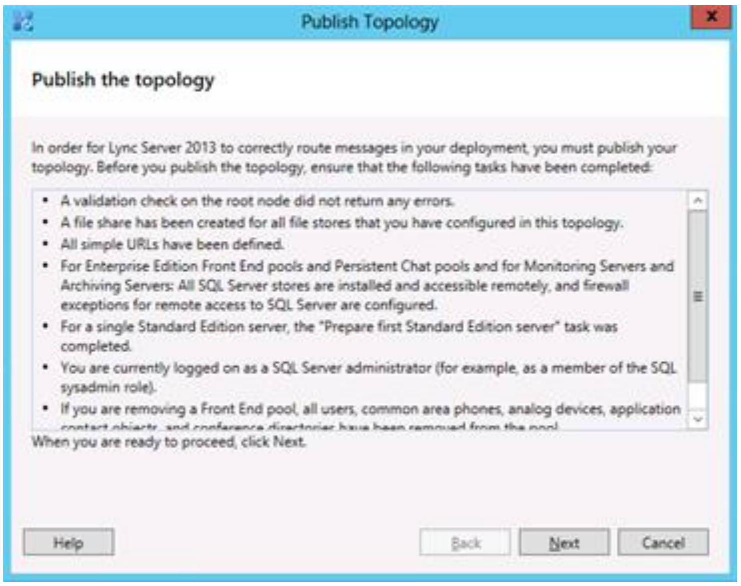
Next we will add the newly created PSTN gateway entry to the Mediation Server.

15. Expand the **Mediation Pool** list and click on the Mediation Server to be utilized. In our example the Mediation Server is **lync2013.med1.acmepackt.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

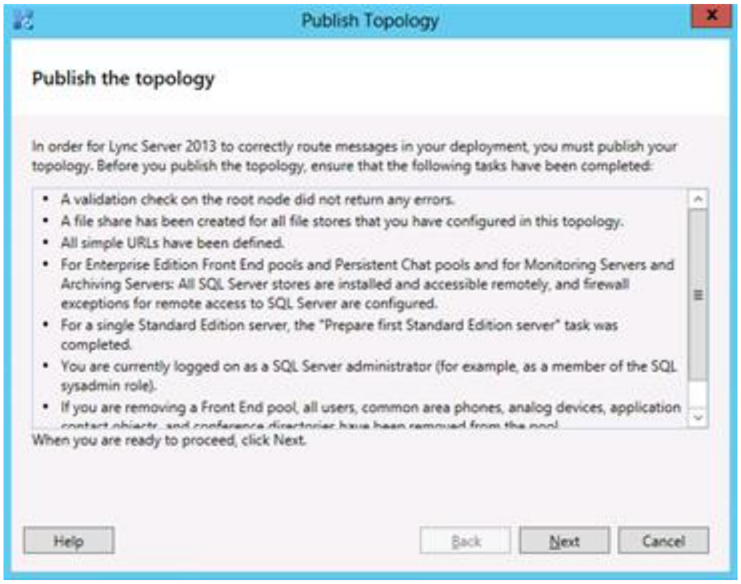
16. In the upper right hand corner of your screen under **Actions** select **Topology** then select **Publish**.
17. You will now see the **Publish Topology** window. Click on the **Next** button



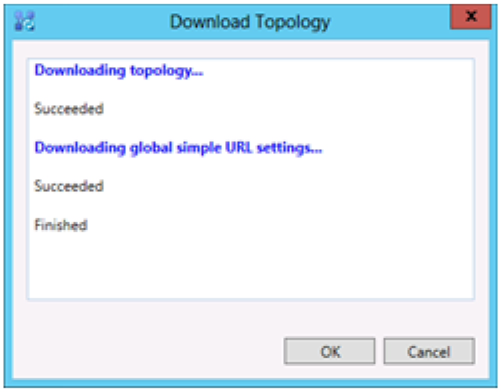
You will now be at a window showing the databases associated with site

18. Click **Next**.

When complete you should see a window from Topology Builder stating that your topology was successfully published.


Publish Topology
Publish the topology
In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:
• A validation check on the root node did not return any errors.
• A file share has been created for all file stores that you have configured in this topology.
• All simple URLs have been defined.
• For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured.
• For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
• You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
• If you are removing a Front End pool, all users, common area phones, analog devices, application
When you are ready to proceed, click Next.
Help
Back
Next
Cancel

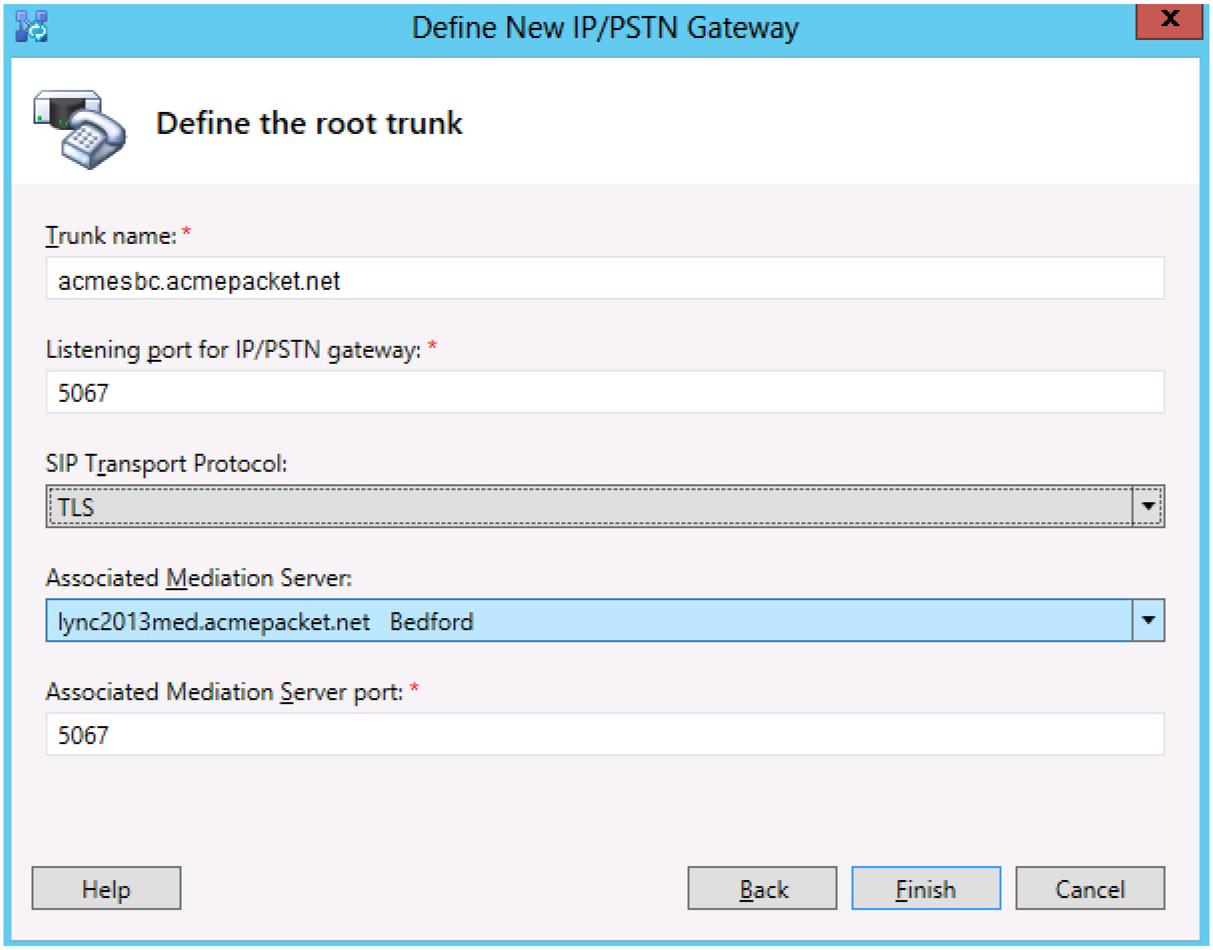
Click the **OK** button.



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.

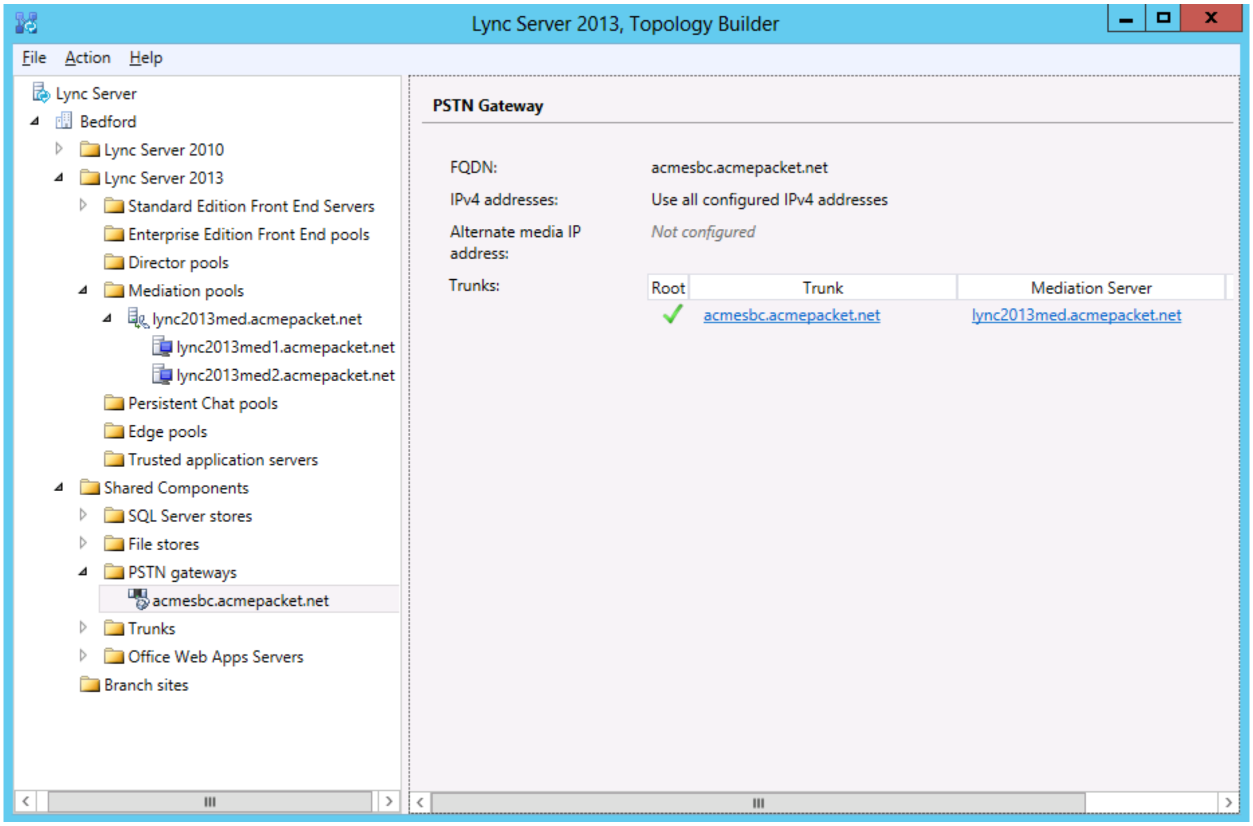
Configure TLS on Lync

1. Repeat steps from section "Adding PSTN Gateway" steps 1 thru 10. – Please NOTE: for TLS the PSTN Gateway must have a FQDN. IP Addresses are not supported.
2. Right click on **PSTN Gateways** and select **New PSTN Gateway**.



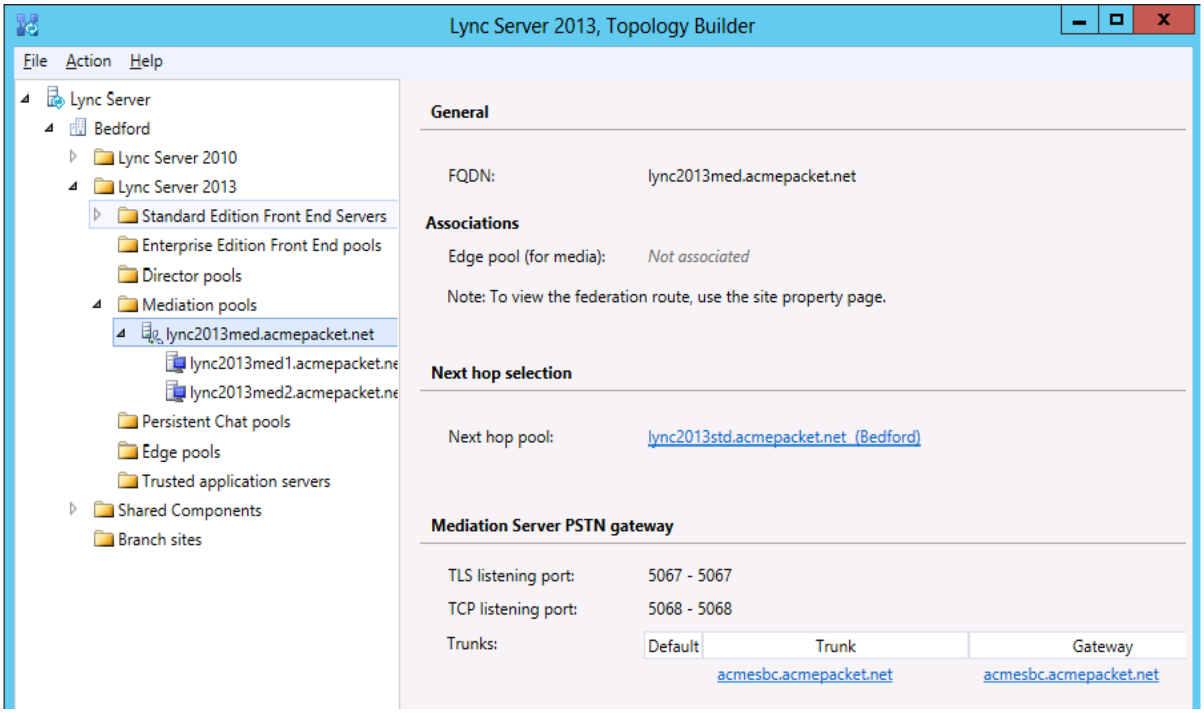
3. Enter the FQDN that will be the outbound interface for the SIP Trunk on the Net-Net ESD. In our example the FQDN is acmesbc.acmepacket.net.
4. Enter the **Listening Port**. In our example the listening port is **5067**. Mediation server as a default listens on port 5066 for TCP signaling
5. Select the **"Sip Transport Protocol**". In our example it is **TLS**. Select this radio button and click **Finish**.

The PSTN Gateway for Lync Server, which is the outbound side of the Net-Net ESD has now been added.



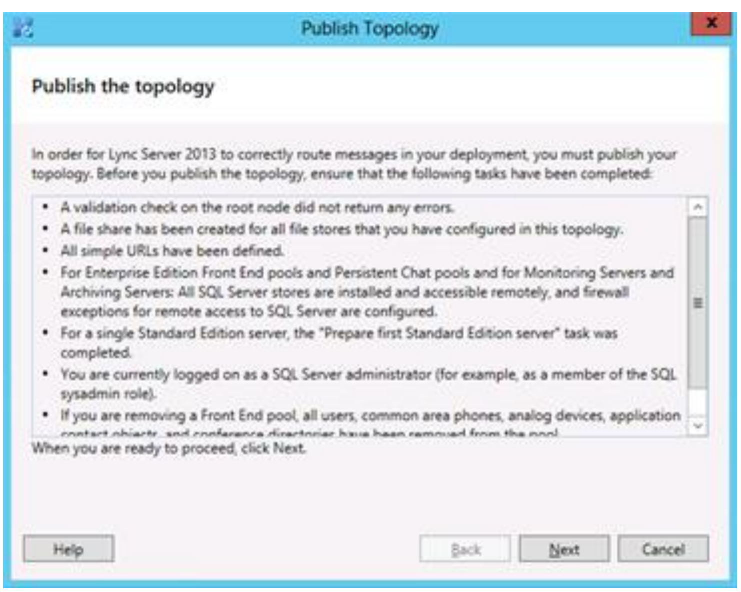
Next we will add the newly created PSTN gateway entry to the Mediation Server.

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



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

7. In the upper right hand corner of your screen under **Actions** select **Topology** then select **Publish**.
8. 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

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.

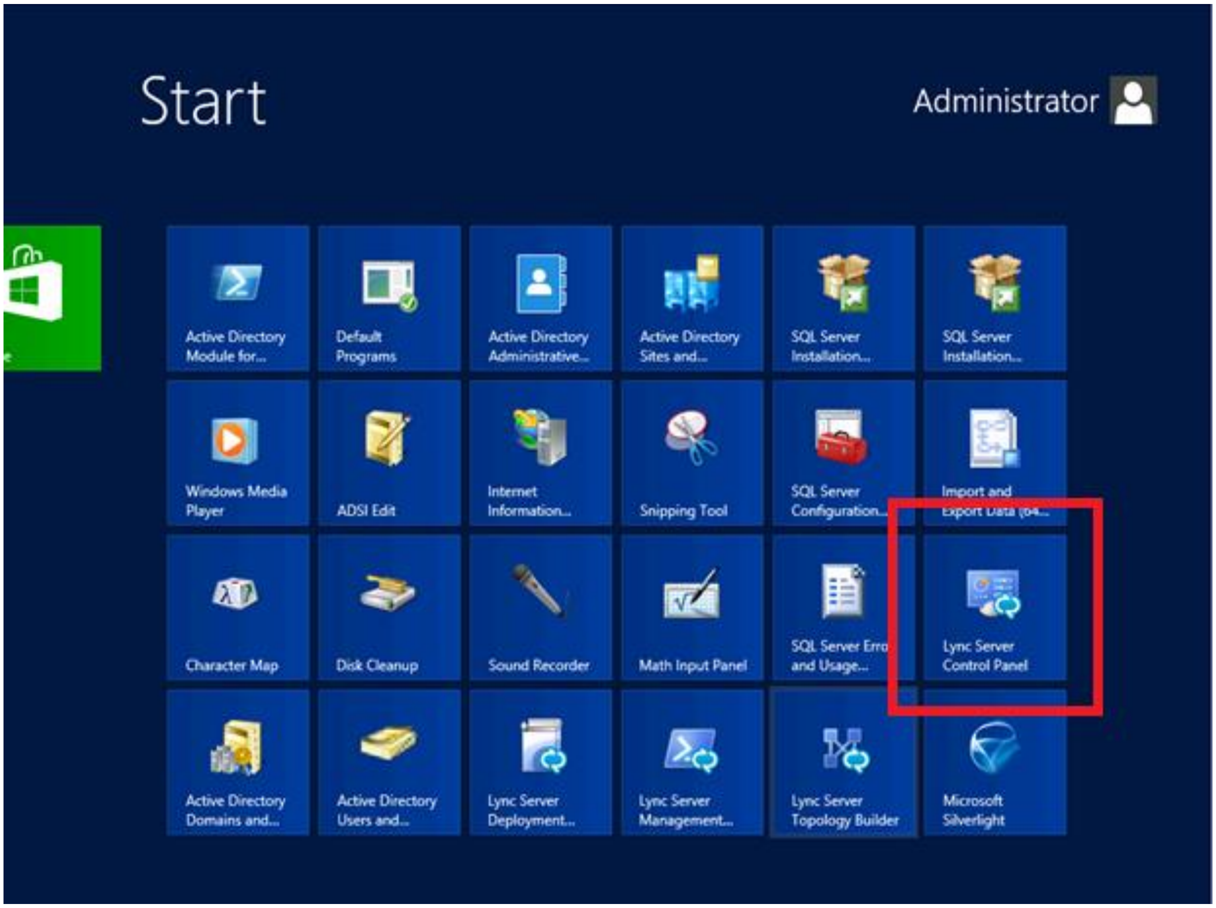
What you will need:

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

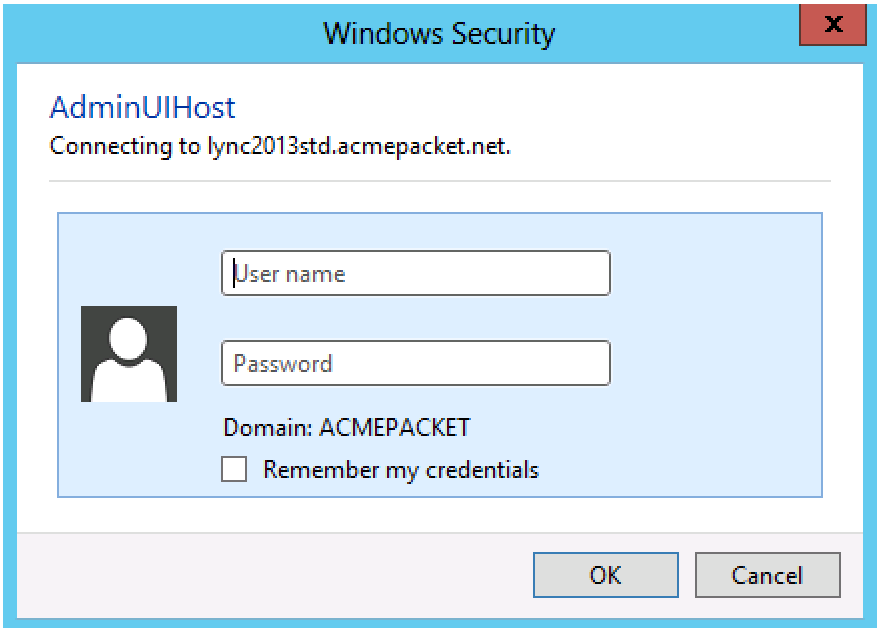
Steps to add the Lync Server Route

On the server where the CSCP is located start the console.

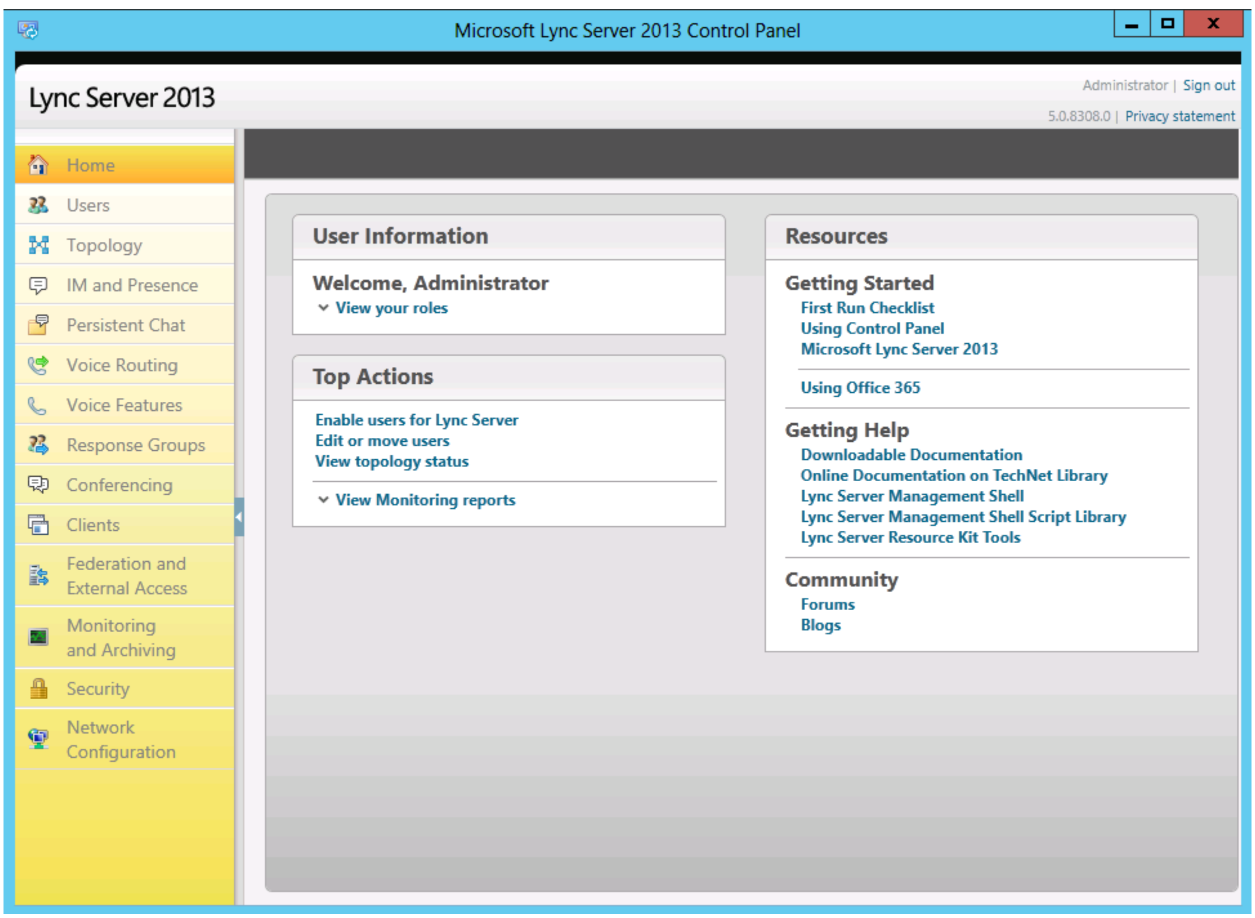
1. Click **Start**, select **All Programs**, then select **Communications Server Control Panel**



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



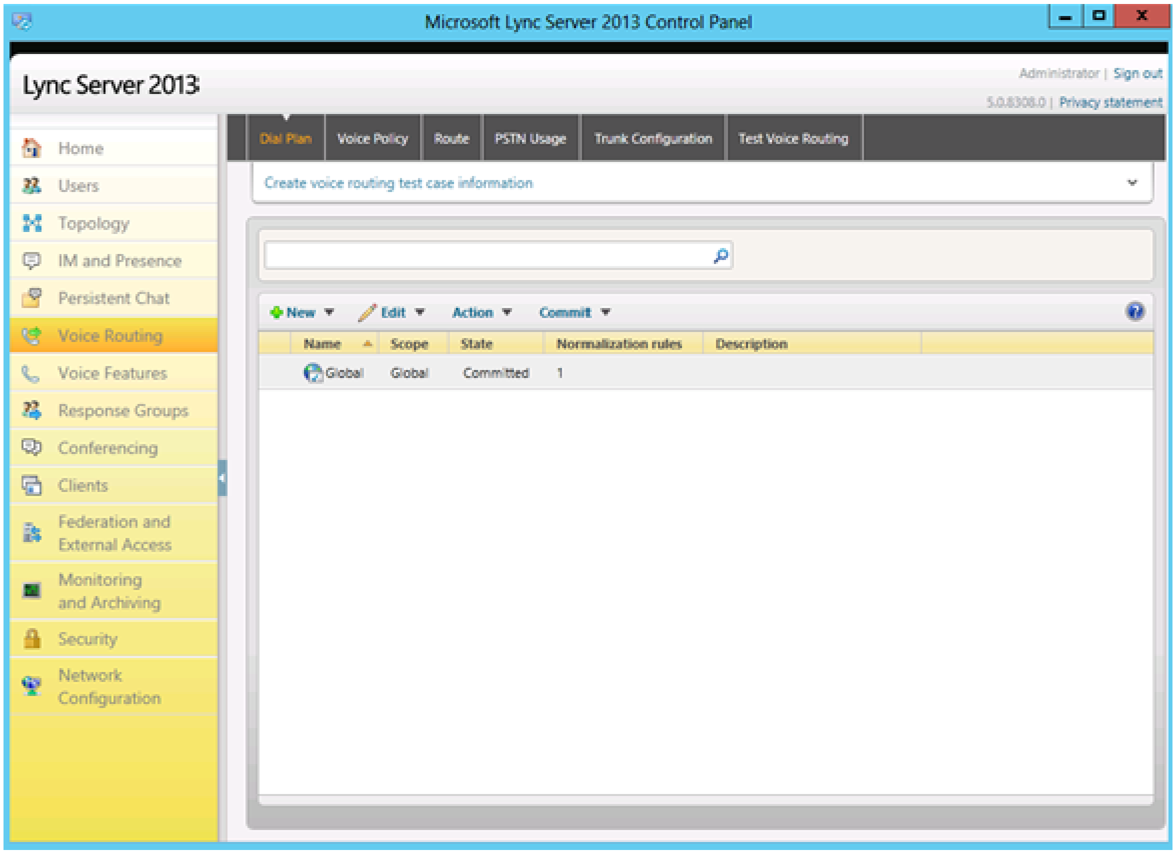
2. Once logged on, you will now be at the CSCP “Welcome Screen”.



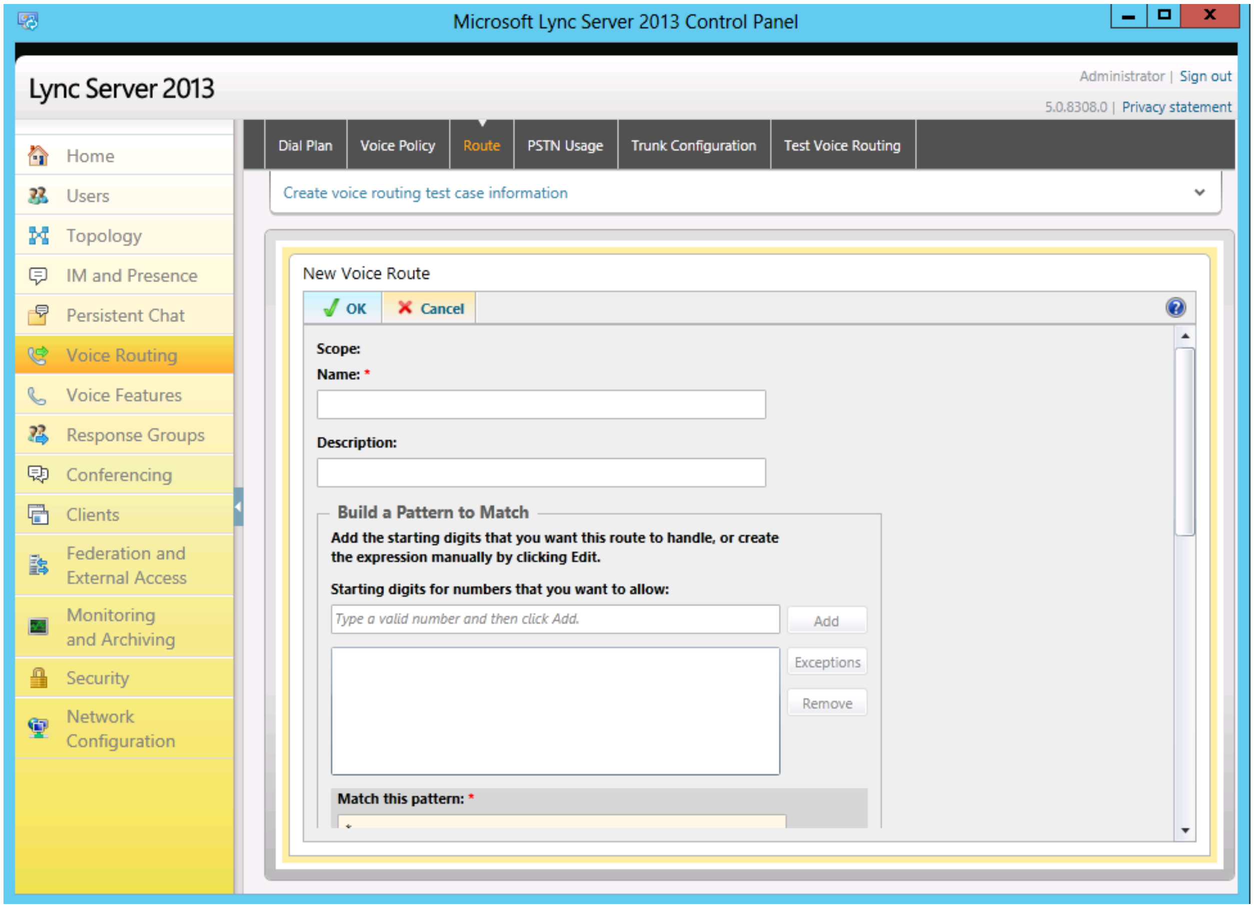
3. On the left hand side of the window click on **Voice Routing**.

You will now be in the Voice Routing section of the CSCP.

4. On the top row of tabs select **Route**.

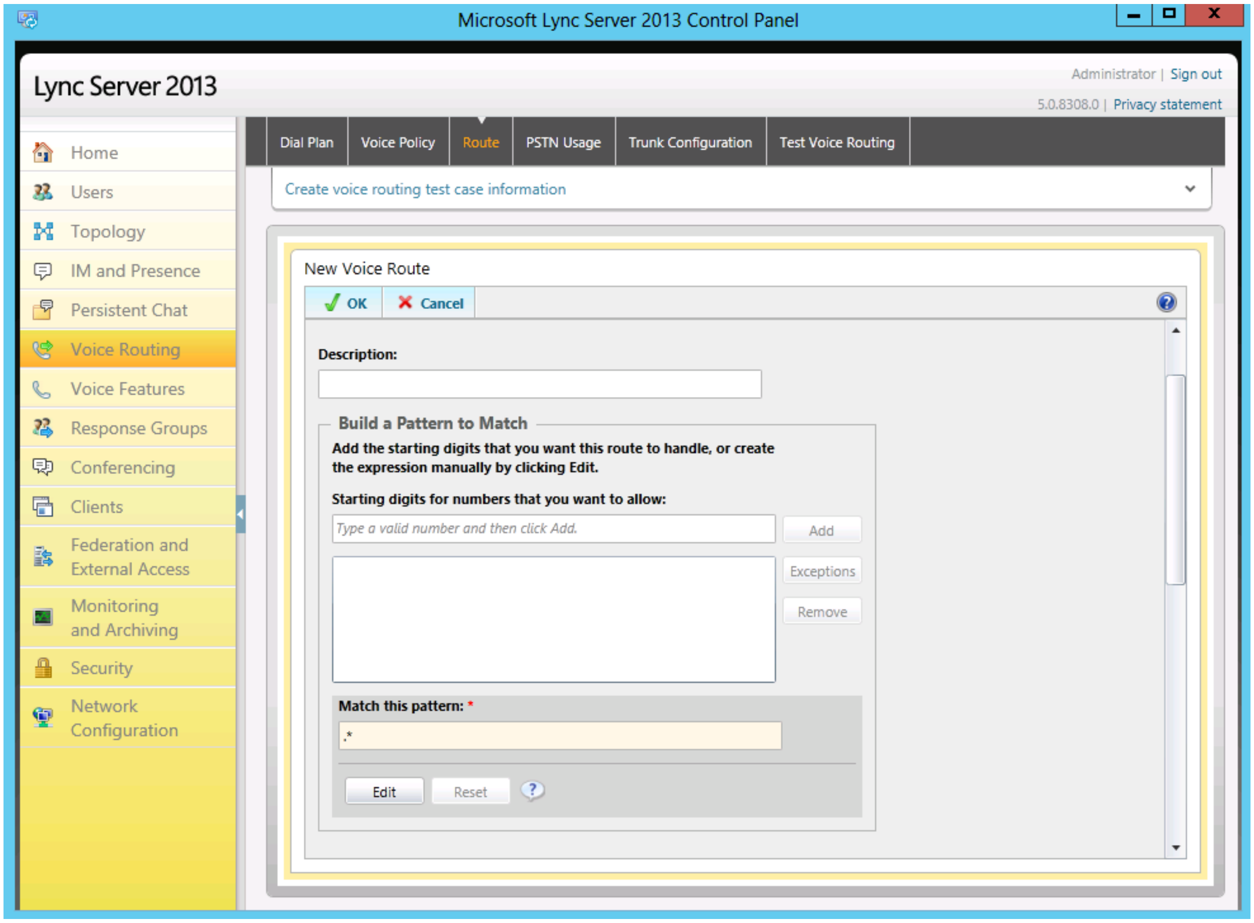


5. On the content area toolbar, click **+New**.

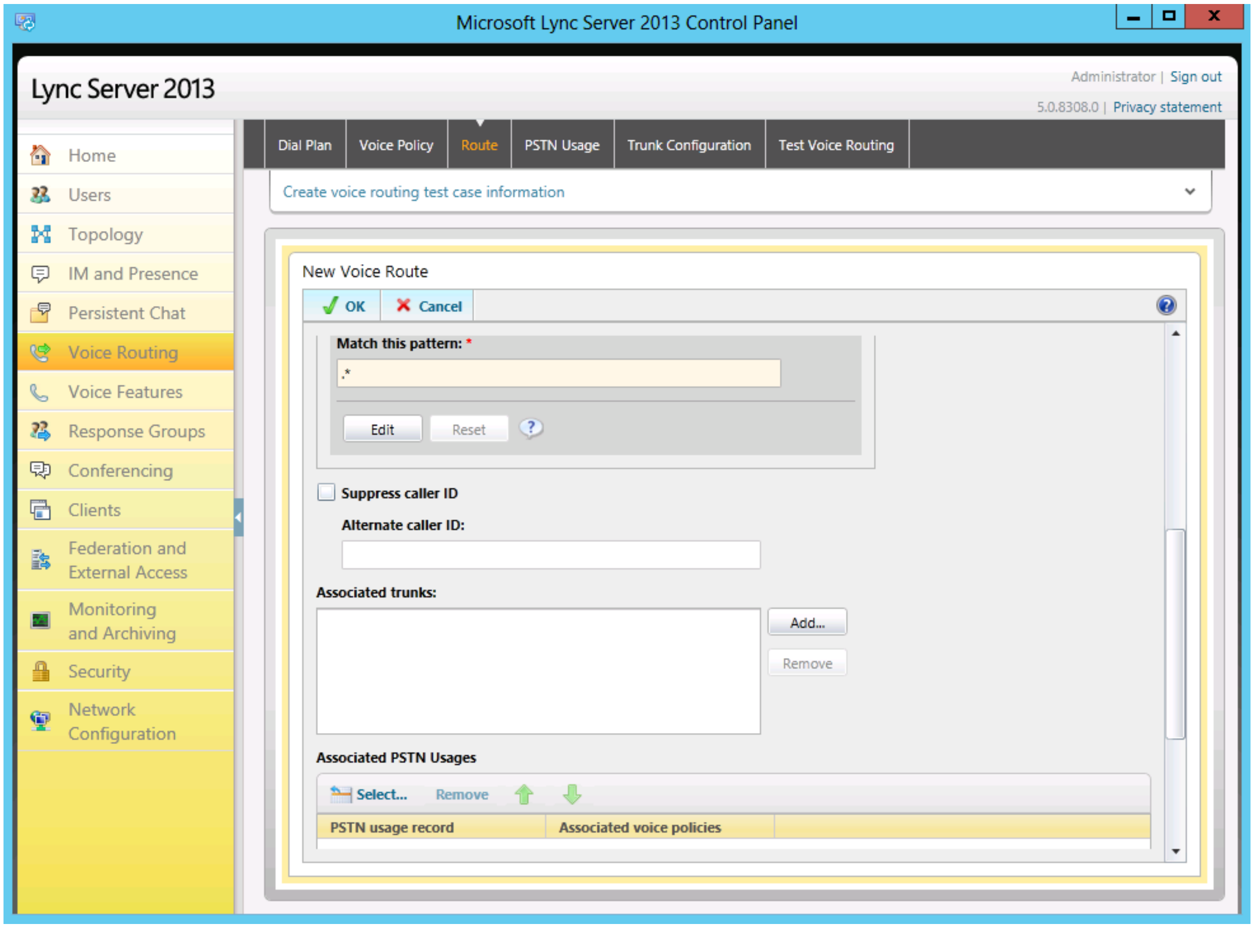


6. On the Create Voice Route page, in the Name field, enter the name you have selected for the Route. In our example, it is **Test**.

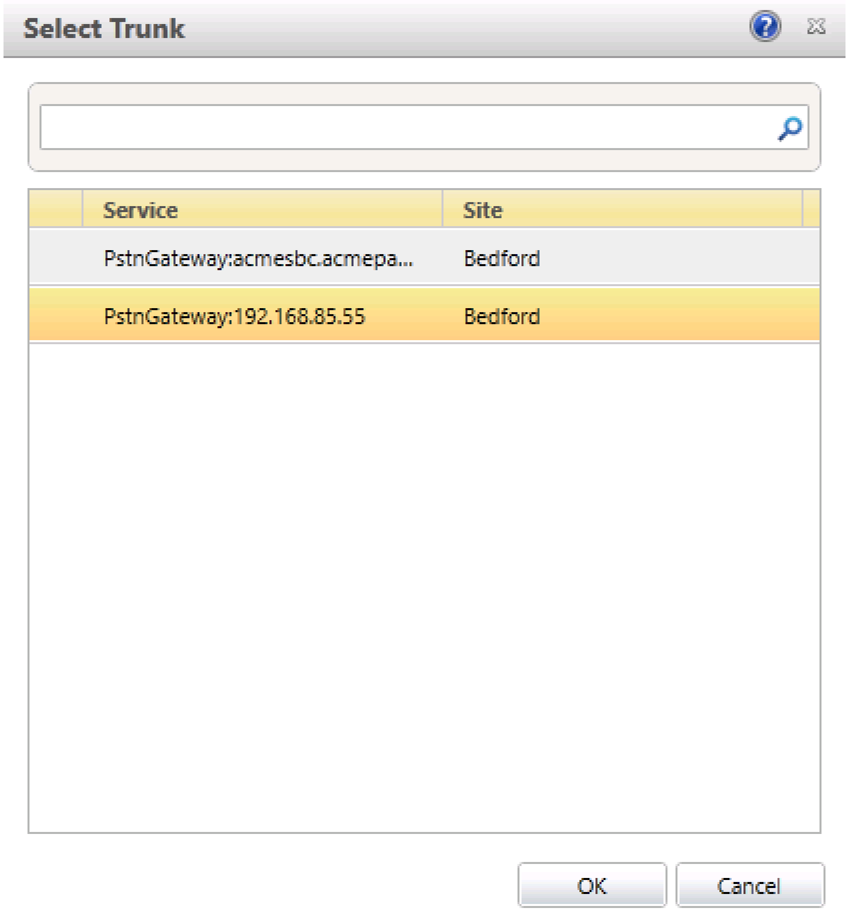
7. Next you build a Pattern Match for the phone numbers you want this route to handle. In our example we use **".*"** since we were using a very simple dial plan for this route and wish to match any outgoing call.



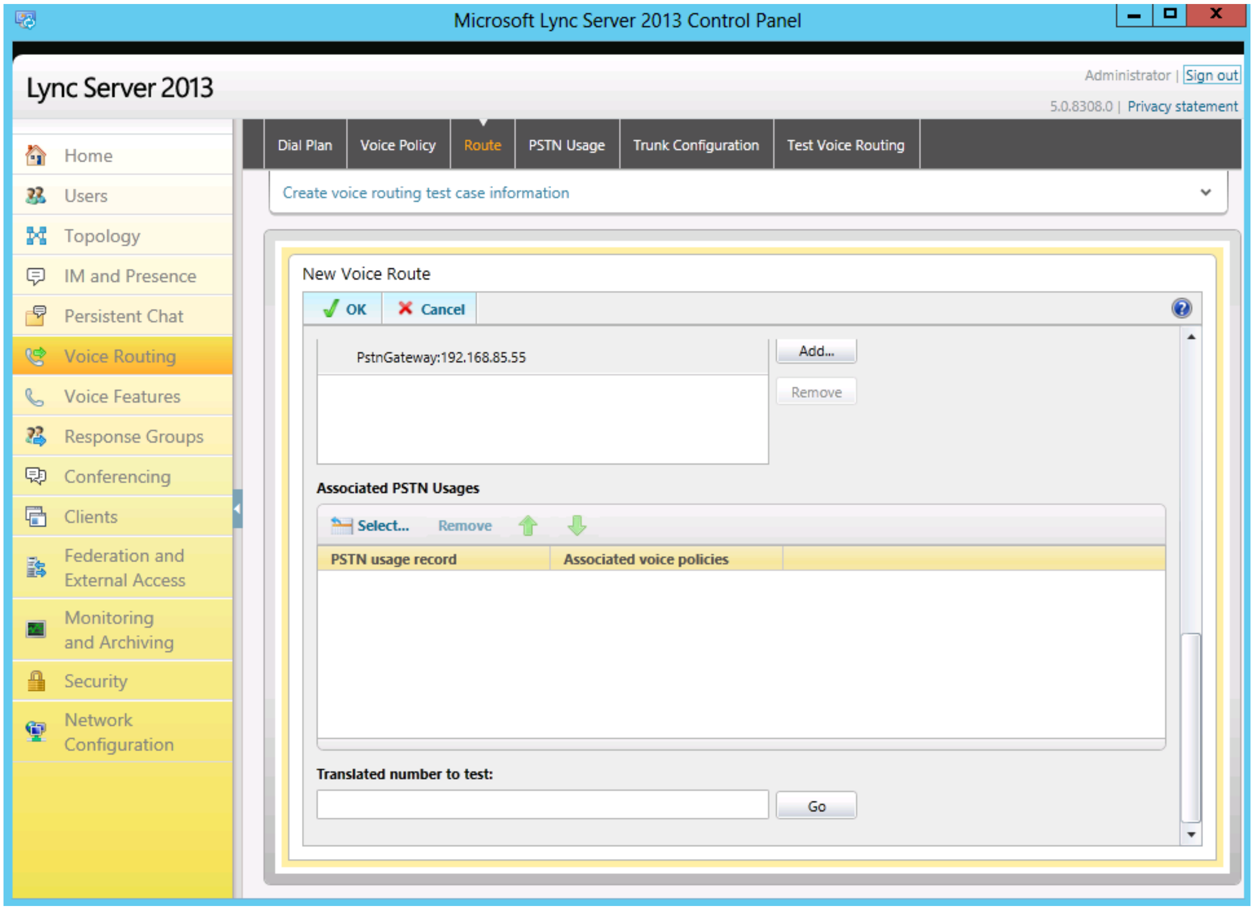
8. Next you want to associate the Voice Route with the PSTN gateway you have just created scroll down to Associated Trunks, click on the **Add** button.



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


Select Trunk
Service
Site
PstnGateway:acmesbc.acmepa...
Bedford
PstnGateway:192.168.85.55
Bedford
OK
Cancel

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

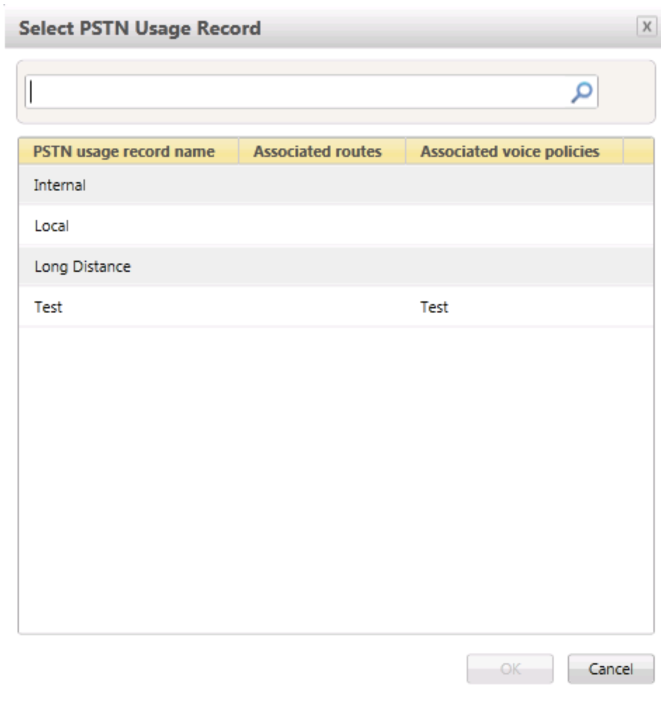


You can now see that you have associated your PSTN gateway with the route you created.

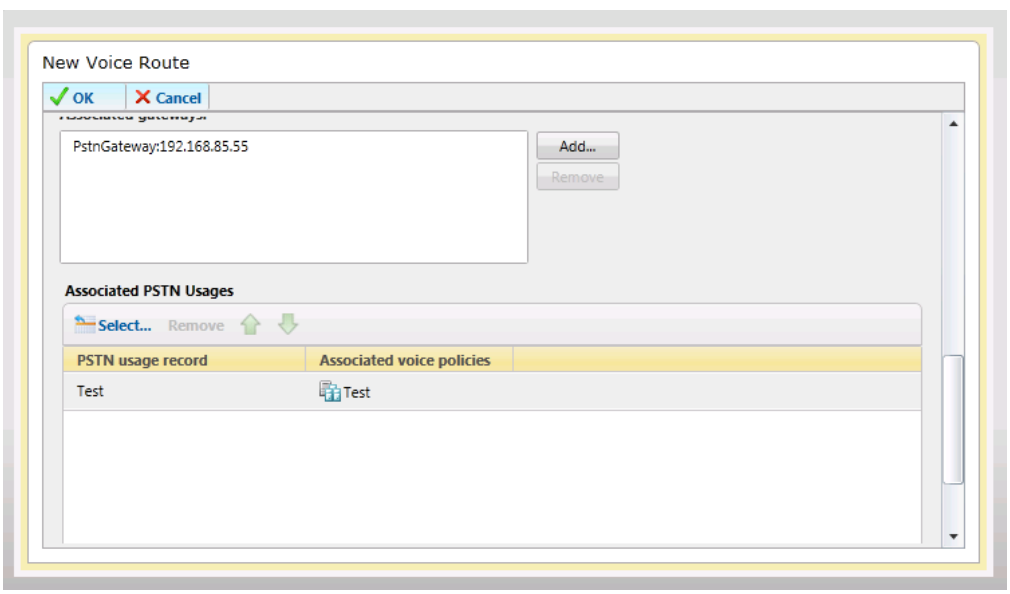
Note that the **Suppress Caller ID**: allows the manipulation of caller ID information for outbound calls, in order to mask employees' direct-dial extensions and replace them with the generic corporate or departmental numbers, this is not a necessary step for this installation, but may need to be addressed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

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

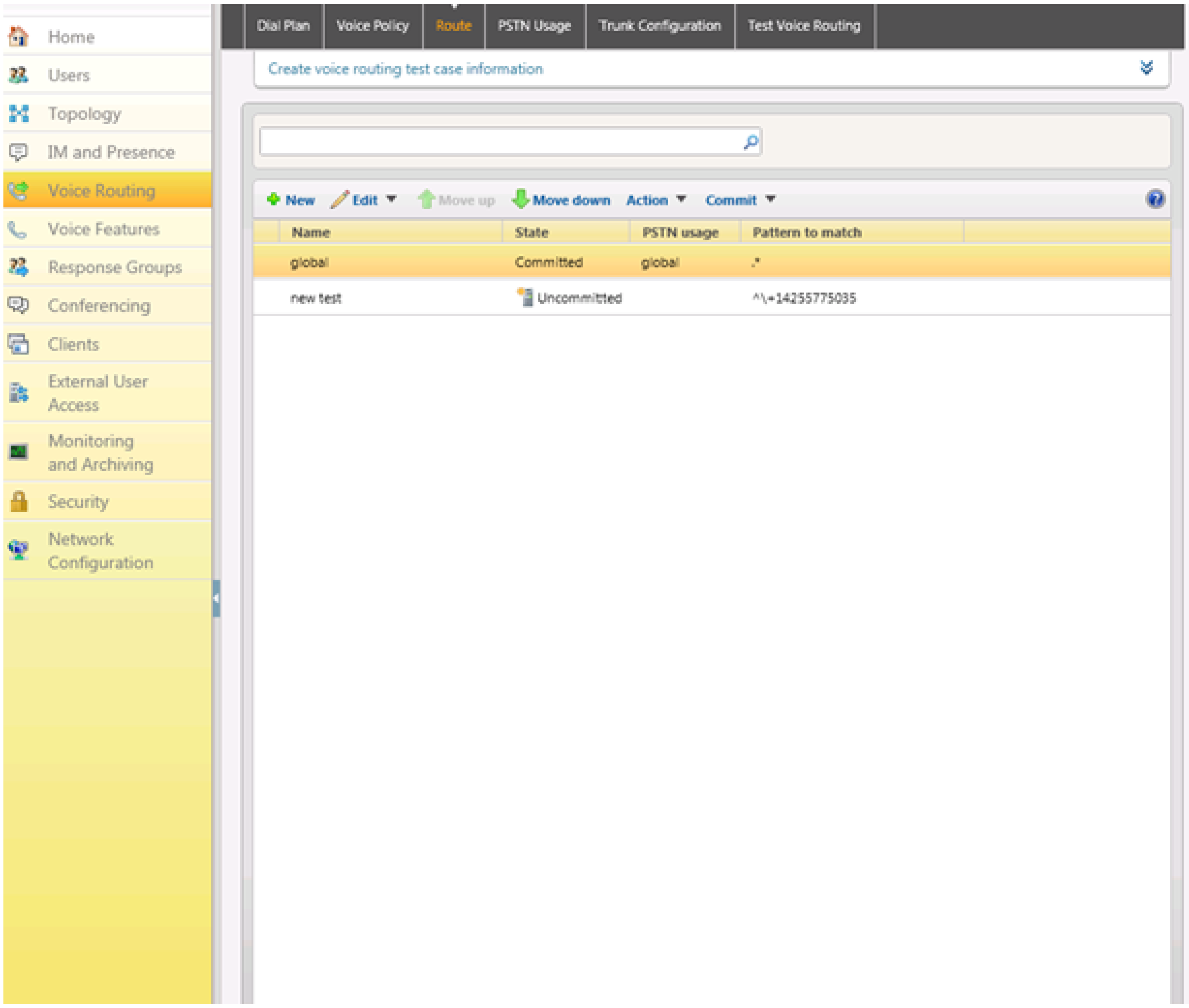


11. Select the appropriate PSTN Usage Record then click the **OK** button.

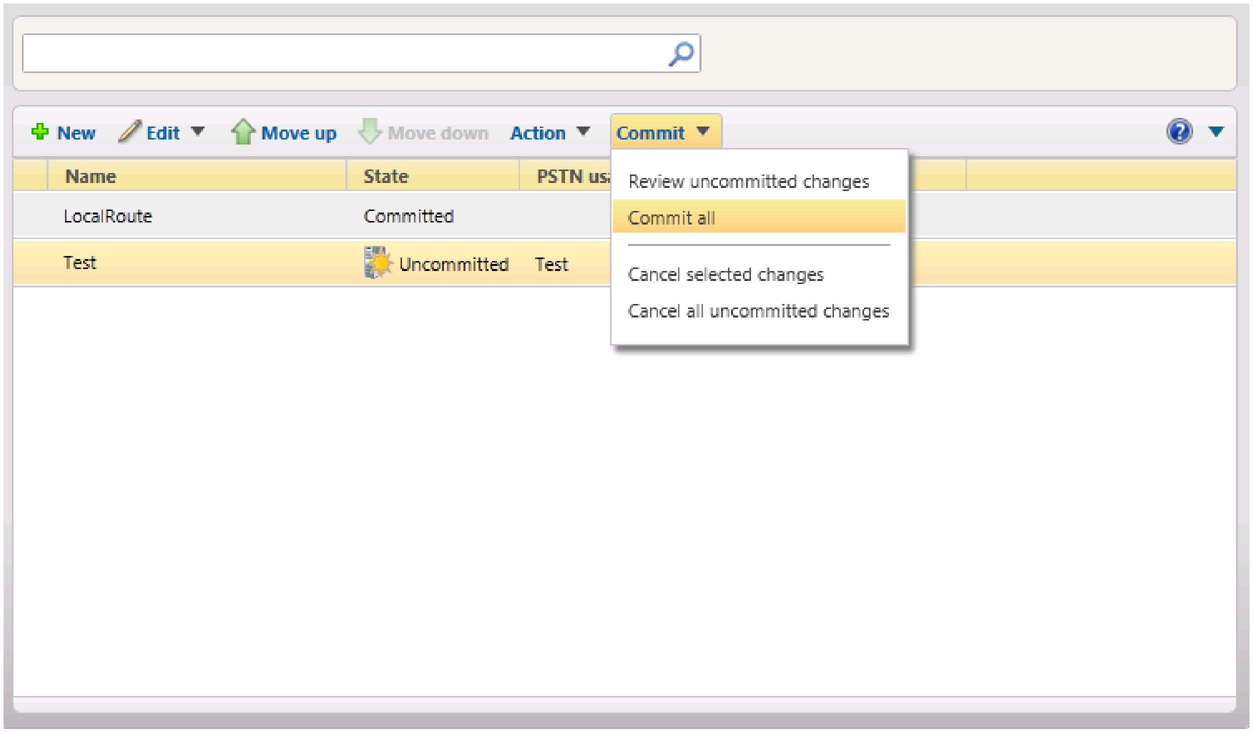


12. You will now see the Associated PSTN Gateway Usages which you have added. Click the **OK** button at the top New Voice Route screen.

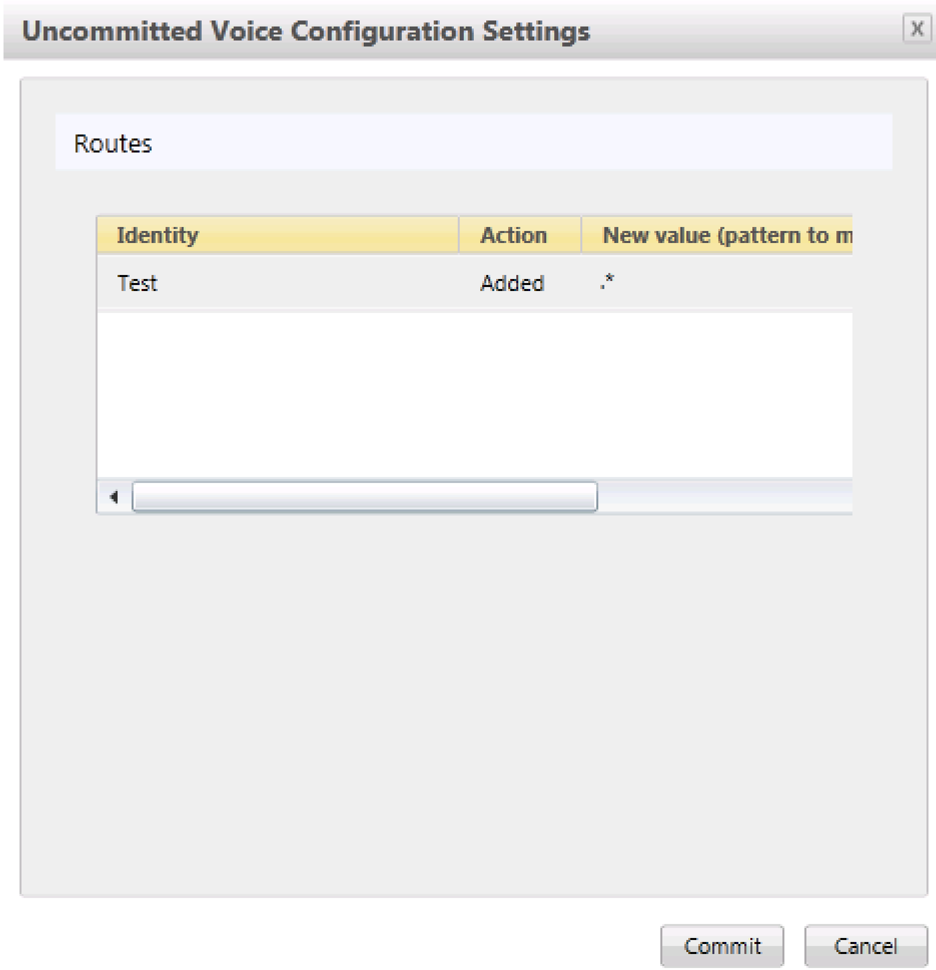
192.85



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



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



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

16. If there are no errors, the new Voice Route has now been successfully created and the State will show as Committed.

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.

To go through them all is out of scope for this document.

Phase II - Configure Session Director

In this section we describe the steps for configuring a Net-Net SD for use with Lync Server in a SIP trunking scenario.

In Scope

The following Step-by-Step guide configuring the Net-Net ESD assumes that this is a newly deployed device dedicated to a single customer.

Note that Acme Packet offers several products and solutions that can interface with Lync Server. This document covers the setup for the Net-Net SD platforms software S-Cx 6.2.0m6p1 or later. A Net-Net 3800-series (NN3820) platform was used as the platform for developing this guide. If instructions are needed for other Acme Packet products, please contact your Acme Packet representative.

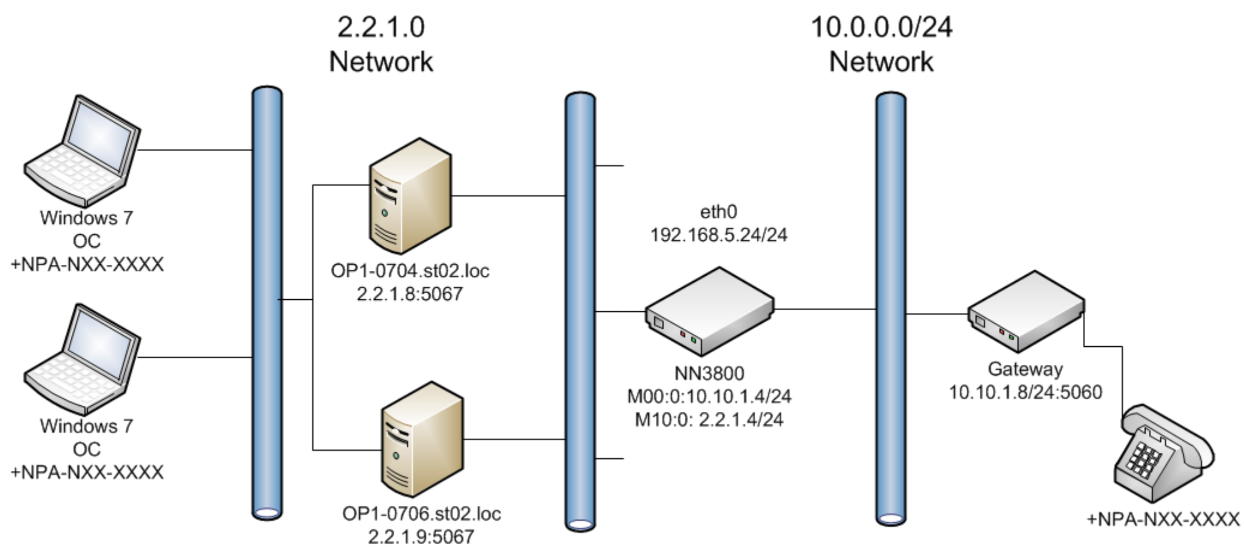
Out of Scope

- Configuration of Network management including SNMP and RADIUS; and
- Redundancy configuration

What you will need

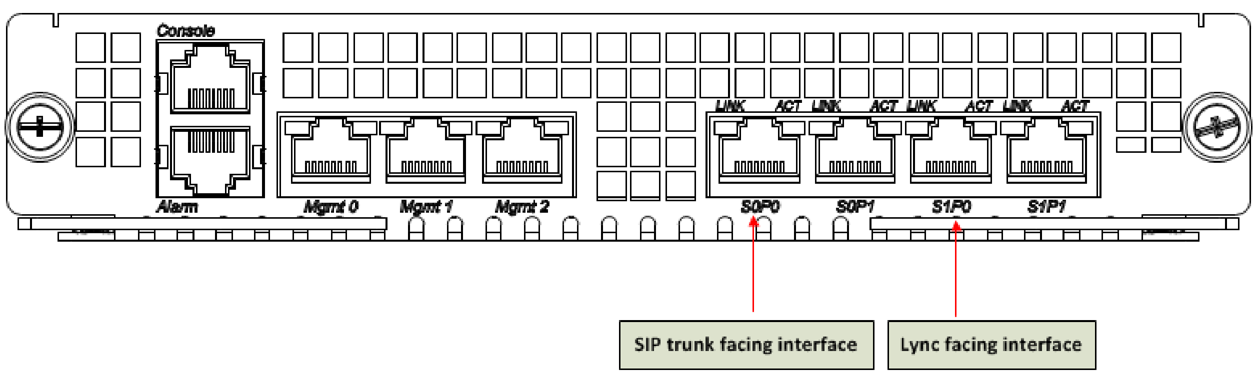
- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Net-Net SD
- Signaling IP address and port of Lync Mediation Server
- Signaling and media IP addresses and ports to be used on the Net-Net SD 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

Lync Server 2010 Acme Packet Test Topology



Configuration

Once the Net-Net SD 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, perform you are ready to power on and perform the following steps.

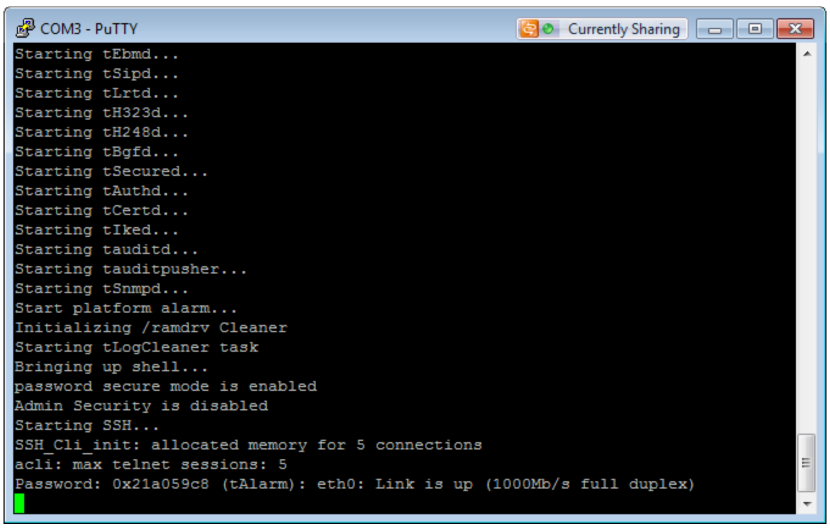
All commands are in bold, such as **configure terminal**; parameters in bold red such as **ACME1A** are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

1. **Establish the serial connection to the Net-Net SD.**

   Confirm the Net-Net SD is powered off and connect the serial console cable to the Net-Net SD 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 Net-Net SD and confirm that you see the following output from the bootup sequence.

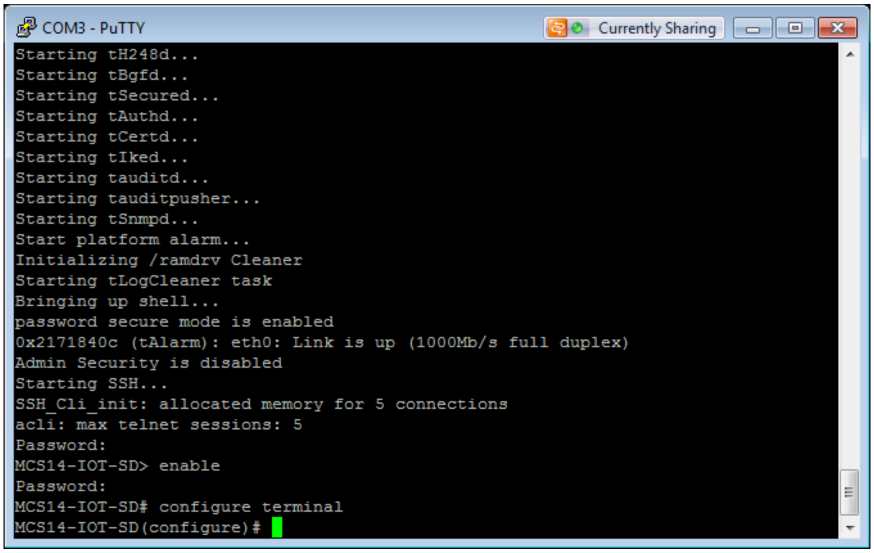


2. **Login to the Net-Net SD and enter the configuration mode**

Enter the following commands to login to the Net-Net SD and move to the configuration mode. Note that the default Net-Net SD password is “**acme**” and the default super user password is “**packet**”.

```
Password: acme
ACME1A> enable
Password: packet
ACME1A# configure terminal
ACME1A (configure)#
```

You are now in the Global Configuration mode.



3. 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.

```
ACME1A (configure)# system
ACME1A (system)# system-config
ACME1A (system-config)# hostname ACME1A
ACME1A (system-config)# description " Lync Server 2013 SIP Trunking "
ACME1A (system-config)# location "Redmond, WA"
ACME1A (system-config)# mib-system-contact "brian@cs.loc"
ACME1A (system-config)# default-gateway 10.176.32.1
ACME1A (system-config)# done
```

Once the **system-config** settings have completed and you enter **done**, the Net-Net SD 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                10.176.32.1
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
```

4. 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 on the rear of the system. This will be the interface/port that connects to your SIP trunk provider.

```
ACME1A(system-config)# exit
ACME1A(system-interface)# phy-interface
ACME1A(phy-interface)# name M00
ACME1A(phy-interface)# operation-type media
ACME1A(phy-interface)# slot 0
ACME1A(phy-interface)# port 0
ACME1A(phy-interface)# done
```

Once the **phy-interface** settings have completed for slot 0 port 0 and you enter **done**, the Net-Net ESD 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 interface/port that connects to the Lync Mediation server (lync facing) network.

```
ACME1A(phy-interface)# name M10
ACME1A(phy-interface)# operation-type media
ACME1A(phy-interface)# slot 1
ACME1A(phy-interface)# port 0
ACME1A(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
```

5. 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 enter the **network-interface** command.

You will first configure the IP characteristics for the M10 interface defined above. A hostname for the network-interface is defined which represents the FQDN of the PSTN gateway in Lync topology and this FQDN will be configured as common-name in the Certificate-record when configuring TLS on the E-SBC

```
ACME1A(phy-interface)# exit
ACME1A(system)# network-interface
ACME1A(network-interface)# name M10
ACME1A(network-interface)# description "Mediation Server-facing interface"
ACME1A(network-interface)# hostname acme1.st02.loc
ACME1A(network-interface)# ip-address 2.2.1.4
ACME1A(network-interface)# netmask 255.255.255.0
ACME1A(network-interface)# gateway 2.2.1.1
ACME1A(network-interface)# dns-ip-primary 2.2.1.5
ACME1A(network-interface)# dns-domain st02.loc
ACME1A(network-interface)#add-hip-ip 2.2.1.4
ACME1A(network-interface)#add-icmp-ip 2.2.1.4
ACME1A(network-interface)# done
```

```
network-interface
name                          M10
sub-port-id                   0
description                   Mediation Server-facing interface
hostname                      acme1.st02.loc
ip-address                    2.2.1.4
pri-utility-addr
sec-utility-addr
netmask                       255.255.255.0
gateway                       2.2.1.1
sec-gateway
gw-heartbeat
state                         disabled
heartbeat                     0
retry-count                   0
retry-timeout                 1
health-score                  0
dns-ip-primary                2.2.1.5
dns-ip-backup1
dns-ip-backup2
dns-domain                    st02.loc
dns-timeout                   11
hip-ip-list                   2.2.1.4
ftp-address
```

```
icmp-address                   2.2.1.4
snmp-address
telnet-address
ssh-address
```

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

```
ACME1A(network-interface)# name M00
ACME1A(network-interface)# description "SIP trunk facing interface"
ACME1A(network-interface)# ip-address 10.10.1.4
ACME1A(network-interface)# netmask 255.255.255.0
ACME1A(network-interface)# gateway 10.10.1.1
ACME1A(network-interface)# add-hip-ip 10.10.1.4
ACME1A(network-interface)# add-icmp-ip 10.10.1.4
ACME1A(network-interface)# done
```

```
network-interface
name                           M00
sub-port-id                    0
description                    SIP Trunk facing interface
hostname
ip-address                     10.10.1.4
pri-utility-addr
sec-utility-addr
netmask                        255.255.255.0
gateway                        10.10.1.10
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                    10.10.1.4
ftp-address
icmp-address                   10.10.1.4
snmp-address
telnet-address
ssh-address
```

6. 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.

```
ACME1A(network-interface)# exit
ACME1A(system)# exit
ACME1A(configure)# session-router
ACME1A(session-router)# sip-config
ACME1A(sip-config)# operation-mode dialog
ACME1A(sip-config)# home-realm-id core
ACME1A(sip-config)# extra-method-stats enabled
ACME1A(sip-config)# done
```

```
sip-config
state                          enabled
operation-mode                 dialog
dialog-transparency            enabled
home-realm-id                  core
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
add-reason-header              disabled
sip-message-len                4096
enum-sag-match                 disabled
extra-method-stats             enabled
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
```

7. 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 Net-Net ESD with the default values.

```
ACME1A(sip-config)# exit
ACME1A(session-router)# exit
ACME1A(configure)# media-manager
ACME1A(media-manager)# media-manager
ACME1A(media-manager-config)# select
ACME1A(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
```

8. 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 core, which represents the mediation server-facing network; and
- The pstn, which represents the SIP trunk facing network.

```
ACME1A(media-manager-config)# exit
ACME1A(media-manager)# realm-config
ACME1A(realm-config)# identifier core
ACME1A(realm-config)# description "Mediation Server facing"
ACME1A(realm-config)# network-interfaces s0p0:0
ACME1A(realm-config)# done
```

```
realm-config
identifier                      core
description                     Mediation Server-facing
addr-prefix                     0.0.0.0
network-interfaces
                                M10:0
mm-in-realm                     disabled
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
ext-policy-svr
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
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             2010-07-15 17:01:33
```

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

```
ACME1A(realm-config)# identifier pstn
ACME1A(realm-config)# description "To Sip Trunk"
ACME1A(realm-config)# network-interfaces M00:0
ACME1A(realm-config)# done
```

```
realm-config
identifier                      pstn
description                     To SIP Trunk
addr-prefix                     0.0.0.0
network-interfaces
                                M00:0
mm-in-realm                     disabled
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
ext-policy-svr
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
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             2010-07-15 17:02:11
```

9. 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 Net-Net SD will listen for and transmit SIP messages. These will be the same IP addresses as configured on the associated network-interface elements.

```
ACME1A(realm-config)# exit
ACME1A(media-manager)# exit
ACME1A(configure)# session-router
ACME1A(session-router)# sip-interface
ACME1A(sip-interface)# realm pstn
ACME1A(sip-interface)# description "SIP Trunk facing"
ACME1A(sip-interface)# sip-ports
ACME1A(sip-port)# address 10.10.1.4
ACME1A(sip-port)# transport-protocol TCP
ACME1A(sip-port)# allow-anonymous agents-only
ACME1A(sip-port)# done
```

```
sip-port
address                        10.10.1.4
port                           5060
transport-protocol             TCP
tls-profile
allow-anonymous                agents-only
ims-aka-profile
```

To ensure that the SBC is doing topology hiding and replacing host-portions in SIP URIs of From and To headers, in-built sip manipulation ACME_NAT_TO_FROM_IP will need to be configured as the out-manipulationid on this sip-interface

```
ACME1A(sip-port)# exit
ACME1A(sip-interface)# out-manipulationid ACME_NAT_TO_FROM_IP
ACME1A(sip-interface)# done
```

```
sip-interface
state                          enabled
realm-id                       pstn
description                    SIP Trunk-facing interface
sip-port
address                        10.10.1.4
port                           5060
transport-protocol             TCP
tls-profile
allow-anonymous                agents-only
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                ACME_NAT_TO_FROM_IP
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
last-modified-by                  admin@console
```

```
last-modified-date             2010-07-15 17:05:47
```

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

```
ACME1A(sip-interface)# realm-id peer
ACME1A(sip-interface)# description "Mediation Server Facing interface"
ACME1A(sip-interface)# sip-ports
ACME1A(sip-port)# address 2.2.1.4
ACME1A(sip-port)# transport-protocol TCP
ACME1A(sip-port)# allow-anonymous agents-only
ACME1A(sip-port)# done
```

```
sip-port
address                        2.2.1.4
port                           5060
transport-protocol             TCP
tls-profile
allow-anonymous                agents-only
ims-aka-profile
```

```
ACME1A(sip-port)# exit
ACME1A(sip-interface)# out-manipulationid ACME_NAT_TO_FROM_IP
ACME1AACME1A(sip-interface)# done
```

```
sip-interface
state                          enabled
realm-id                       peer
description                    Mediation Server-facing interface
sip-port
address                        2.2.1.4
port                           5060
transport-protocol             TCP
tls-profile
allow-anonymous                agents-only
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              ACME_NAT_TO_FROM_IP
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
```

10. Configure next-hop signaling elements

To configure the next-hop signaling elements (i.e., the mediation server and service provider next-hop network element) you define session-agents. Use the **session-agent** command under the session-router branch. To enter the session-router 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 Net-Net SD 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 on SW version SCX6.2 by the Acme Packet SBC via DNS A or DNS 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 service provider next-hop gateway/network element.

```
ACME1A(sip-interface)# exit
ACME1A(session-router)# session-agent
ACME1A(session-agent)# hostname 10.10.1.8
ACME1A(session-agent)# ip-address 10.10.1.8
ACME1A(session-agent)# port 5060
ACME1A(session-agent)# app-protocol sip
ACME1A(session-agent)# transport-method statictcp
ACME1A(session-agent)# realm-id pstn
ACME1A(session-agent)# done
```

```
session-agent
hostname                        10.10.1.8
ip-address
port                            5060
state                           enabled
app-protocol                    SIP
app-type
transport-method                StaticTCP
realm-id                        pstn
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
ping-interval
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
last-modified-by             admin@console
last-modified-date           2010-07-15 17:09:46
```

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

```
acme1a(session-group)# group-name Mediation
acme1a(session-group)# strategy RoundRobin
acme1a(session-group)# dest OP1-0704.st02.loc
acme1a(session-group)# dest + OP1-0706.st02.loc
acme1a(session-group)# sag-recursion enabled
acme1a(session-group) # done
```

Defining Mediation Server 1

```
acme1a(session-agent)# hostname OP1-0704.st02.loc
acme1a(session-agent)# ip-address 2.2.1.8
acme1a(session-agent)# port 5066
acme1a(session-agent)# app-protocol sip
acme1a(session-agent)# transport-method staticTCP
acme1a(session-agent)# realm core
acme1a(session-agent)# ping-method OPTIONS
acme1a(session-agent)# ping-interval 60
acme1a(session-agent)# refer-call-transfer enabled
acme1a(session-agent)# done
```

```
session-agent
      hostname                     OP1-0704.st02.loc
      ip-address                   2.2.1.8
      port                         5066
      state                        enabled
      app-protocol                 SIP
      app-type
      transport-method             StaticTCP
      realm-id                     core
      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;next-hop=0
ping-interval                  60
ping-send-mode                 keep-alive
ping-all-addresses             enabled
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
```

Defining Mediation Server 2

```
acme1a(session-agent)# hostname OP1-0706.st02.loc
acme1a(session-agent)# ip-address 2.2.1.9
acme1a(session-agent)# port 5066
acme1a(session-agent)# app-protocol sip
acme1a(session-agent)# transport-method staticTCP
acme1a(session-agent)# realm core
acme1a(session-agent)# ping-method OPTIONS
acme1a(session-agent)# ping-interval 60
acme1a(session-agent)# refer-call-transfer enabled
acme1a(session-agent)# done
```

```
session-agent
      hostname                       OP1-0706.st02.loc
      ip-address                     2.2.1.9
      port                           5066
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               StaticTCP
      realm-id                       core
      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;next-hop=0
ping-interval                   60
ping-send-mode                  keep-alive
ping-all-addresses              enabled
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
```

11. 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.

```
ACME1A(session-agent)# exit
ACME1A(session-router)# local-policy
ACME1A(local-policy)# from-address *
ACME1A(local-policy)# to-address *
ACME1A(local-policy)# source-realm pstn
ACME1A(local-policy)# policy-attributes
ACME1A(local-policy-attributes)# next-hop SAG:Mediaton
ACME1A(local-policy-attributes)# action replace-uri
ACME1A(local-policy-attributes)# app-protocol sip
ACME1A(local-policy-attributes)# done
```

```
policy-attribute
next-hop                       SAG:Mediation
            realm
            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
```

```
ACME1A(local-policy-attributes)# exit
ACME1A(local-policy)# done
```

```
local-policy
from-address
                               *
to-address
                               *
source-realm
                               pstn
description
```

```
activate-time                  N/A
deactivate-time                N/A
state                          enabled
policy-priority                none
next-hop                       SAG:Mediation
            realm
            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
```

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

```
ACME1A(local-policy)# from-address *
ACME1A(local-policy)# to-address *
ACME1A(local-policy)# source-realm core
ACME1A(local-policy)# policy-attributes
ACME1A(local-policy-attributes)# next-hop 10.10.1.8
ACME1A(local-policy-attributes)# realm pstn
ACME1A(local-policy-attributes)# app-protocol sip
ACME1A(local-policy-attributes)# done
```

```
policy-attribute
next-hop                       10.10.1.8
realm                          pstn
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
```

```
ACME1A(local-policy-attributes)# exit
ACME1A(local-policy)# done
```

```
local-policy
      from-address                    *
      to-address                      *

      source-realm
                                      core
      description
      activate-time                   N/A
      deactivate-time                 N/A
      state                           enabled
      policy-priority                 none
            policy-attribute
            next-hop                        10.10.1.8
            realm                           pstn
            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
```

11 a. Call Transfer Scnearios

Lync Server 2013 authorizes transfers of all Lync initiated calls whether it is Lync to Lync or Lync to PSTN. Acme Packet Net-Net SBC provides REFER handling by terminating the REFER from Lync and generating an INVITE for the referred party towards Lync Mediation server. Lync then process the INVITE, authorizes the call transfer and sends either a new INVITE (for call transferred to PSTN) to the SBC or transfers call internally to transferred Lync client

To handle 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

```
ACME1A(local-policy)# from-address *
ACME1A(local-policy)# to-address OP1-0704.st02.loc
ACME1A(local-policy)# source-realm pstn
ACME1A(local-policy)# description "for referred party OP1-
0704.st02.loc"
ACME1A(local-policy)# policy-attributes
ACME1A(local-policy-attributes)# next-hop OP1-0704.st02.loc
ACME1A(local-policy-attributes)# realm core
ACME1A(local-policy-attributes)# action replace-uri
ACME1A(local-policy-attributes)# done
ACME1A(local-policy-attributes)# exit
ACME1A(local-policy)# done
ACME1A(local-policy)# from-address *
ACME1A(local-policy)# to-address OP1-0706.st02.loc
ACME1A(local-policy)# source-realm pstn
ACME1A(local-policy)# description "for referred party OP1-
0706.st02.loc"
ACME1A(local-policy)# policy-attributes
ACME1A(local-policy-attributes)# next-hop OP1-0706.st02.loc
ACME1A(local-policy-attributes)# realm core
ACME1A(local-policy-attributes)# action replace-uri
ACME1A(local-policy-attributes)# done
ACME1A(local-policy-attributes)# exit
ACME1A(local-policy)# done
```

```
local-policy
      from-address                    *
      to-address                     OP1-0704.st02.loc
      source-realm                   pstn
      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                        OP1-0704.st02.loc
            realm                           core
            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
                                       OP1-0706.st02.loc
      source-realm
                                       pstn
      description                      for referred party OP1-
0706.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                         OP1-0706.st02.loc
            realm                            core
            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
```

12. 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).

```
ACME1A(local-policy)# exit
ACME1A(session-router)# exit
ACME1A(configure)# media-manager
ACME1A(media-manager)# steering-pool
ACME1A(steering-pool)# ip-address 10.10.1.8
ACME1A(steering-pool)# start-port 40000
ACME1A(steering-pool)# end-port 60000
ACME1A(steering-pool)# realm-id pstn
ACME1A(steering-pool)# done
```

```
steering-pool
ip-address                          10.10.1.8
start-port                          40000
end-port                            60000
realm-id                            pstn
network-interface
```

You will now configure the media handling for the core (Lync mediation server) realm.

```
ACME1A(steering-pool)# ip-address 2.2.1.4
ACME1A(steering-pool)# start-port 40000
ACME1A(steering-pool)# end-port 60000
ACME1A(steering-pool)# realm-id core
ACME1A(steering-pool)# done
```

```
steering-pool
ip-address                          2.2.1.4
start-port                          40000
end-port                            60000
realm-id                            core
network-interface
```

13. Configuring 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 supported header The SBC can interwork and provide RFC

3262 PRACK interworking towards Lync and it is mandatory configuration in all Acme Packet – 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 sip-manipulation to add a Require:100rel header in incoming SIP INVITE from mediation server and delete the Supported:100rel header

```
ACME1A(session-router)# sip-interface
ACME1A(sip-interface)# select
<realm-id>:
1: core       2.2.1.4:5067
2: pstn       10.10.1.4:5060
selection: 1
ACME1A(sip-interface)#options 100rel-interworking
```

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

```
ACME1A(session-router)#sip-feature
ACME1A(sip-feature)#name 100rel-interworking
ACME1A(sip-feature)#realm pstn
ACME1A(sip-feature)# support-mode-inbound Pass
ACME1A(sip-feature)# require-mode-inbound Pass
ACME1A(sip-feature)# proxy-require-mode-inbound Pass
ACME1A(sip-feature)# support-mode-outbound Pass
ACME1A(sip-feature)# require-mode-outbound Pass
ACME1A(sip-feature)# proxy-require-mode-outbound Pass
ACME1A(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
```

```
ACME1A(sip-manipulation)# name Forearlymedia
ACME1A(sip-manipulation)# header-rules
ACME1A(sip-header-rules)# name delsupported
ACME1A(sip-header-rules)# header-name Supported
ACME1A(sip-header-rules)# action delete
ACME1A(sip-header-rules)# comparison-type case-sensitive
ACME1A(sip-header-rules)# msg-type request
ACME1A(sip-header-rules)# methods INVITE
ACME1A(sip-header-rules)# done
ACME1A(sip-header-rules)# name addrequireinINVITE
ACME1A(sip-header-rules)# header-name Require
ACME1A(sip-header-rules)# action add
ACME1A(sip-header-rules)# comparison-type case-sensitive
```

```
ACME1A(sip-header-rules)# msg-type request
ACME1A(sip-header-rules)# methods INVITE
ACME1A(sip-header-rules)# done
ACME1A(sip-header-rules)# exit
ACME1A(sip-manipulation)# done
```

```
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
```

Reference the sip-manipulation name/id as an in-manipulationid on the 2.2.1.4 sip-interface

```
ACME1A(session-router)# sip-interface
ACME1A(sip-interface)# select
<realm-id>:
1: core       2.2.1.4:5067
2: pstn       10.10.1.4:5060
selection: 1
ACME1A(sip-interface)#in-manipulationid Forearlymedia
ACME1A(sip-interface)#done
```

14. TLS & SRTP configuration on Net-Net SD

In some applications, it may be required for the E-SBC to establish a TLS connection and use media encryption (support SRTP) with Lync server. The Net-Net ESD can interwork and terminate SIP over TLS and SRTP between Lync and the Sip trunk provider. This portion of the guide provides instructions on how to achieve this. Note that the Net-Net ESD must have the appropriate hardware (IPSec NIUs) and at a minimum a software TLS license to support this capability. If you have any questions regarding these, please contact your Acme Packet representative.

14.1 TLS Configuration on the Net-Net SD

To configure TLS on the Net-Net Session Director, the following steps will need to be followed:

- Create certificate-record, generate certificate request and import signed certificate
- Create a TLS profile
- Apply tls-profile on the sip-interface
- Change transport-protocol on Session-agent (from TCP to TLS)

14 1.1 Create certificate-record

To configure certificate-record use the certificate-record menu under the security branch. Since Lync server requires mutual TLS authentication, both parties (SBC and mediation server) will need to provide their own certificate to the peer during the TLS handshake for the purpose of authenticating themselves to each other.

Create certificate record holder for Microsoft Certificate authority (Enterprise CA)

```
Acme1a(configure terminal)#security
Acme1a(security)#certificate-record
Acme1a(certificate-record)#name ST02-OP1-0703-CA
Acme1a(certificate-record)#country US
Acme1a(certificate-record)#state WA
Acme1a(certificate-record)locality Redmond
Acme1a(certificate-record)key-size 2048
   Acme1a(certificate-record)done
```

```
certificate-record
      name                          ST02-OP1-0703-CA
      country                       US
      state                         WA
      locality                      Redmond
      organization                  loc
      unit                          ST02
      common-name
      key-size                      2048
      alternate-name
      trusted                       enabled
      key-usage-list
                                    digitalSignature
                                    keyEncipherment
      extended-key-usage-list
                                    serverAuth
```

You will now configure an additional certificate record holder for the Net-Net Session Director (end-entity certificate). The common-name needs to be an FQDN per Lync server 2013 gateway specification and is exchanged in the CN part of the Subject field of X.509 TLS certificate that is presented by the Net-Net SBC. This FQDN is also provisioned in Lync that resolves to the Lync mediation server facing Sip-interface IP address of the SBC

```
Acme1a(certificate-record)#name acme-rcrd
Acme1a(certificate-record)#country US
Acme1a(certificate-record)# state WA
Acme1a(certificate-record)#common-name acme1.st02.loc
Acme1a(certificate-record)#key-size 2048
   Acme1a(certificate-record)#done
```

```
certificate-record
      name                             acme-rcrd
      country                          US
      state                            WA
      locality                         Redmond
      organization                     loc
      unit                             ST02
      common-name                      acmesbc.acmepacket.net
      key-size                         2048
      alternate-name
      trusted                          enabled
      key-usage-list
                                       digitalSignature
                                       keyEncipherment
      extended-key-usage-list
                                       serverAuth
```

Once the certificate records are created, you will generate a certificate request and have the CA sign the SBC certificate request

As an example a screenshot below is provided to generate a certificate request and import the signed certificate from the CA

```
comptnr-ddos# generate-certificate-request acme-rcrd
Generating Certificate Signing Request. This can take several minutes....

-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwVDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzENMAsGA1UEAxMEYWNt
ZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvJF6D8gnSvc9Ug4aCkyIqQeW
kgkyk+kNYXESQNoOHJTdre9R6IB5f1UdsM/8k1TTpyBwMn+GooeOc8iJ4wks+7VG
QegsZEawyDFoTClwQCppWsEFjOQWtnybP3ZLVBBPJ4Mcowi7qKJK/Pe4aCgfEhue
27BWc/HHD2lZIMlyhyECAwEAAaBCMBQGA1UdJTENEwtzZXJ2ZXJBdXRoIDAqBgNV
HQ8xIxMhZGlnaXRhbFNpZ25hdHVyZSBrZXlFbmNpcGhlcm1lbnQgMA0GCSqGSIb3
DQEBBQUAA4GBAKOwXNVG33sBrNcLCndMrzEA5xONY7q2f2PXhm7dfgrgS2e2XNoZ
rqeh127aBTcgCidRAEGYVL1EVFOCT1Mo9++B7dyfa3K5eG6m78GILqoonZluIqbA
Y7ZOkFnAgiyR65ZjpmjFzlhNjrNtH4qWyT49fDWC7NfKrNKd8o1Al6U9
-----END CERTIFICATE REQUEST-----

WARNING: Configuration changed, run "save-config" command.
```

Once the certificate request is generated, be sure to run the save-config and activate-config command. The certificate request can be FTP'd to the CA (the highlighted portion is saved in a text file)

FTP the signed certificate file "xyz.crt"to /ramdrv/; or copy to clipboard so that you can paste from ACLI (example shown below)

```
comptnr-ddos# import-certificate try-all acme-rcrd
IMPORTANT:
        Please enter the certificate in the PEM format.
        Terminate the certificate with ";" to exit.......
-----BEGIN CERTIFICATE-----
MIICQDCCAakCAQQwDQYJKoZIhvcNAQEFBQAwfTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMRMwEQYDVQQHEwpCdXJsaW5ndG9uMQ0wCwYDVQQKEwRBY211MQswCQYD
VQQLEwJTZTEOMAwGA1UEAxMFU21tb24xIDAeBgkqhkiG9w0BCQEWEXNsZWVsc2NA
eWFob28uY29tMB4XDTA5MDUxMzIwMzExOVoXDTEwMDUxMzIwMzExOVowVDELMAkG
A1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQHEwpCdXJsaW5ndG9uMRQwEgYD
VQQKEwtFbmdpbmVlcmluZzENMAsGA1UEAxMEYWNtZTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAvJF6D8gnSvc9Ug4aCkyIqQeWkgkyk+kNYXESQNoOHJTdre9R
6IB5f1UdsM/8klTTpyBwMn+GooeOc8iJ4wks+7VGQegsZEawyDFoTClwQCppWsEF
jOQWtnybP3ZLVBBPJ4Mcowi7qKJK/Pe4aCgfEhue27BWc/HHD2lZIMlyhyECAwEA
ATANBgkqhkiG9w0BAQUFAAOBgQCByeJQ/35H3FtCKtGivKQ19jOunHCynUQHU/eO
DVzUswBlzW+MpOCIz/2fo4eFYNFUrKEiPsOeYSjoOLkgAZMUI5n/x3JcjQX6EiRu
8doByx8DQoEoSIqEbVOBa7fQoZMTke6YMjpnIatEg9Z5seV1AZjgMTTh/p+O3r+7
1jlmbA==
-----END CERTIFICATE-----;

Certificate imported successfully....
WARNING: Configuration changed, run "save-config" command
```

When you see the "Certificate imported successfully" message, ensure the save-config and activate-config commands are run. As a tip, look out for terminal client (like PuTty, Tera Term, etc.) related signed certificate text copy/paste error issues, which may or may not be successful and you may run into certificate import errors. You can delete certificate-record configuration objects and issue a save-config/activate-config to start again (in case of issues) and remove the private key in the SBC associated with the previous certificate

14.1.2 Create a tls-profile

To create a TLS profile use the tls-profile menu under the security branch.

```
Acme1a(configure terminal)# security
Acme1a(security)#tls-profile
Acme1a(tls-profile)#name core
Acme1a(tls-profile)#end-entity-certificate acme1aServerCert
Acme1a(tls-profile)# trusted-ca-certificates ST02-OP1-0703-CA
Acme1a(tls-profile)#done
```

```
tls-profile
      name                              core
      end-entity-certificate            acme1aServerCert
      trusted-ca-certificates
                                        ST02-OP1-0703-CA
      cipher-list
                                        ALL
      verify-depth                      10
      mutual-authenticate               enabled
      tls-version                       compatibility
      cert-status-check                 disabled
      cert-status-profile-list
```

14.1.3 Apply TLS profile on the sip-interface

Exit out of the tls-profile sub-menu and security branch and enter session-router, sip-interface sub-menu.

```
Acme1a(tls-profile)#exit
Acme1a(security)#exit
Acme1a(configure)#session-router
Acme1a(session-router)#sip-interface
Acme1a(sip-interface)#select
<realm-id>:
1: core       2.2.1.4:5067
2: pstn       10.10.1.4:5060
selection: 1
Acme1a(sip-interface)#sip-ports
Acme1a(sip-port)#address 2.2.1.4
Acme1a(sip-port)#port 5067
Acme1a(sip-port)#tls-profile core
Acme1a(sip-port)#transport-protocol TLS
Acme1a(sip-port)#allow-anonymous agents-only
Acme1a(sip-port)#done
```

```
sip-port
                address                         2.2.1.4
                port                            5067
                transport-protocol              TLS
                tls-profile                     core
                allow-anonymous                 agents-only
                ims-aka-profile
Acme1a(sip-port)#exit
Acme1a(sip-interface)#done
```

```
sip-interface
      state                             enabled
      realm-id                          core
      description
      sip-port
            address                           2.2.1.4
            port                              5067
            transport-protocol                TLS
```

```
      tls-profile                     core
      allow-anonymous                 agents-only
      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
options                         100rel-interworking
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               Forearlymedia
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
```

14 2. SRTP Configuration on Net-Net SD

Configuration elements – A brief explanation of the elements needed for SRTP configuration is provided below:

- Configure sdes (or mikey) profile to define the algorithm and cryptos to be used
- Configure a media-sec-policy to instruct the SBC on how to handle media related parameters in SDP received/sent in a realm (RTP, SRTP). Media-sec-policy will be referenced in the realm
- Configure security-policy element which creates a security association in the SBC to do the SRTP encryption and decryption

14.2.1 Algorithm and Crypto configuration on the SBC

Firstly you would configure an element which defines the algorithm and cryptos to be used which is the sdes or mikey profile. Exit out of the sip-interface/session-router branch and go to security -- >media-security -- >sdes-profile

```
Acme1a(sdes-profile)#name sdes1
Acme1a(sdes-profile)#crypto-list "AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32"
Acme1a(sdes-profile)#egress-offer-format same-as-ingress
Acme1a(sdes-profile)#done
```

```
sdes-profile
      name                             sdes1
      crypto-list                      AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
      srtp-auth                        enabled
      srtp-encrypt                     enabled
      srtcp-encrypt                    enabled
      mki                              disabled
      egress-offer-format              same-as-ingress
      use-ingress-session-params
      key
      salt
```

14.2.2 Media Security Policy for SRTP and RTP

Configure a media-sec-policy for SRTP and RTP and reference it in the appropriate realms (srtp policy for mediation server facing realm and rtp for SIP Trunk facing realm). Exit out of the sdes-profile sub-menu and go to media-sec-policy under security branch

```
Acme1a(security)#media-sec-policy
Acme1a(media-sec-policy)name sdespolicy
Acme1a(media-sec-policy)inbound
Acme1a(media-sec-inbound)#profile sdes1
Acme1a(media-sec-inbound)#mode srtp
Acme1a(media-sec-inbound)#protocol sdes
Acme1a(media-sec-inbound)#done
```

```
inbound
            profile                         sdes1
            mode                            srtp
            protocol                        sdes
Acme1a(media-sec-inbound)#
```

```
Acme1a(media-sec-inbound)#exit
Acme1a(media-sec-policy)#outbound
Acme1a(media-sec-outbound)# profile sdes1
Acme1a(media-sec-outbound)#mode srtp
Acme1a(media-sec-outbound)#protocol sdes
Acme1a(media-sec-outbound)#done
outbound
            profile                         sdes1
            mode                            srtp
            protocol                        sdes
Acme1a(media-sec-outbound)#exit
Acme1a(media-sec-policy)#done
```

```
media-sec-policy
      name                            sdespolicy
      pass-through                    disabled
      inbound
            profile                         sdes1
            mode                            srtp
            protocol                        sdes
      outbound
            profile                         sdes1
            mode                            srtp
            protocol                        sdes
      last-modified-by                admin@10.80.20.43
      last-modified-date              2011-04-28 16:55:45
```

```
Acme1a(media-sec-policy)#name rtponly
Acme1a(media-sec-policy)#inbound
Acme1a(media-sec-inbound)#mode rtp
Acme1a(media-sec-policy)#done
```

```
inbound
            profile
            mode                            rtp
            protocol                        none
Acme1a(media-sec-inbound)#
```

```
Acme1a(media-sec-policy)#outbound
Acme1a(media-sec-outbound)# mode rtp
Acme1a(media-sec-outbound)#done
outbound
            profile
            mode                            rtp
            protocol                        none
Acme1a(media-sec-outbound)#
Acme1a(media-sec-outbound)#exit
Acme1a(media-sec-policy)#done
```

```
media-sec-policy
      name                            rtponly
      pass-through                    disabled
      inbound
            profile
            mode                            rtp
            protocol                        none
      outbound
            profile
            mode                            rtp
            protocol                        none
      last-modified-by                admin@10.176.33.21
      last-modified-date              2011-03-29 17:17:43
```

Once media-sec-policy is configured, it will need to be referenced in the realms. Select core realm from the realm-config sub-menu and reference media-sec-policy sdespolicy. Select pstn realm and reference the rtponly policy.

14.2.3. Configure Security Policy

Configure security-policy to create security association in the SBC for encryption/decryption of SRTP. Since the same network-interface will be associated with doing SRTP, you will need to define an explicit tls signal and dns security policy with action set to allow to permit the interface to allow tls sip signaling and dns queries. Exit out of the realm-config/media-manager branch and go to security/ipsec/security-policy

```
Acme1a(security-policy)#name core-tls-signal
Acme1a(security-policy)#network-interface M10:0
Acme1a(security-policy)#priority 1
Acme1a(security-policy)# local-ip-addr-match 2.2.1.4
Acme1a(security-policy)# local-port-match 5067
Acme1a(security-policy)#action allow
Acme1a(security-policy)#done
```

```
security-policy
      name                          core-tls-signal
      network-interface             M10:0
      priority                      1
      local-ip-addr-match           2.2.1.4
      remote-ip-addr-match          0.0.0.0
      local-port-match              5067
      remote-port-match             0
      trans-protocol-match          ALL
      direction                     both
      local-ip-mask                 255.255.255.255
      remote-ip-mask                0.0.0.0
      action                        allow
      ike-sainfo-name
      outbound-sa-fine-grained-mask
            local-ip-mask                 255.255.255.255
            remote-ip-mask                255.255.255.255
            local-port-mask               0
            remote-port-mask              0
            trans-protocol-mask           0
            valid                         enabled
            vlan-mask                     0xFFF
      last-modified-by              admin@10.176.33.21
      last-modified-date            2011-03-29 15:43:58
```

```
Acme1a(security-policy)#name core-srtp
Acme1a(security-policy)#network-interface M10:0
Acme1a(security-policy)#priority 100
Acme1a(security-policy)# local-ip-addr-match 2.2.1.4
Acme1a(security-policy)#action srtp
Acme1a(security-policy)# outbound-sa-fine-grained-mask
Acme1a(outbound-sa-fine-grained-mask)#select
Acme1a(outbound-sa-fine-grained-mask)#local-ip-mask 0.0.0.0
Acme1a(outbound-sa-fine-grained-mask)#remote-port-mask 65535
Acme1a(outbound-sa-fine-grained-mask)#trans-protocol-mask 255
Acme1a(outbound-sa-fine-grained-mask)#done
```

```
outbound-sa-fine-grained-mask
            local-ip-mask                   0.0.0.0
            remote-ip-mask                  255.255.255.255
            local-port-mask                 0
            remote-port-mask                65535
            trans-protocol-mask             255
            valid                           enabled
            vlan-mask                       0xFFF
```

```
Acme1a (outbound-sa-fine-grained-mask)#
Acme1a (outbound-sa-fine-grained-mask)#exit
Acme1a (security)#done
```

```
security-policy
      name                            core-srtp
      network-interface               M10:0
      priority                        100
      local-ip-addr-match             2.2.1.4
      remote-ip-addr-match            0.0.0.0
      local-port-match                0
      remote-port-match               0
      trans-protocol-match            UDP
      direction                       both
      local-ip-mask                   255.255.255.255
      remote-ip-mask                  0.0.0.0
      action                          srtp
      ike-sainfo-name
      outbound-sa-fine-grained-mask
            local-ip-mask                   0.0.0.0
            remote-ip-mask                  255.255.255.255
            local-port-mask                 0
            remote-port-mask                65535
            trans-protocol-mask             255
            valid                           enabled
            vlan-mask                       0xFFF
      last-modified-by                admin@10.80.20.43
      last-modified-date              2011-04-28 13:15:28
```

```
Acme1a(security-policy)#name core-dns
Acme1a(security-policy)#network-interface M10:0
Acme1a(security-policy)#priority 2
Acme1a(security-policy)# local-ip-addr-match 2.2.1.4
Acme1a(security-policy)# remote-ip-addr-match 2.2.1.5
Acme1a(security-policy)#action allow
Acme1a(security-policy)#done
```

```
security-policy
      name                            core-dns
      network-interface               M10:0
      priority                        2
      local-ip-addr-match             2.2.1.4
      remote-ip-addr-match            2.2.1.5
      local-port-match                0
      remote-port-match               0
      trans-protocol-match            ALL
      direction                       both
      local-ip-mask                   255.255.255.255
      remote-ip-mask                  255.255.255.255
      action                          allow
      ike-sainfo-name
      outbound-sa-fine-grained-mask
            local-ip-mask                   255.255.255.255
            remote-ip-mask                  255.255.255.255
            local-port-mask                 0
            remote-port-mask                0
            trans-protocol-mask             0
            valid                           enabled
            vlan-mask                       0xFFF
      last-modified-by                admin@10.80.20.43
      last-modified-date              2011-04-27 18:52:23
```

14.2.4 Change transport-method and port on Lync mediation server Session-agent

Mediation server listens for TLS signaling on port 5067 (as default) so that along with transport-method will need to be reflected in the E-SBC session-agent. Exit out from security branch and go to session-router, session-agent branch of the CLI

```
ACME1A(session-router)# session-agent
ACME1A(session-router)# select
<hostname>:

1: OP1-0704.st02.loc realm=core ip=2.2.1.8

2: OP1-0706.st02.loc realm=core   ip=2.2.1.9

3: 10.10.1.8 realm=pstn ip=

Selection: 1
ACME1A(session-agent)#transport-method staticTLS
ACME1A(session-agent)#port 5067
ACME1A(session-agent)#done
```

Similarly, make the change for Mediation server 2 (with hostname `OP1-0706.st02.loc`)

15. 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 (Net-Net SD).

Media Bypass from SD's perspective is to be able route RTP traffic to an endpoint/lync client on a private routable network directly (instead of RTP going to mediation server). To enable the SBC to handle media bypass feature in Lync , one 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

```
acme1a(realm-config)#restricted-latching sdp
acme1a(realm-config)#done
```

```
realm-config
identifier                      core
description                     Mediation Server-facing
addr-prefix                     0.0.0.0
network-interfaces
                                M10:0
mm-in-realm                     disabled
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
   ext-policy-svr
   symmetric-latching              disabled
   pai-strip                       disabled
   trunk-context
   early-media-allow
   enforcement-profile
   additional-prefixes
   restricted-latching             sdp
   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
   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
```

Exit out.and do a save-config and an activate-config to make the configuration complete and persistent This will make it persistent through reboots.

```
ACME1A# 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'.
ACME1A# 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
```

16. 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.

```
ACME1A(steering-pool)# exit
ACME1A(media-manager)# exit
ACME1A(configure)# exit
ACME1A# verify-config
-----------------------------------------------------------------------
Verification successful! No errors nor warnings in the configuration
```

Configuration is now complete.

A basic configuration on the Net-Net ESD to route calls to and from the Lync Server 2013 environment is now complete. You can now test connectivity and verify calls working following the tests outlined in the next section.

Phase III – Test connectivity to SIP Trunk

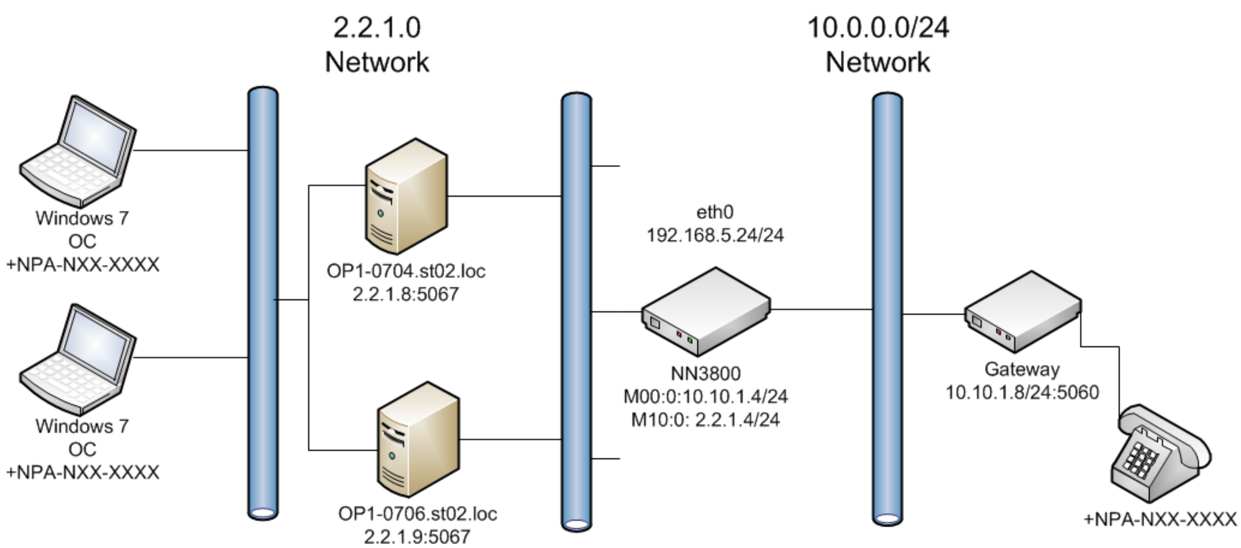
Overview

Once the Lync Server 2013 and the Net-Net Session Director have been configured, the final phase is to test connectivity and the SIP trunk interface. Acme Packet Net-Net Session Director 3820 and NN4500 have been qualified with Lync Server 2013 as part of the Unified Communications open Interoperability Program (UCOIP) test plan. Some of the test cases to verify connectivity and inbound/outbound calling are enlisted below. This section provides an overview of the topology/setup and a list of tests to verify is the deployment was successful. It is highly recommended that you use this test plan as a baseline in addition to any other tests that you may plan to run.

UCOIP Test Plan & Results

The following diagram shows the test topology.

Lync Server 2010 Acme Packet Test Topology



Test Case#	Description of Test Case	Result	Comments
408347	Lync End Point receives a call from PSTN End Point with G.711 A-law and/or G.711 U-law codecs	Pass	
408351	PSTN End Point places a call from Lync End Point on hold for 15 minutes and then resumes	Pass	
408348	PSTN End Point1 calls Lync End Point that forwards the call to PSTN End Point2	Pass	
408352	PSTN End Point calls Lync End Point1 that performs Blind Transfer to Lync End Point2 with REFER	Pass	
408349	PSTN End Point1 calls Lync End Point that escalates the call to a conference by inviting PSTN End Point2	Pass	
408350	Device fails over incoming call to Mediation Server2 when Mediation Server1 sends 503 Service Unavailable response	Pass	
408282	Device utilizes 'pool' certificates for a secure call	Pass	
408127	Device adds at least one "crypto" attribute for each media description line in the SDP	Pass	
408117	Device handles 488 Not Acceptable Here response from the Mediation Server operating in RTP only mode	Pass	
408124	Device sends Crypto attributes in SDP for call from PSTN End Point to Lync End Point	Pass	
408118	Device sends its own FQDN in contact header for TLS call from Lync End Point to PSTN End Point	Pass	
408070	PSTN End Point calls Lync End Point and hangs up while Lync End Point is still ringing	Pass	
408125	PSTN End Point calls Lync End Point with security enabled and Lync End Point later hangs up	Pass	
408080	Inbound call to Lync End Point from PSTN End Point with a very long Request-URI in the INVITE	Pass	
408065	Device correctly handles non-E.164 number in outbound Request	Pass	

	URI		
408085	Device establishes call to Lync End Point with configured value of ptime	Pass	
408063	Device generates 603 Decline response for a call rejected by PSTN End Point	Pass	
408078	Device handles call from Mediation Server with an alias name in the FROM header	Pass	
408073	Device processes call from Lync End Point with E.164 number in FROM Header URI	Pass	
408071	Device processes phone-context in Request and To URI from Lync End Point	Pass	
408066	Lync End Point calls PSTN End Point and hangs up before receiving 200 OK from Device	Pass	
408062	Lync End Point calls PSTN End Point with a call duration longer than 32 seconds	Pass	
408077	Lync End Point calls an IVR number and navigates through the IVR menu after call connection.	Pass	
408074	Lync End Point response to PSTN End Point is delayed due to network delay	Pass	
408072	Lync End Point sends INVITE with E.164 number and extension in Request and To URI	Pass	
408081	Mediation Server renegotiates an existing voice session with a different IP address	Pass	
408069	PSTN End Point disconnects established call from Lync End Point	Pass	
408068	PSTN End Point disconnects established call to Lync End PointEnd Point disconnects established call to Lync End Point	Pass	
408067	PSTN End Point displays Lync End Point Caller ID for Outbound Call	Pass	
408183	Device negotiates Comfort Noise in a call from Lync End Point to PSTN End Point. (IPv6)	Pass	

408101	Device offers DTMF payload type in the range of 96-127 to Mediation Server	Pass	
408092	Lync End Point is able to establish a call with PSTN End Point using G.711 A-law codec	Pass	
408086	Lync End Point makes a call to PSTN End Point with G.711 A-law and/or G.711 U-law codecs	Pass	
408114	Lync End Point makes a call to PSTN End Point with G.711 U-law codec	Pass	
408119	Lync End Point receives a call from PSTN End Point with G.711 U-law codecs	Pass	
408121	Mediation Server renegotiates an existing voice session with a different RTP port	Pass	
408090	PSTN End Point is able to establish a call with Lync End Point using G.711 A-law codec	Pass	
408112	Device sends PRACK for reliable Early Media for a call from PSTN End Point to Lync End Point	Pass	
408113	Device sends PRACK for reliable Early Media for call from PSTN End Point to Lync End Point with SRTP Optional	Pass	
408064	Lync End Point calls IVR number and navigates through the IVR menu before call Connection	Pass	
408106	Lync End Point hears Early Media for a call to PSTN End Point	Pass	
408104	Device does not change the SSRC of an established inbound RTP session	Pass	
408126	Device does not change the SSRC of an established inbound SRTP session	Pass	
408100	Device does not change the SSRC of an established outbound RTP session	Pass	
408123	Device does not change the SSRC of an established outbound SRTP session	Pass	
408093	Device handles multiple RTP streams for a call to Lync End Point	Pass	

408097	Device sends RTCP packets when Lync End Point places call on hold	Pass	
408128	Device sends RTCP packets while playing music on hold	Pass	
408103	Device sends RTCP sender and receiver reports	Pass	
408105	Device sends RTCP sender and receiver reports for a secure call	Pass	
408109	Device disconnects a forked call if PSTN End Point hangs up while phones are ringing	Pass	
408079	PSTN End Point1 calls Lync End Point that is set to simultaneous ring to Lync End Point and PSTN End Point2 answers	Pass	
408110	Device disconnects a forked secure call if PSTN End Point hangs up while phones are ringing	Pass	
408094	Device handles multiple SRTP streams for a secure call to Lync End Point	Pass	
408095	Device handles multiple SRTP streams for a secure call to Lync End Point when Media Bypass is OFF	Pass	
408107	Lync End Point hears Early Media for a secure call to PSTN End Point	Pass	
408108	Lync End Point hears Early Media for a secure call to PSTN End Point when Media Bypass OFF	Pass	
408129	Lync End Point makes a secure call to PSTN End Point	Pass	
408122	Lync End Point makes a secure call to PSTN End Point and PSTN End Point later hangs up	Pass	
408130	Lync End Point makes a secure call to PSTN End Point with call duration more than 32 seconds and SRTP set to Optional	Pass	
408120	Lync End Point receives a secure call with G.711 U-law codec with Media Bypass OFF	Pass	
408091	PSTN End Point is able to establish a secure call with Lync End Point using G.711 A-law codec	Pass	
408199	Device receives History-Info headers in the SIP Invite without	Pass	

	adverse effect		
408200	3rd Party Presence headers do not cause Device failure	Pass	
408225	PSTN End Point places a call with Media Bypass OFF from Lync End Point on hold for 15 minutes and then resumes	Pass	
408235	PSTN End Point places a secure call from Lync End Point on hold and then resumes	Pass	
408224	PSTN End Point places a secure call to Lync End Point on hold and resumes after 15 minutes	Pass	
408236	PSTN End Point places a secure call to Lync End Point on hold and then resumes	Pass	
408226	PSTN End Point puts Lync End Point on hold and resumes after 15 minutes for a secure call	Pass	
408234	Lync End Point places a call from PSTN End Point on hold for 15 minutes and then resumes	Pass	
408229	Lync End Point places a call to PSTN End Point on hold and resumes after 12 minutes	Pass	
408232	Lync End Point places a secure call from PSTN End Point on hold and resumes after 15 minutes	Pass	
408230	Lync End Point places a secure call to PSTN End Point on hold and resumes after 12 minutes	Pass	
408227	Lync End Point resumes call to PSTN End Point after playing music on hold for 15 minutes	Pass	
408228	Lync End Point plays music on hold when it holds a secure call from PSTN End Point to Lync End Point	Pass	
408231	Lync End Point plays music when it holds call from PSTN End Point to Lync End Point	Pass	
408207	PSTN End Point1 calls Lync End Point that forwards all calls to PSTN End Point2 when Media Bypass OFF	Pass	
408206	PSTN End Point1 makes a secure call to Lync End Point that forwards the call to PSTN End Point2 with Media Bypass OFF	Pass	

408205	PSTN End Point1 makes a secure call to Lync End Point that has call forwarded to PSTN End Point2	Pass	
408258	Device generates INVITE with Replaces and Referred-By headers when it receives a REFER request	Pass	
408254	Device includes REFER in ALLOW header in INVITE sent to Mediation Server	Pass	
408259	Device maintains the original session when rejecting a call transfer with REFER	Pass	
408257	Device supports Hairpin Elimination for Blind Transfer with REFER	Pass	
408260	Device supports Hairpin Elimination for secure Blind Transfer with REFER	Pass	
408255	PSTN End Point1 calls Lync End Point and Lync End Point Blinds Transfers the call to PSTN End Point2	Pass	
408256	PSTN End Point1 makes a secure call to Lync End Point and Lync End Point Blinds Transfers the call to PSTN End Point2	Pass	
408263	Device does not drop the call when Consultative Transfer by Lync End Point to second PSTN End Point fails	Pass	
408264	Device supports Hairpin Elimination for Consultative Transfer with REFER	Pass	
408265	Device supports Hairpin Elimination for secure Consultative Transfer with REFER	Pass	
408261	PSTN End Point1 calls Lync End Point and Lync End Point Consultative Transfers to PSTN End Point2	Pass	
408262	PSTN End Point1 makes a secure call to Lync End Point and Lync End Point Consultative Transfers to PSTN End Point2	Pass	
408213	Lync End Point1 calls Lync End Point2 and escalates the call to a conference, inviting PSTN End Point and later removing it	Pass	
408214	PSTN End Point establishes a call with the Conference Auto Attendant	Pass	
408215	Conference call involving two Lync End Points and PSTN End Point,	Pass	

	Lync End Point puts the call on hold		
408309	Device distributes new calls among DNS configured Mediation Serversn	Pass	
408311	Device honors TTL when distributing new calls among DNS configured Mediation Servers	Pass	
408286	Device responds to OPTIONS as keep alive to Mediation Server over TCP	Pass	
408288	Device responds to OPTIONS as keep alive to Mediation Server over TLS	Pass	
408289	Device resumes sending calls to Mediation Server when it starts receiving OPTIONS response from that Mediation Server	Pass	
408292	Device routes calls from newly added Mediation Server after DNS cache is updated	Pass	
408287	Device sends periodic OPTIONS message as keep alive to Mediation Server	Pass	
408285	Device uses load balancing to distribute inbound calls among Mediation Servers in a cluster	Pass	
408290	Lync End Point establishes a call with PSTN End Point when interface between Device and Mediation Server1 goes down	Pass	
408291	PSTN End Point establishes a call with Lync End Point when interface of Mediation Server1 goes down	Pass	
408294	Device does not offer new calls to a failed Mediation Server	Pass	
408293	Device fails over incoming call to a second Mediation Server when the first Mediation Server times out	Pass	
408306	Device utilizes failover and does not offer new calls to a failed Mediation Server	Pass	
408058	PSTN End Point calls Lync End Point with Caller ID set to 'Anonymous' on Device	Pass	

408321	Device disconnects call when Mediation Server sends 408 Request Timeout for call from PSTN End Point	Pass	
408327	Device disconnects call when Mediation Server sends 501 Not Implemented for call from PSTN End Point	Pass	
408328	Device disconnects call when Mediation Server sends 606 Not Acceptable for call from PSTN End Point	Pass	
408319	Device generates 482 Loop Detected response to a call from Lync End Point when a loop is detected	Pass	
408325	Device generates 486 Busy Here response from a busy PSTN End Point	Pass	
408324	Device handles call from Lync End Point to a user that does not exist in the domain	Pass	
408318	Device processes 482 Loop Detected response from Lync End Point	Pass	
408326	Device processes 486 Busy Here response from a busy Lync End Point	Pass	
408317	Device processes 488 Not Acceptable Here response for unsupported codec from Mediation Server	Pass	
408322	Device processes 603 Decline from Lync End Point for a secure call	Pass	
408323	Device processes 603 Decline response from Lync End Point	Pass	
408320	Device rejects call from Lync End Point to PSTN End Point when the associated PRI line is down	Pass	
408329	Device responds with 488 Not Acceptable Here when Mediation Server offers a codec unsupported on the device	Pass	
408315	Device sends 414 Request-URI Too Long when unable to handle very long Request URI	Pass	
408316	Device times out after 180 seconds of no response from Lync End Point following 100 Trying	Pass	

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 Net-Net ESD 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

Net-Net ESD

The Net-Net ESD 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 Net-Net ESD Console:

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

Examining the log files.

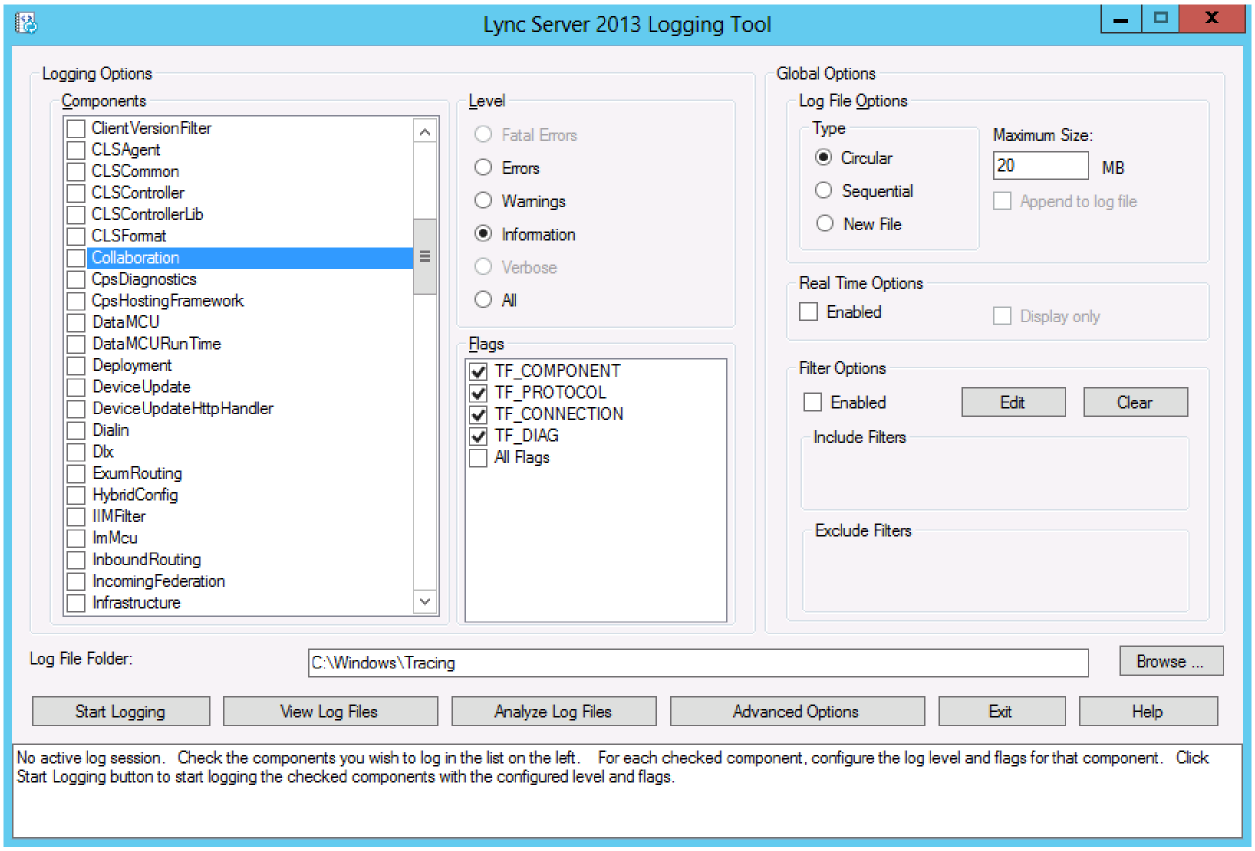
Note: You will FTP to the management interface of the Net-Net SBC with the username user and user mode password (the default is "**acme**").

```
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.



Appendix

Known Issues

No Ring Back Tone heard for inbound calls from PSTN to MS Lync through E-SBC

Recently, in some accounts where MS Lync and Acme Packet SBCs 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 Acme Packet. The workaround is an interim solution while a permanent solution is being researched and developed by Acme Packet Engineering

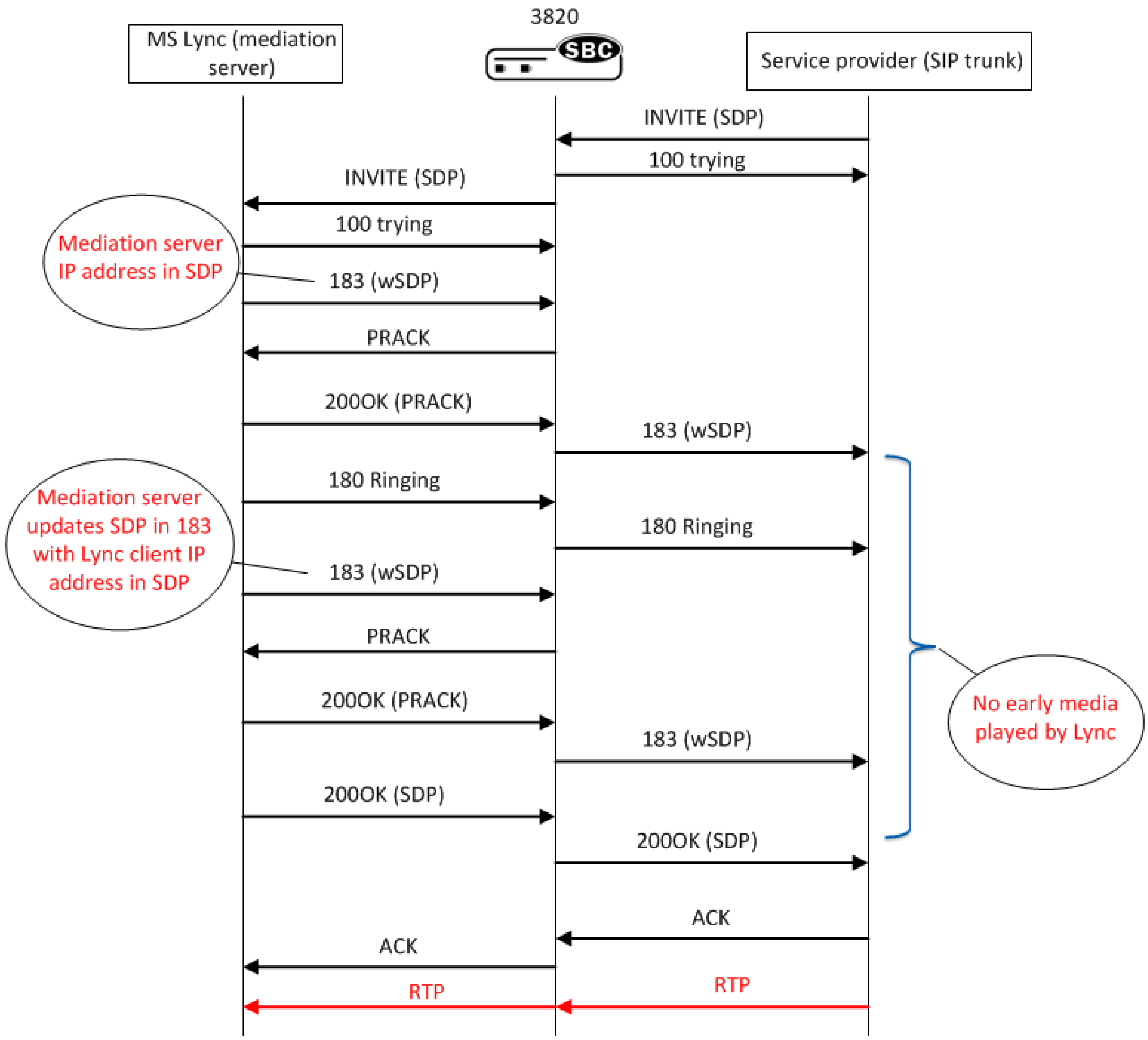
Media Bypass

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:

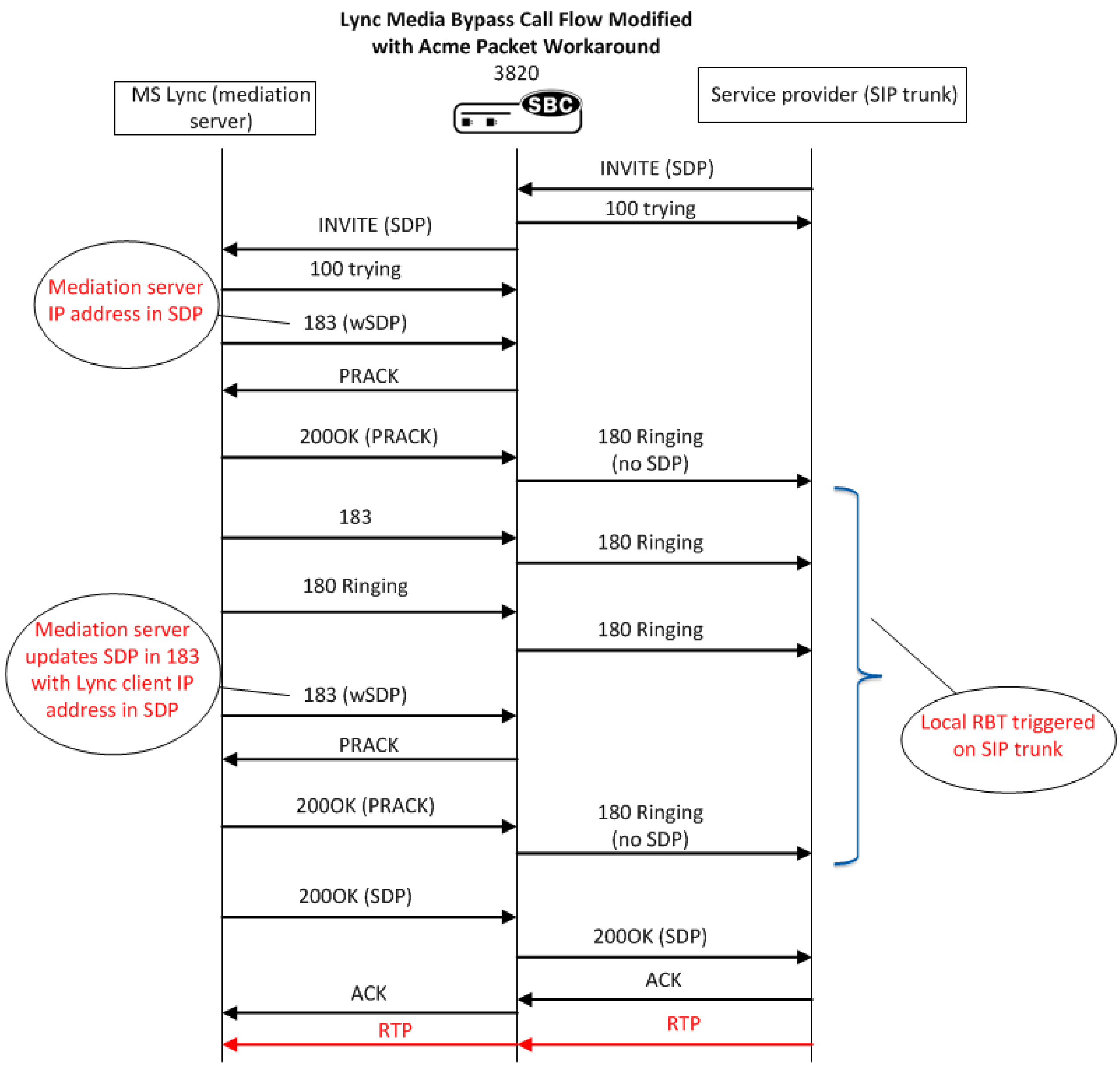
Lync Media Bypass enabled Call Flow



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.

Acme Packet 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 Acme Packet's robust Sip Manipulation and Sip Response Map features to the following:



Configuration Changes required

In-manipulation Forearlymedia to be applied on Lync facing sip-interface

==

```
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                              formod183
        header-name                       From
        action                            sip-manip
        comparison-type                   case-sensitive
        msg-type                          any
        methods
        match-value
        new-value                         Stripsdp183
```

```
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
```

SIP Response Map to be applied on SIP Trunk facing Sip-interface

==

```
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                        pstn
      description                     SIP Trunk-facing interface
      sip-port
      address                         10.10.1.4
      port                            5060
      transport-protocol              TCP
      tls-profile
      allow-anonymous                 agents-only
…
      response-map                    change183to180
```