510-0031-01 Acme Packet Transcoding – Microsoft Lync with VZB IP Trunking

Document Overview

This application note defines a SIP configuration model suitable for the Acme Packet NN3000-4000 series Session Border Controllers (SBCs) connecting Microsoft Lync Server 2010 from a customer premise to Verizon Business' IP Trunking service (US/EMEA/IPCC) with PIP transport. The reference configuration presented was tested in Verizon's labs.

Contents

Document Overview

Microsoft Lync Server 2010 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. Acme Packet Net-Net Session Director (Net-Net SD) Session Border Controllers (SBCs) play an important role in SIP trunking as they are used by many ITSPs and some enterprises as part of their SIP trunking infrastructure.

This application note has been prepared as a means of ensuring that SIP trunking between Lync Server, Acme Packet SBCs and Verizon Business IP Trunking services are 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.*

It should be noted that while this application note focuses on the optimal configurations for the Acme Packet Net-Net SD 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 SD 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 with any questions pertaining to this topic.

For additional information on Lync Server, please visit http://www.microsoft.com/lync. For further configuration support, please refer to the following:

- www.microsoft.com/download/en/details.aspx?id=23888 (Help file)
- http://technet.microsoft.com/en-us/library/gg293124.aspx (Lync planning and installation documentation)
- http://www.microsoft.com/download/en/details.aspx?id=19711 (Lync Planning Tool)

For additional information on Acme Packet SBCs and Lync Server, please visit the URLs below.

- http://www.acmepacket.com/enterprise-solutions-ms-lync.htm
- http://www.acmepacket.com/fixed-line-solutions-ms-lync.htm

Introduction

1.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring both the Net-Net SD SBC and the Lync Mediation Server. 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.

1.2. Requirements

- Fully functioning Lync Server deployment, including Active Directory and DNS
- A dedicated Mediation Server for the SIP trunking connection
- Lync Server 2010, Version 4.0.7577.0
- Lync Client 2010- Version 4.0.7577.254
- Acme Packet Net-Net SD 3820 or 4500 series running Net-Net OS SCX6.3.7f2p4. Note: the configuration running on the SBC is backward/forward compatible with any release in the 6.3.7 stream.

1.3. Architecture

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

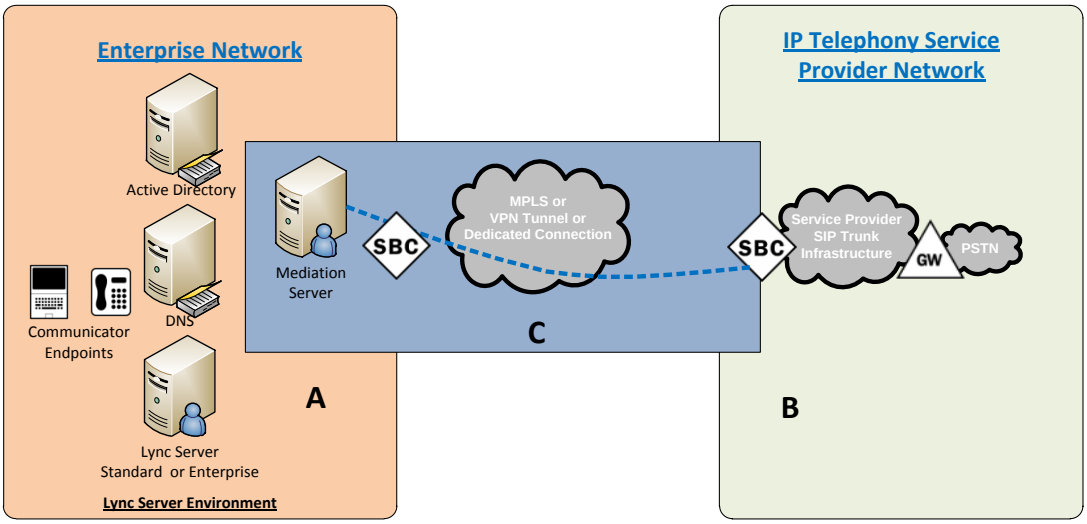


Figure 1 – Logical Reference Architecture

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 the Mediation Server
- Phase 2 – Configure the Session Director
- Phase 3 – Test the Interface

1.4. Lab Configuration

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

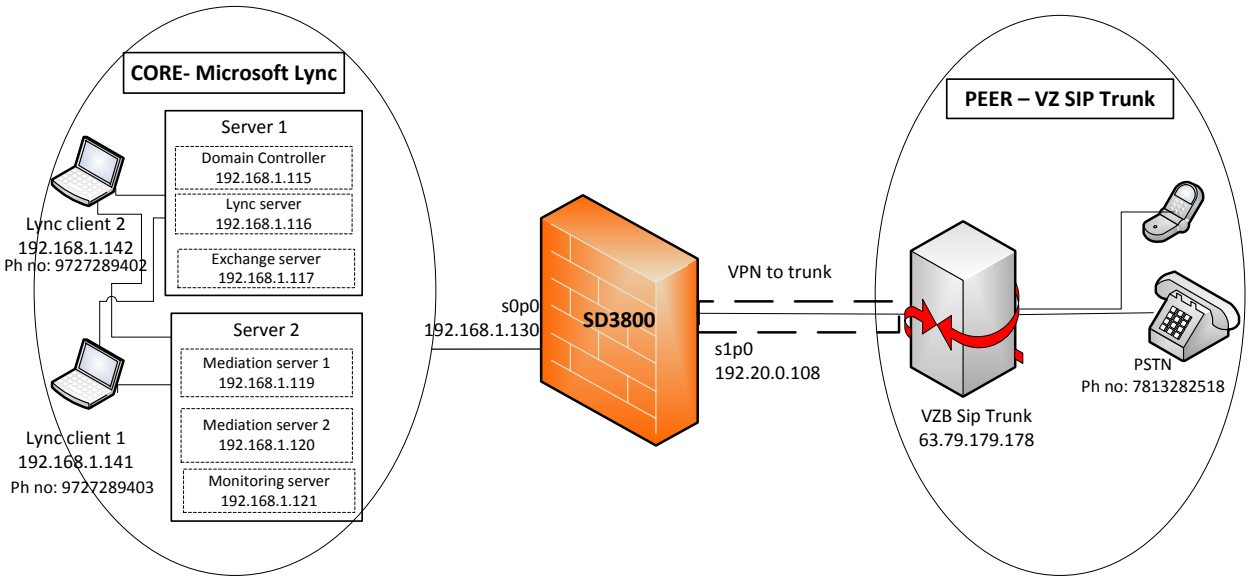


Figure 2 – Lab Architecture

Verizon Feature Support

1.5. US Features

Test Case ID	Requirement	Microsoft	Comments	Acme Packet	Comments
Security					
TC1	Layer 2 IPSec Authentication	Not supported	Acme Packet SBC to terminate IPSec tunnels (SBC-only); Lync Rel. 7.1	Supported	
DNS SRV					
TC2	DNS SRV Service Protocols/Port Adherence	Not supported		Supported	
Inbound					
TC3	Inbound Call Loop Avoidance	Supported	SBC can change header response code	Supported	
TC4	Inbound call with originator (PSTN) release	Supported		Supported	
TC5	Inbound call with terminator (CPE) release	Supported		Supported	
TC6	Inbound call - Hang-up during Ring phase	Supported		Supported	
TC7	Inbound Call - customer phone not registered/online	Supported		Supported	
TC8	Inbound Calling Line Identification (Caller-ID)	Supported		Supported	
TC9	Inbound Call Waiting	Supported		Supported	
TC10	Inbound FAX	Not supported	SBC to terminate fax-data & to support media-bypass (Note: Request traces)	Supported	
TC11	Inbound Call from PSTN with Privacy Restricted	Supported	May need SBC to translate Anonymous-Invalid	Supported	
TC12	Inbound call - User Busy	Supported	Respond with 486	Supported	
TC13	Inbound Call - Ring No Answer Timer Expire	Supported		Supported	
TC14	Inbound Call - Long Call Duration	Supported		Supported	
Outbound				Supported	
TC15	Unscreened ANI using Diversion Header	Not supported	Referred-by header in SIP INVITE, SBC to add DIVERSION header	Supported	
TC16	Unscreened ANI using P-Asserted Identity	Not supported	SBC assistance, test	Supported	
TC17	Outbound call with Originator (CPE) release	Supported		Supported	
TC18	Outbound call with Terminator (PSTN) release	Supported		Supported	
TC19	Outbound call - Hangup during ring phase	Supported		Supported	
TC20	Outbound 1+10digit call	Supported		Supported	
TC21	Outbound International Call	Supported		Supported	
TC22	Outbound 311 Non Emergency call	Supported		Supported	

TC23	Outbound 555-1212 Directory Assistance	Supported		Supported
TC24	Outbound 411 Directory Assistance	Supported		Supported
TC25	Outbound 1411 Directory Assistance	Supported		Supported
TC26	Outbound 711 Telephone Relay Services (Hearing Impaired)	Supported	TTY-mode supported in Lync client; may need SBC assistance (Test)	Supported
TC27	911 Emergency Service	Supported	Supported with ELIN gateway (Note: SBC to provide similar header format, test)	Supported
TC28	Outbound 511 Information Line	Supported	Note: anticipate call-routing test	Supported
TC29	Outbound Toll-Free Call	Supported		Supported
TC30	Operator assistance (0+Local)	Supported		Supported
TC31	Operator assistance (0+Toll)	Supported		Supported
TC32	Operator assistance (0Minus)	TBD	E.164 number; test	Supported
TC33	Operator assistance (00Minus)	TBD	E.164 number; test	Supported
TC34	Operator assistance (01+international)	TBD	E.164 number; test	Supported
TC35	Outbound FAX	Not supported	G.711 supported; transcoding required for T.38 (TBD)	Supported
TC36	Outbound Calling Line Identifier (Caller ID)	Supported		Supported
TC37	Outbound Fast Answer	Supported	Test: SDP in 200 OK	Supported
TC38	Outbound Call to PSTN with Privacy Requested	TBD	Test if its supported	Supported
TC39	Calling Party Number not provisioned	Supported	Provisionally supported based on receiving 408 from network	Supported
TC40	Premium Call (900)	Supported		Supported
TC41	Premium Call (976)	Supported		Supported
TC42	Outbound Call - Long Call Duration	Supported		Supported
TC43	Outbound Call – User Busy	Supported		Supported
TC44	Outbound Call – Ring No Answer Timer Expire	Supported		Supported
TC45	Private Dialing Plan	Supported	Routing assistance from SBC (Two SBC/Lync locations)	Supported
Protocols				
TC46	UDP for SIP	Not supported	SBC to translate from TCP-to-UDP	Supported
TC47	SDP support (RFC 2327)	Supported		Supported
TC48	RTP and RTCP support (RFC 3550)	Supported		Supported
TC49	SIP Headers	Supported	Compact header (short) format not supported by Lync, SBC support required	Supported
TC50	18x Behavior	Supported		Supported
TC51	302 Behavior	Not supported	SBC to proxy 302	Supported
TC52	Diversion Header	Not supported	Lync does not support outbound DIVERSION HEADER; SBC to translate from REFERRED-BY	Supported
TC53	DTMF RFC 2833—Outbound	Supported	Only for G.711; SBC transcoding required for G.729-to-G.711	Supported
TC54	DTMF RFC 2833—Inbound	Supported	Only for G.711; SBC transcoding required	Supported

			for G.729-to-G.711	
TC55	Offer/Answer with SDP (RFC3264)	Supported		Supported
TC56	Call Hold (RFC 3264)	Supported		Supported
TC57	Media Inactivity	Supported		Supported
TC58	FQDN	Supported		Supported
Media				
TC59	G.711 ulaw	Supported		Supported
TC60	G.729 and G.729a	Not supported		Supported
TC61	Codec Negotiation	Supported		Supported
TC62	Early Media Support	Supported	PRACK interworking via SBC	Supported
Diffserv				
TC63	RTP	Supported		Supported
TC64	SIP	Supported		Supported
Attended Transfer Re-Invite Method				
TC65	IPPBX-PSTN-IPPBX	Supported		Supported
TC66	IPPBX-PSTN-PSTN	Supported		Supported
TC67	PSTN-IPPBX-IPPBX	Supported		Supported
TC68	PSTN-IPPBX-PSTN	Supported		Supported
Semi-Attended Call Transfer Reinvite method				
TC69	IPPBX-PSTN-IPPBX	Supported	Test if its supported	Supported
TC70	IPPBX-PSTN-PSTN	Supported	Test if its supported	Supported
TC71	PSTN-IPPBX-IPPBX	Supported	Test if its supported	Supported
TC72	PSTN-IPPBX-PSTN	Supported	Test if its supported	Supported
Blind Call Transfer Re-INVITE Method				
TC73	IPPBX-PSTN-IPPBX	Supported	Test if its supported	Supported
TC74	IPPBX-PSTN-PSTN	Supported	Test if its supported	Supported
TC75	PSTN-IPPBX-IPPBX	Supported	Test if its supported	Supported
TC76	PSTN-IPPBX-PSTN	Supported	Test if its supported	Supported
Attended Call Transfer REFER Method				
TC77	IPPBX-PSTN-IPPBX	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported
TC78	IPPBX-PSTN-PSTN	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported
TC79	PSTN-IPPBX-IPPBX	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported
TC80	PSTN-IPPBX-PSTN	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported
Semi-Attended Call Transfer REFER Method				
TC81	IPPBX-PSTN-IPPBX	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported
TC82	IPPBX-PSTN-PSTN	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER;	Supported

			SBC to mediate)		
TC83	PSTN-IPPBX-IPPBX	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported	
TC84	PSTN-IPPBX-PSTN	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported	
Blind Call Transfer REFER Method					
TC85	IPPBX-PSTN-IPPBX	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported	
TC86	IPPBX-PSTN-PSTN	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported	
TC87	PSTN-IPPBX-IPPBX	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported	
TC88	PSTN-IPPBX-PSTN	TBD	SBC will terminate SIP REFER (Lync can originate REFER, but not accept REFER; SBC to mediate)	Supported	
Call Conference (Optional)			Hmmm \		
TC89	IPPBX-PSTN-IPPBX	Supported		Supported	
TC90	IPPBX-PSTN-PSTN	Supported		Supported	
TC91	PSTN-IPPBX-IPPBX	Supported		Supported	
TC92	PSTN-IPPBX-PSTN	Supported		Supported	
CPE Failover Behavior (Optional)					
TC93	Options method request and response	Supported		Supported	
TC94	Round-Robin (Load share 50/50 between the two CPEs	Supported	DNS SRV load-balancing; SBC can define mediation servers if DNS not involved	Supported	
TC95	Primary/Secondary failover (Hunt)	Supported		Supported	
TC96	Both CPE Fail behavior	Supported	Lync/SBC originates 503/506	Supported	
TC97	Ambient Noise – CPE to PSTN	Not supported		Supported	Pass through only. Do not generate
TC98	Ambient Noise – PSTN to CPE	Not supported		Supported	Pass through only. Do not generate

1.6. EMEA Features

Test #	Test Case Description	Lync	Comments	Acme Packet	Comments
7.1. Security Test Case					
TCA	Layer-2 IPSec Authentication (Mandatory)	Not supported	Acme Packet SBC to terminate IPSec tunnels (SBC-only); Lync Rel. 7.1	Supported	
7.2. DNS-SRV Test Case					

TCB	DNS-SRV – Service Protocols/Port Adherence	Not supported		Supported
7.3. Inbound – Calls From Verizon PSTN to the Customer VoIP				
TC1	Inbound - Call Loop Avoidance Verification	Supported	SBC can change header response code	Supported
TC2	Inbound - Hang Up During Ring Phase (Call Canceled)	Supported		Supported
TC3	Inbound - Phone not connected/not online /not registered	Supported		Supported
TC4	Inbound - PSTN to Customer CPN Presentation = Allowed, Terminator Release		Supported	
TC5	Inbound - Fax	Not supported	SBC to terminate fax-data & to support media-bypass (Note: Request traces)	Supported
TC6	Inbound - PSTN to Customer with Privacy Requested	Supported	May need SBC to translate Anonymous-Invalid	Supported
TC7	Inbound - Busy Line	Supported	Respond with 486	Supported
TC8	Inbound - Ring No Answer (RNA)	Supported		Supported
TC9	Inbound - Long Duration Call with Originator Release	Supported		Supported
TC10	Inbound - G.711 CODEC Negotiation	Supported		Supported
TC11	Inbound - G.729 CODEC Negotiation	Not supported	SBC to transcode Codecs, when necessary	Supported
TC12	Inbound- Customer is Off-hook	Supported		Supported
TC13	Inbound - DTMF (RFC2833)	Supported		Supported
TC14	Inbound - Ambient Noise – PSTN to CPE	Not supported		Supported
TC15	Inbound – Call Forward to CPE Using SIP Diversion Header	Not supported	Referred-by header in SIP INVITE, SBC to add DIVERSION header	Supported
7.4. Outbound – Customer VOIP TO Verizon PSTN CALL DIRECTION				
TC16	Outbound - Hang Up During Ring Phase (Call Canceled)	Supported		Supported
TC17	Outbound - Local Geographic National PSTN Call Originator Release	Supported		Supported
TC18	Outbound - Geographic National PSTN Call Terminator Release	Supported		Supported
TC19	Outbound - National Cell Call	Supported		Supported
TC20	Outbound - International PSTN Call	Supported		Supported
TC21	Outbound - Short Dial Number Calls	Supported		Supported
TC22	Outbound - Emergency Services Call (Police, EMS/Fire)	Supported	Supported with ELIN gateway (Note: SBC to provide similar header format, test)	Supported
TC23	Outbound - Freephone Call (080X)	Supported		Supported
TC24	Outbound - Business Rate Services (08XX)	Supported		Supported
TC25	Outbound - FAX	Not supported	G.711 supported; transcoding required for T.38 (TBD)	Supported

TC26	Outbound - Fast Answer Call	Supported	Test; SDP in 200 OK	Supported
TC27	Outbound - Call with Privacy Asserted (VoIP to PSTN)	TBD	Test if its supported	Supported
TC28	Outbound - CPN Not Provisioned in Verizon Proxy	Supported		Supported
TC29	Outbound - Premium Rate – 09XX	Supported		Supported
TC30	Outbound - Long Duration Call with INFO Method Call Audit	Supported		Supported
TC31	Outbound - Call Origination with 183 Session Progress (with SDP)	Supported		Supported
TC32	Outbound - Call Forward to PSTN using SIP Diversion Header	Supported		Supported
TC33	Outbound - Call Hold	Supported		Supported
TC34	Outbound - DTMF (RFC2833) NTE Payload Negotiation	Supported		Supported
TC35	Outbound - G711 CODEC Negotiation	Supported		Supported
TC36	Outbound - G729 CODEC Negotiation	Not supported	SBC to transcode Codecs, when necessary	Supported
TC37	Outbound - Ring No Answer (RNA)	Supported		Supported
TC38	Outbound - Ambient Noise – CPE to PSTN	Not supported		Supported
7.5. Protocol Test Cases				
TC39	UDP for SIP	Not supported	SBC to translate from TCP-to-UDP	Supported
TC40	SDP Support (RFC 2327)	Supported		Supported
TC41	RTP and RTCP (RFC 3550)	Supported		Supported
TC42	SIP Headers	Supported	Compact header (short) format not supported by Lync, SBC support required	Supported
TC43	'18X' Behavior	Supported		Supported
TC44	'302' Behavior	Not supported	SBC to proxy 302	Supported
TC45	Support for Offer / Answer with SDP (RFC3264)	Supported		Supported
TC46	Media Inactivity	Supported		Supported
TC47	Use of FQDN IP Addressing in SIP Messaging	Supported		Supported
'7.6. Differentiated Services (DiffServ) Test Cases				
TC48	RTP media marked with DSCP EF or CS5	Supported		Supported
TC49	SIP signaling marked with DSCP AF32 or CS3	Supported		Supported
7.7. Re-Invite Call Test Cases				
7.7.1. Attended Call Transfer Test Cases				
TC50	IP-PBX calls PSTN attended transfer to IP-PBX	Supported		Supported
TC51	IP-PBX calls PSTN attended transfer to PSTN	Supported		Supported
TC52	PSTN calls IP-PBX attended transfer to IP-PBX	Supported		Supported
TC53	PSTN calls IP-PBX	Supported		Supported

	attended transfer to PSTN			
7.7.2. Semi-Attended Call Transfer Test Cases				
TC54	IP-PBX calls PSTN semi-attended transfer to IP-PBX	Supported	Test if its supported	Supported
TC55	IP-PBX calls PSTN semi-attended transfer to PSTN	Supported	Test if its supported	Supported
TC56	PSTN calls IP-PBX semi-attended transfer to IP-PBX	Supported	Test if its supported	Supported
TC57	PSTN calls IP-PBX semi-attended transfer to PSTN	Supported	Test if its supported	Supported
7.7.3. Blind Call Transfer Test Cases				
TC58	IP-PBX calls PSTN with blind transfer to IP-PBX	Supported	Test if its supported	Supported
TC59	IP-PBX calls PSTN with blind transfer to PSTN	Supported	Test if its supported	Supported
TC60	PSTN calls IP-PBX with blind transfer to IP-PBX	Supported	Test if its supported	Supported
TC61	PSTN calls IP-PBX with blind transfer to PSTN	Supported	Test if its supported	Supported
7.8. REFER Call Transfer Test Cases				
7.8.1. Attended Call Transfer Test Cases				
TC62 IP-PBX calls PSTN attended transfer to IP-PBX	Supported		Supported	
TC63 IP-PBX calls PSTN attended transfer to PSTN	Supported		Supported	
TC64 PSTN calls IP-PBX attended transfer to IP-PBX	Supported		Supported	
TC65 PSTN calls IP-PBX attended transfer to PSTN	Supported		Supported	
7.8.2. Semi-Attended Call Transfer Test Cases				
TC66 IP-PBX calls PSTN semi-attended transfer to IP-PBX	Supported		Supported	
TC67 IP-PBX calls PSTN semi-attended transfer to PSTN	Supported		Supported	
TC68 PSTN calls IP-PBX semi-attended transfer to IP-PBX	Supported		Supported	
TC69 PSTN calls IP-PBX semi-attended transfer to PSTN	Supported		Supported	
7.8.3. Blind Call Transfer Test Cases				
TC70 IP-PBX calls PSTN with blind transfer to IP-PBX	Supported		Supported	
TC71 IP-PBX calls PSTN with blind transfer to PSTN	Supported		Supported	
TC72 PSTN calls IP-PBX with blind transfer to IP-PBX	Supported		Supported	
TC73 PSTN calls IP-PBX with blind transfer to PSTN	Supported		Supported	
7.9. Conference Call Test Cases				
TC74	IP-PBX calls PSTN conference to IP-PBX	Supported		Supported
TC75	IP-PBX calls PSTN conference to PSTN	Supported		Supported

TC76	PSTN calls IP-PBX conference to IP-PBX	Supported	Supported
TC77	PSTN calls IP-PBX conference to PSTN	Supported	Supported
7.10. CPE Failover Behavior Test Cases (Optional)			
TC78	OPTIONS method – request and response	Supported	Supported
TC79	Round – Robin (load share 50/50 between the two CPEs)	Supported	Supported
TC80	Primary/Secondary Failover (Hunt)	Supported	Supported
TC81	Both CPE Fail	Supported	Supported

Phase I – Configure the Lync Server

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

1. Adding the Net-Net SD as a PSTN gateway to the Lync Server infrastructure; and
2. Creating a route within the Lync Server infrastructure to utilize the SIP trunk connected to the Net-Net SD.

1.7. 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.

1.8. Adding the PSTN Gateway

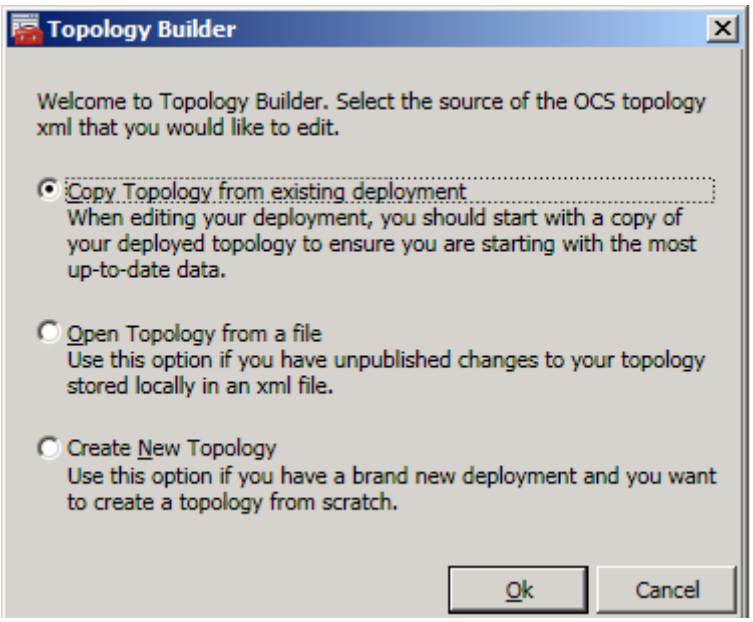
What you will need:

- 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

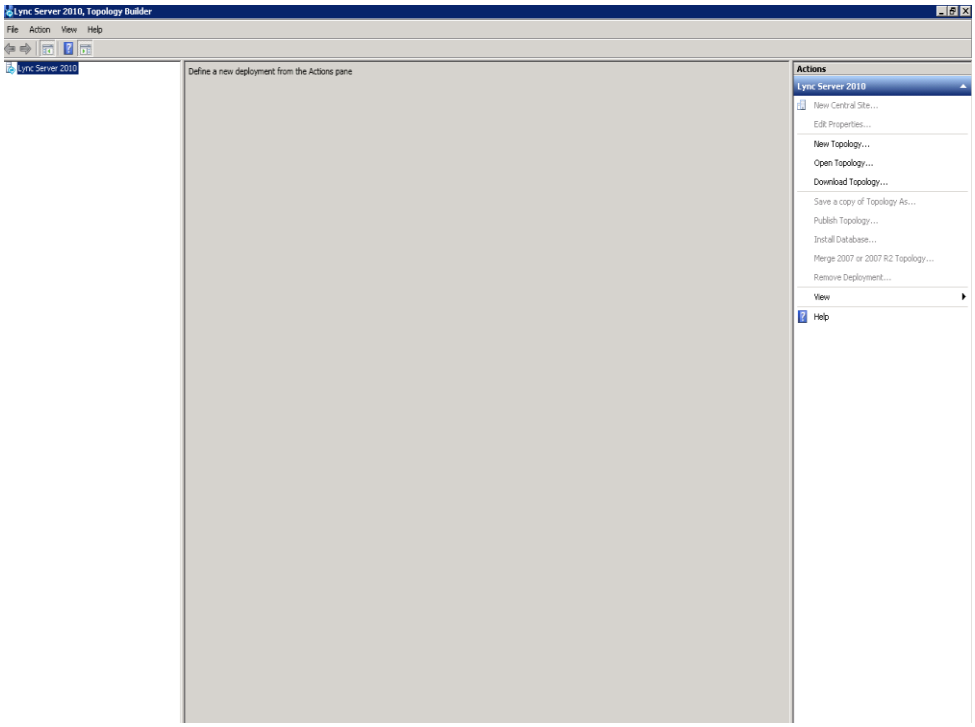
Steps to add the PSTN gateway

1. On the server where the Topology Builder is located start the console.
2. Click **Start**, select **All Programs**, then select **Communications Server Topology Builder**

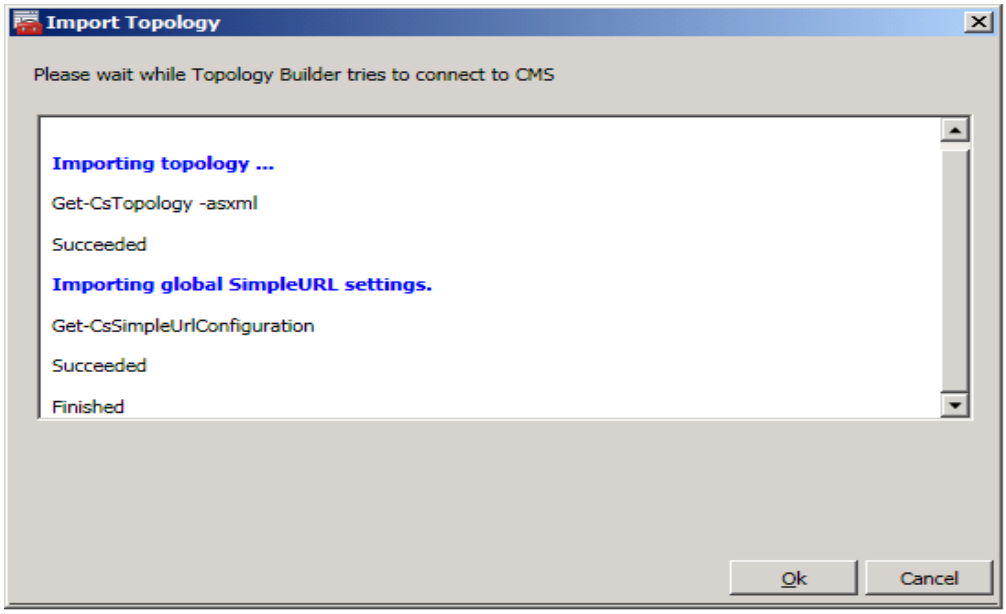
You will now be at the opening screen in the Topology Builder.



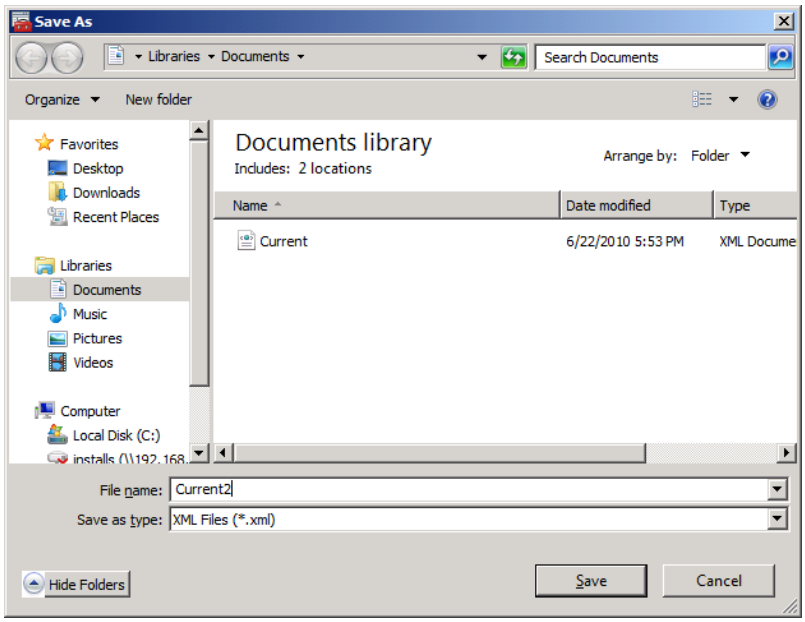
3. Click on the **Cancel** button.



4. In the upper right hand corner of the Topology Builder select **Import Topology**.



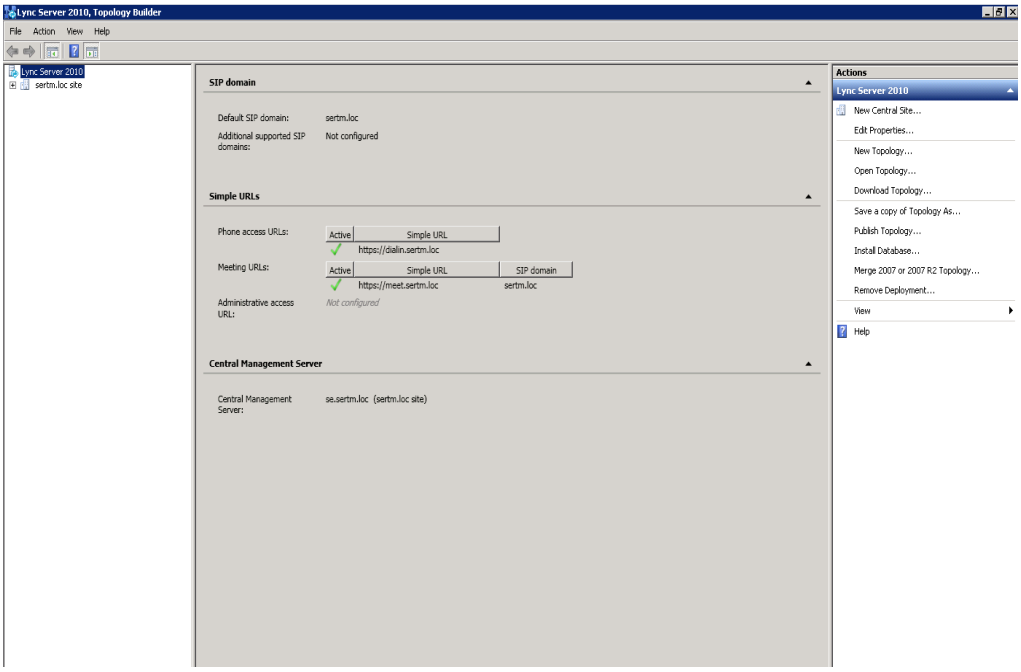
5. You will then see a screen showing that you have successfully imported the topology. Click the **Ok** button.



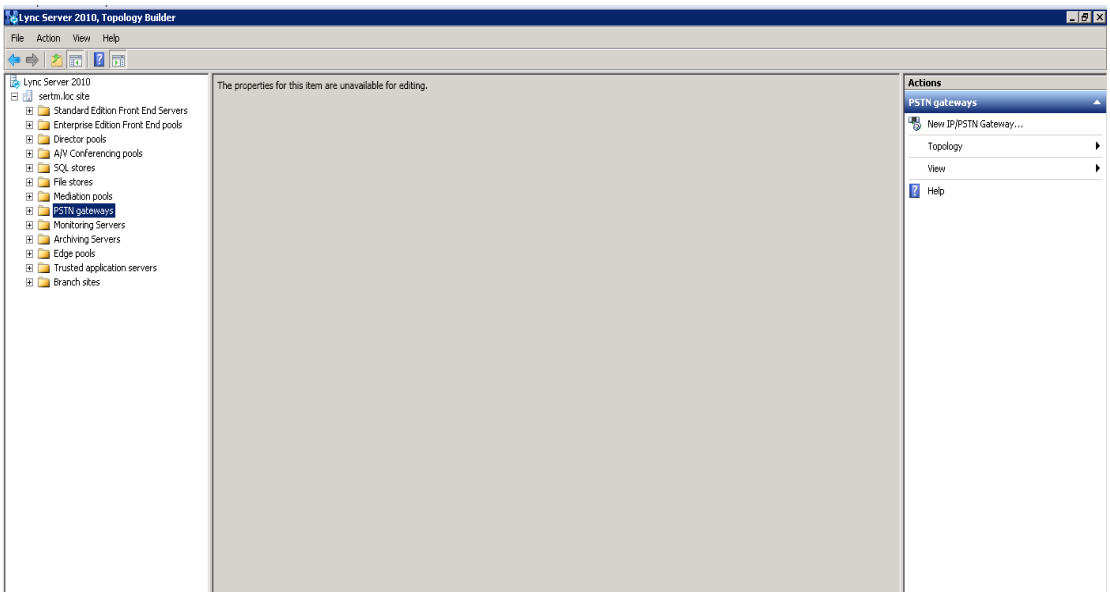
6. Next you will be prompted to save the topology which you have imported.
7. You should revision the name or number of the topology according to the standards used within the enterprise.

   Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make during this installation.
8. Click the **Save** button.

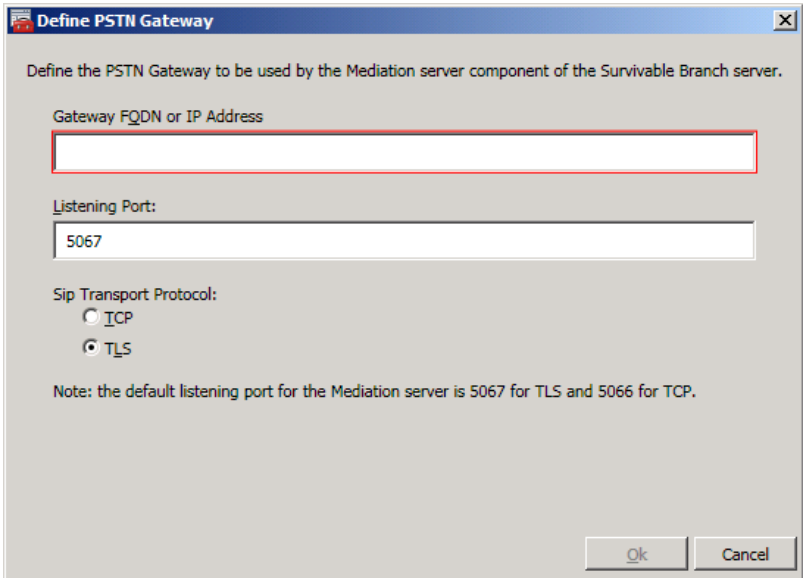
You will now see the topology builder screen with the enterprise's topology imported.



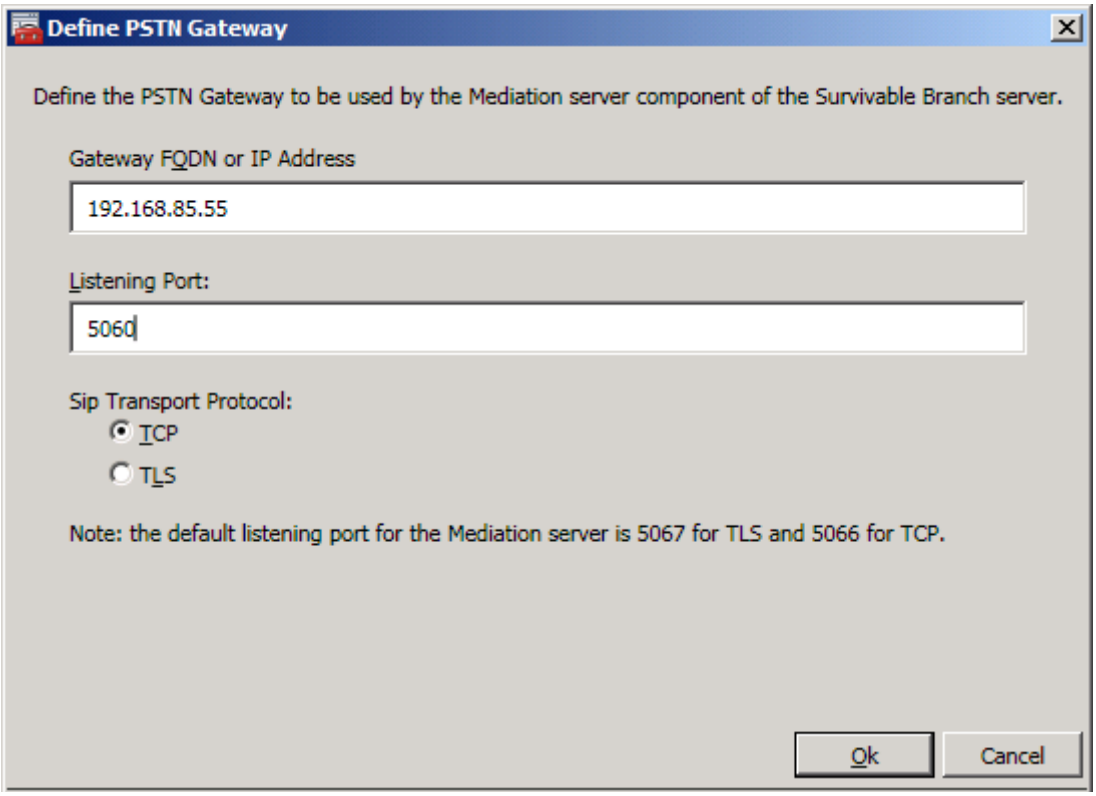
9. In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is **Test**. Then click on the **PSTN Gateways**.



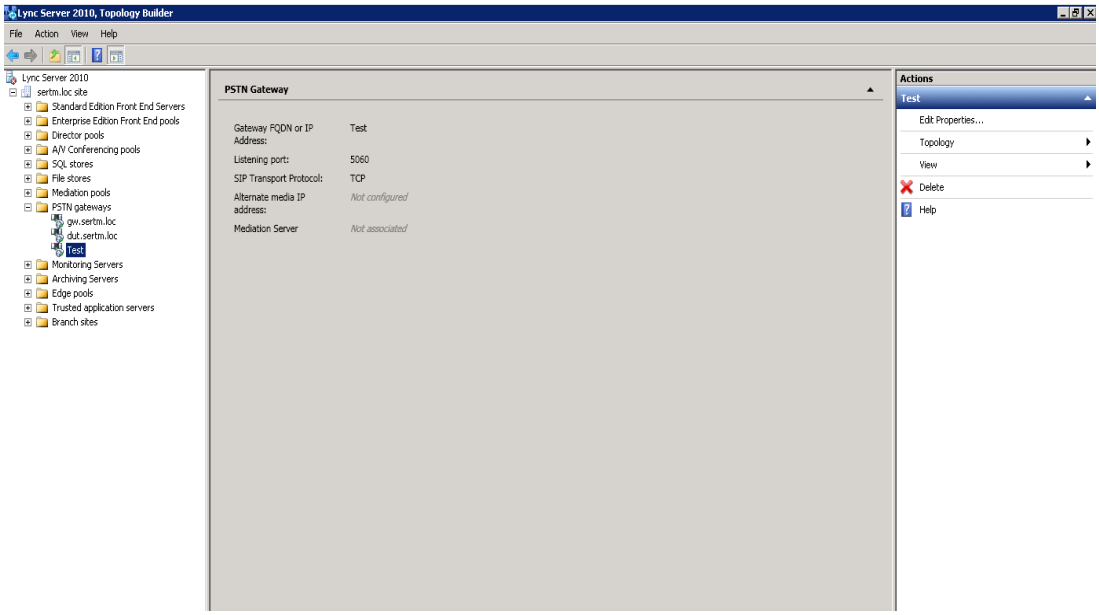
10. Right click on **PSTN Gateways** and select **New PSTN Gateway**.



11. 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**.
12. Enter the **Listening Port**. In our example the listening port is **5060**.
13. Select the **"Sip Transport Protocol**". In our example it is **TCP**. Select this radio button and click **Ok**.

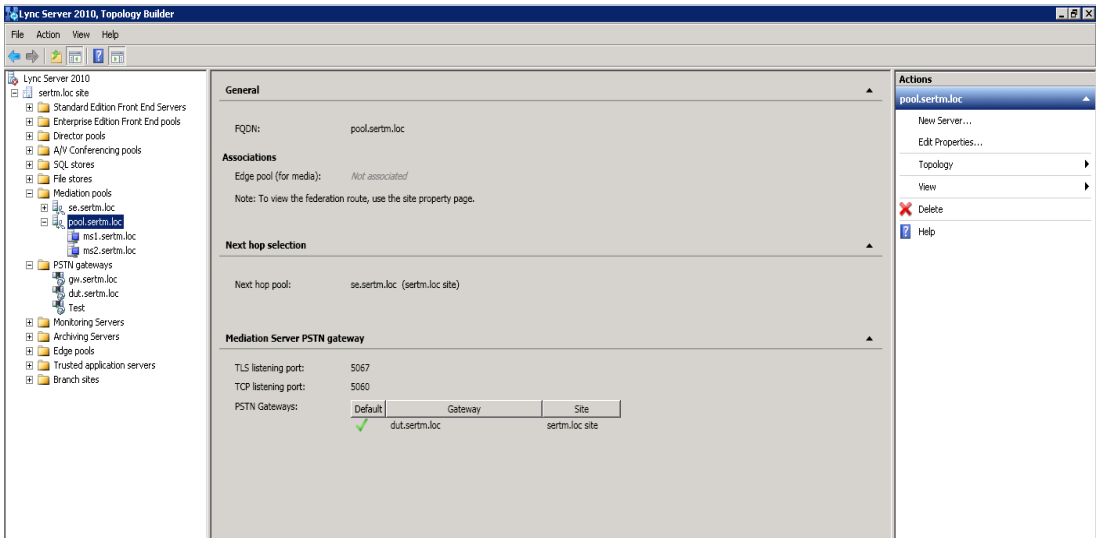


The PSTN Gateway for Lync Server, which is the outbound side of the Net-Net SD has now been added.



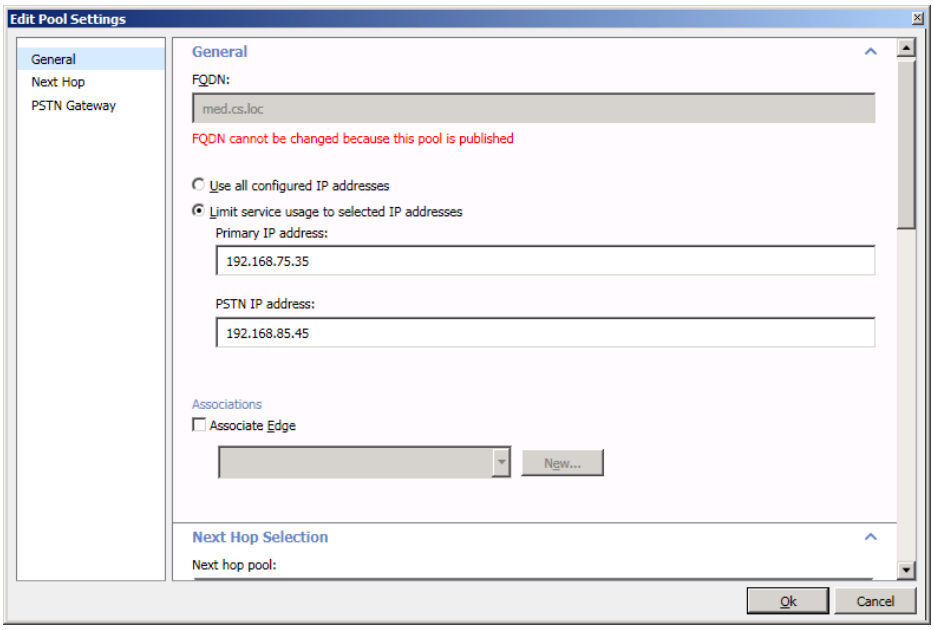
Next we will add the newly created PSTN gateway entry to the Mediation Server.

14. Expand the **Mediation Severs** list and click on the Mediation Server to be utilized. In our example the Mediation Server is **med.cs.loc**.

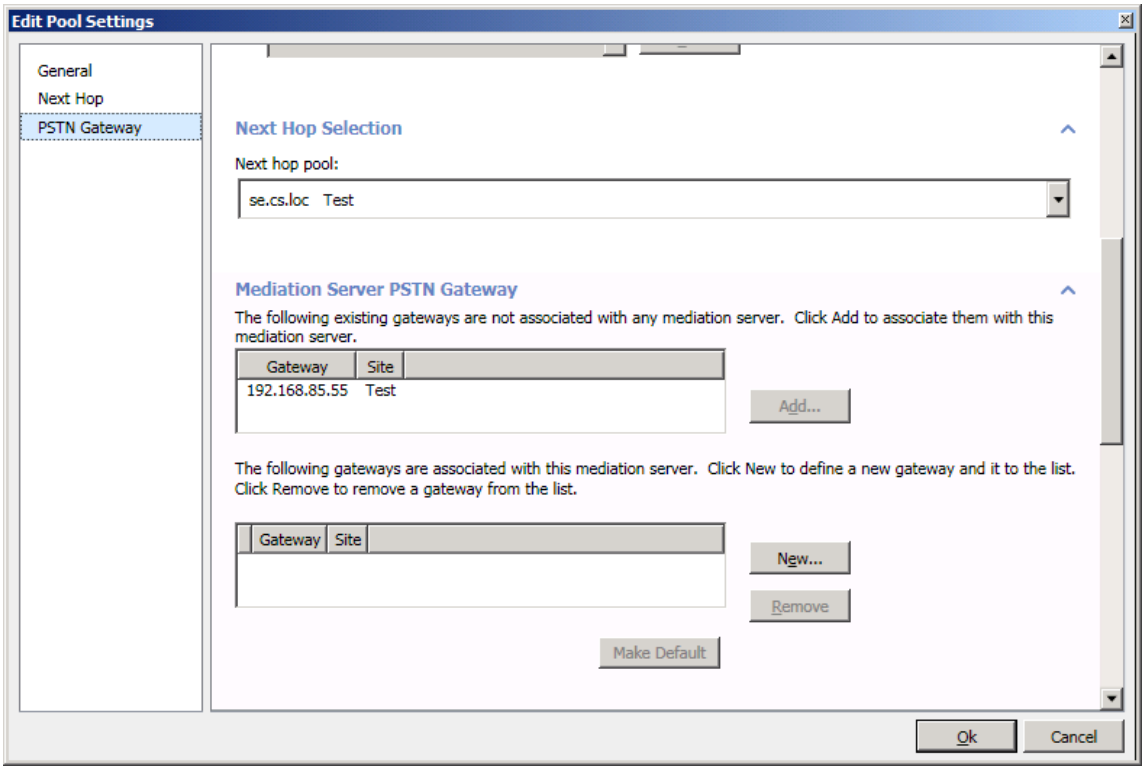


Note that in the right hand pane at the bottom, there is no PSTN gateway associated with the Mediation Server. We will do this now.

15. Right click on the Mediation Server and select **Edit Properties**.

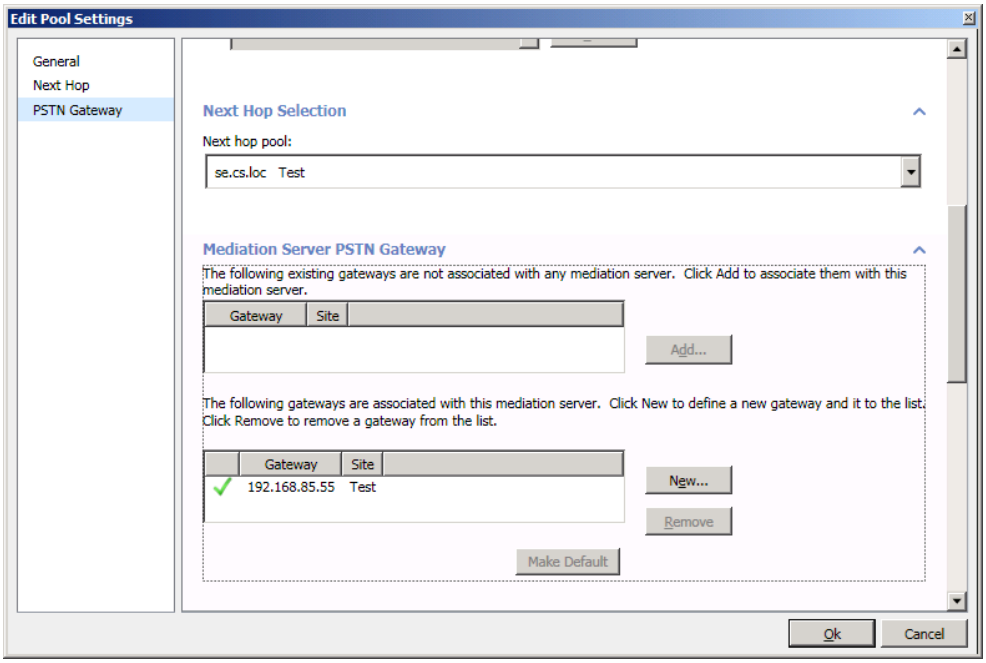


16. In the upper left corner of the window select **PSTN Gateway**.



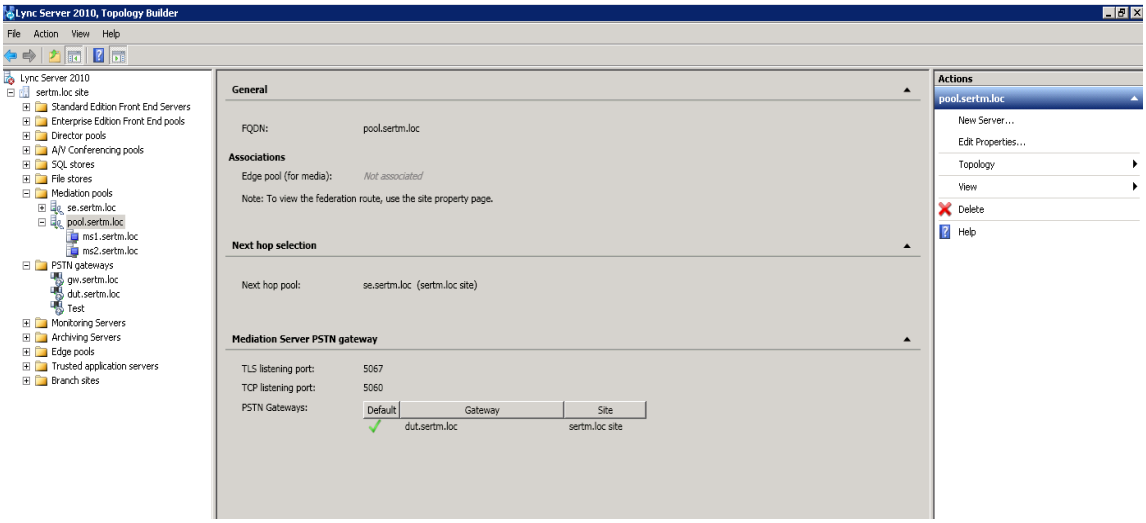
Notice that the PSTN gateway that you just added is not associated with any Mediation Server.

17. Click on the **PSTN Gateway** and then click on the **Add** button.



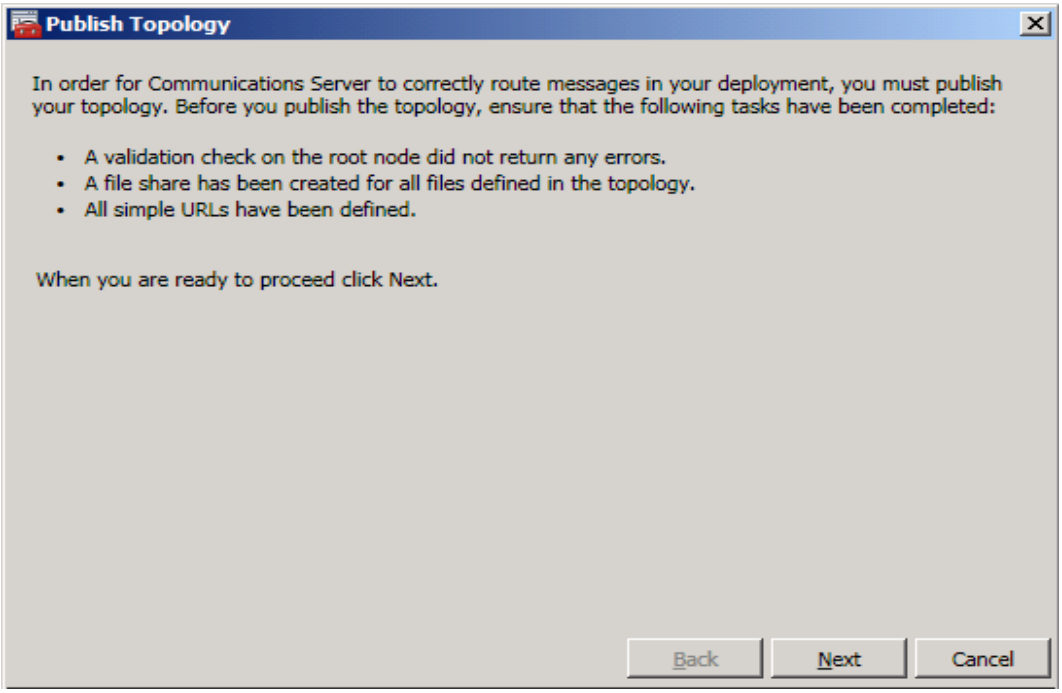
You will now see the PSTN Gateway that you added earlier.

18. Click the **OK** button.

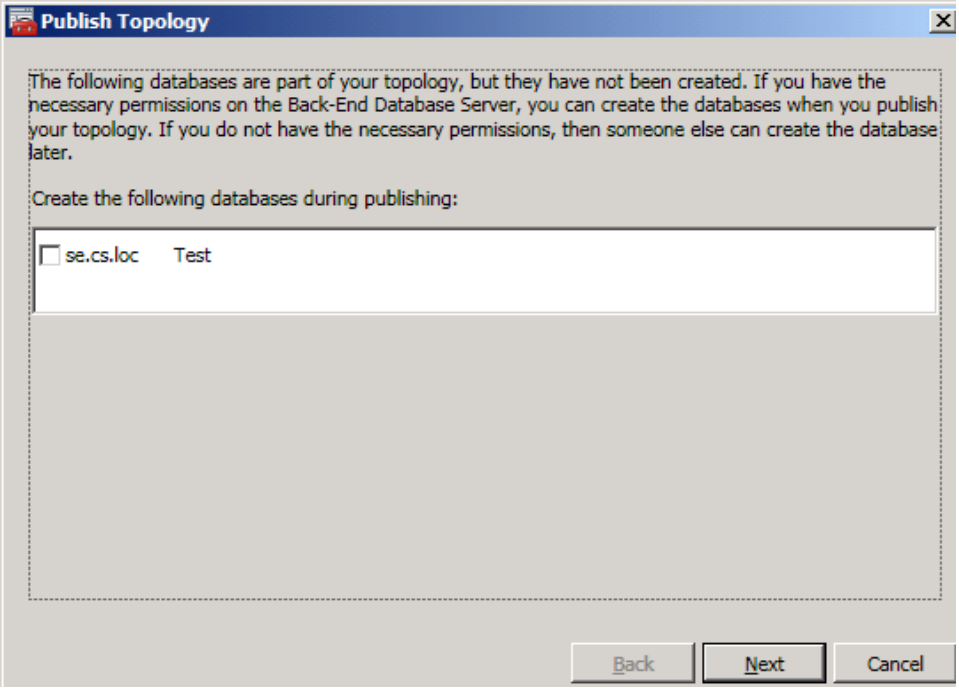


You will now be back at the Topology Builder screen and you can now see that your PSTN Gateway is associated with the Mediation Server

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

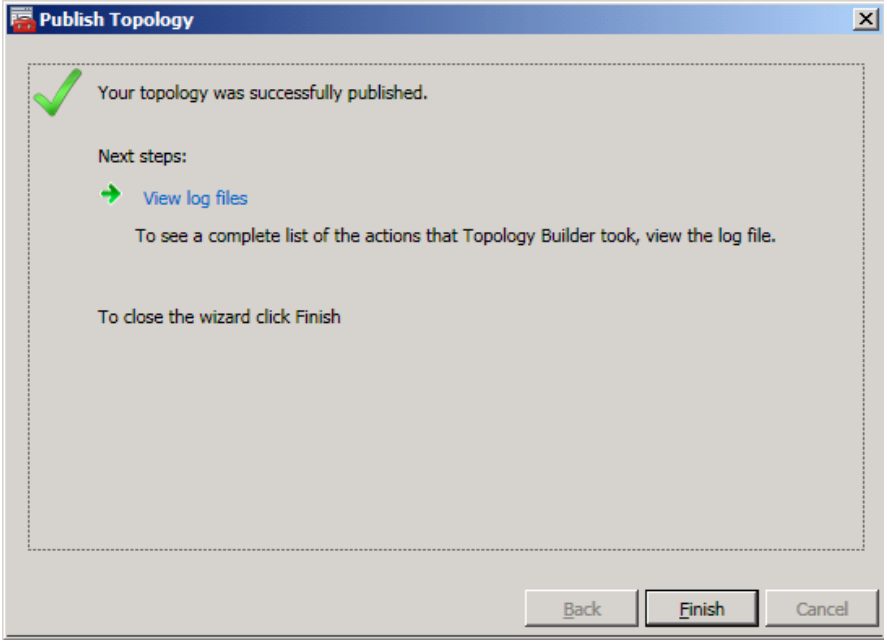


You will now be at a window showing the databases associated with site



21. Do not check any of the boxes - leave them as were when the window opened and click **Next**.

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



22. Click the **Finish** button.
23. 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.

1.9. 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 a Lync Server Enterprise Voice deployments such as dial plans, voice policies, and PSTN usages are not covered.

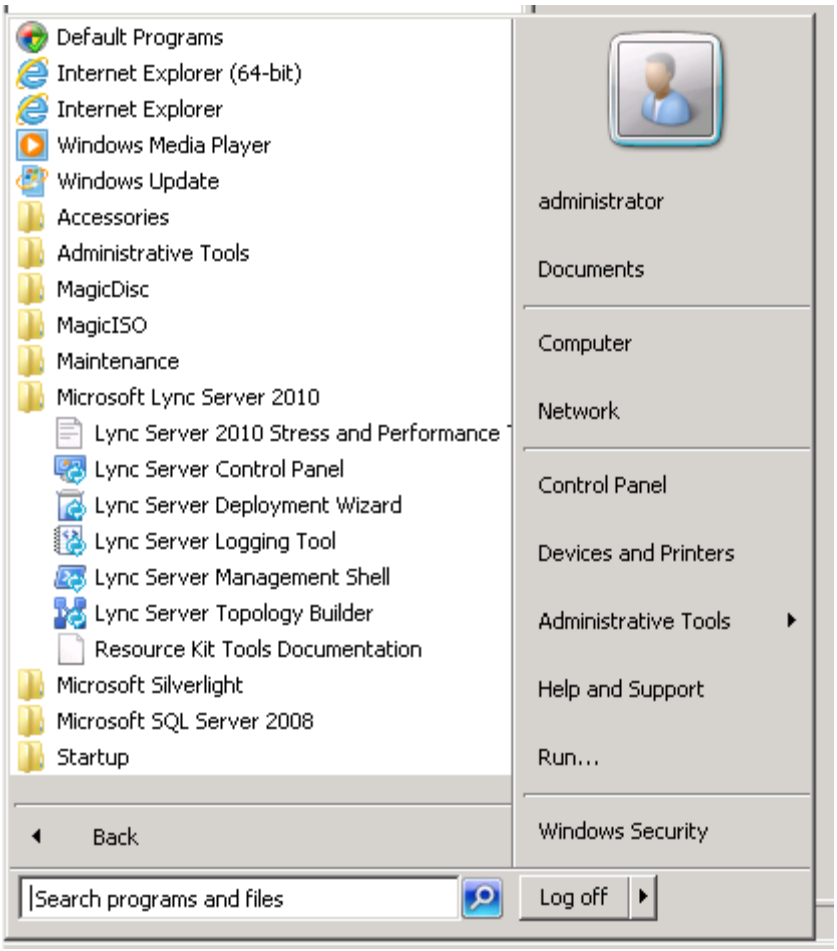
What you will need:

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

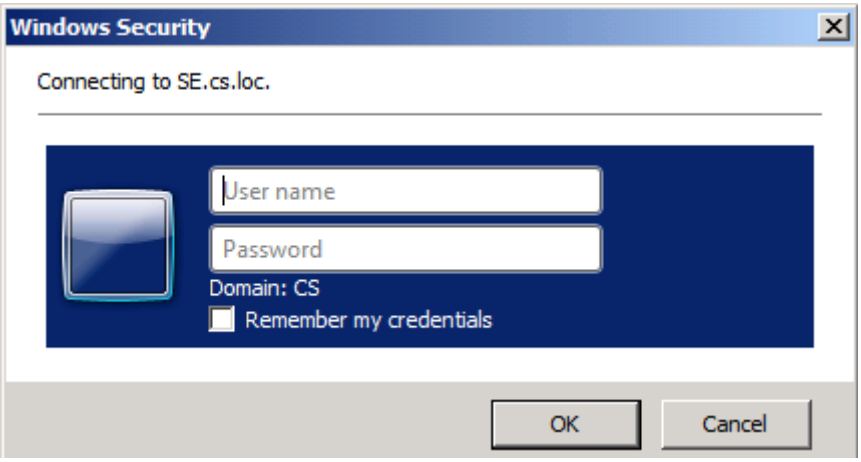
Steps to add the Lync Server Route

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

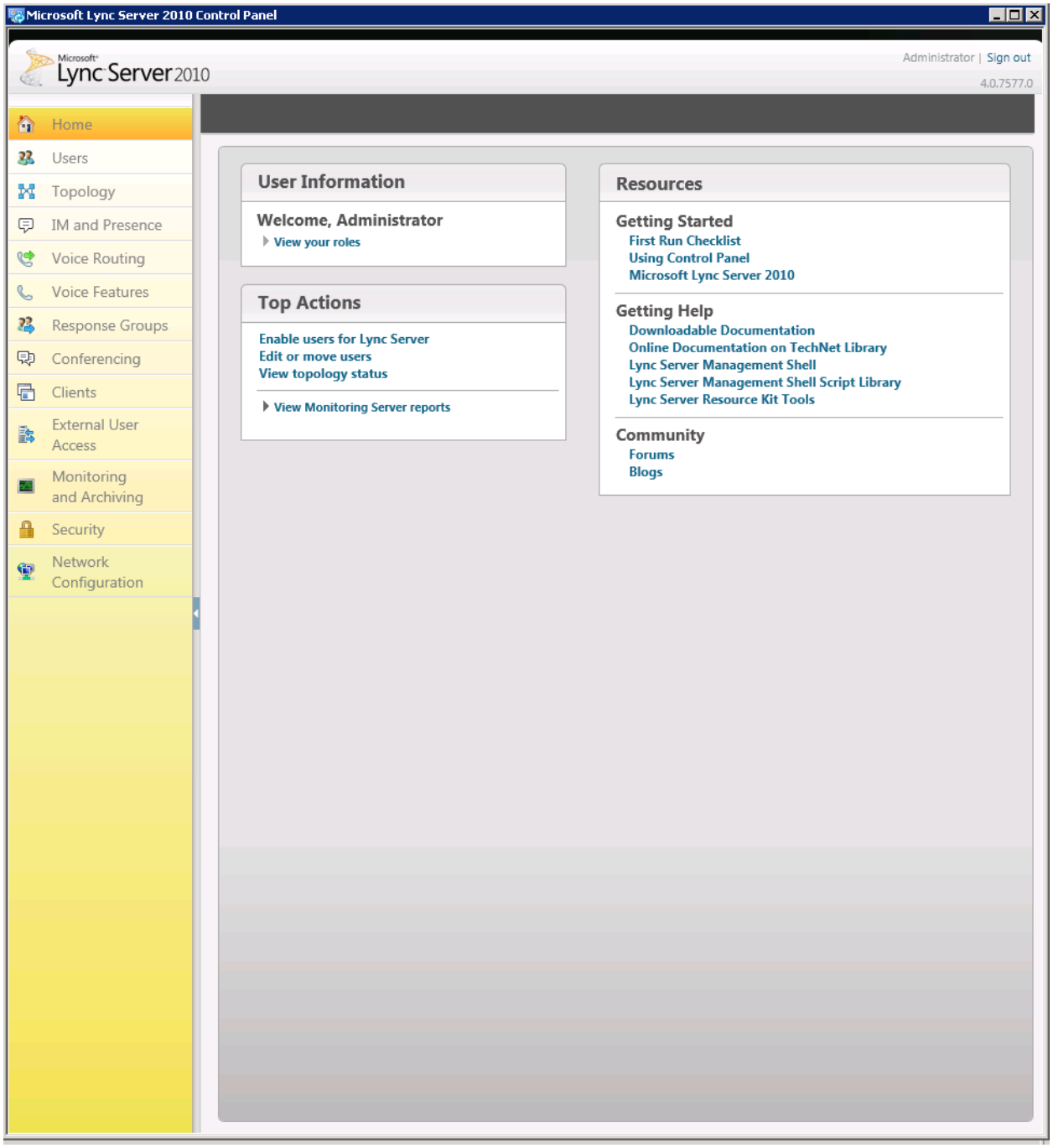
1. Click **Start**, select **All Programs**, then select **Communications Server Control Panel**



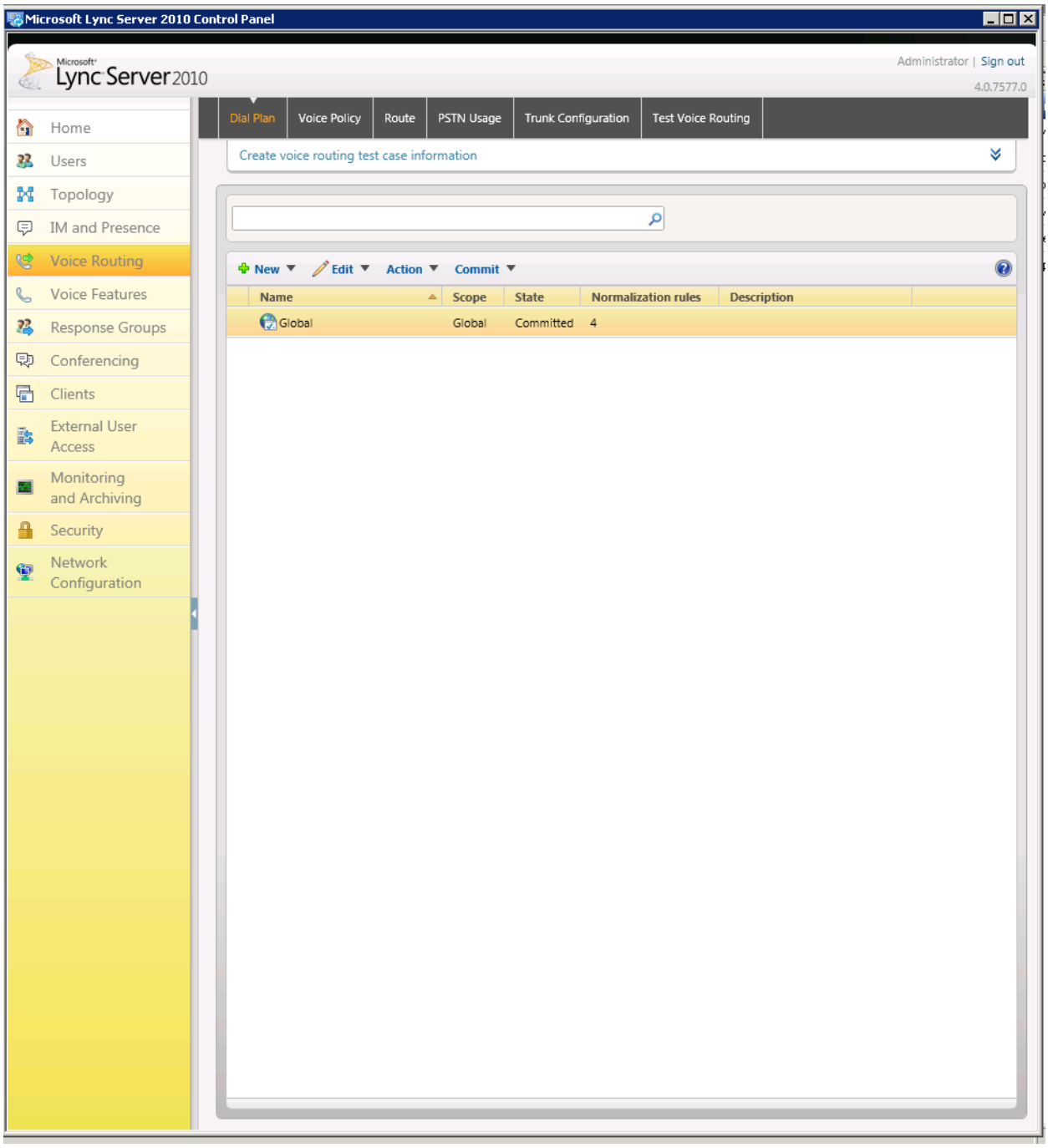
You will be prompted for credentials enter your domain username and password.



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



3. On the top row of tabs select **Dial Plan**.



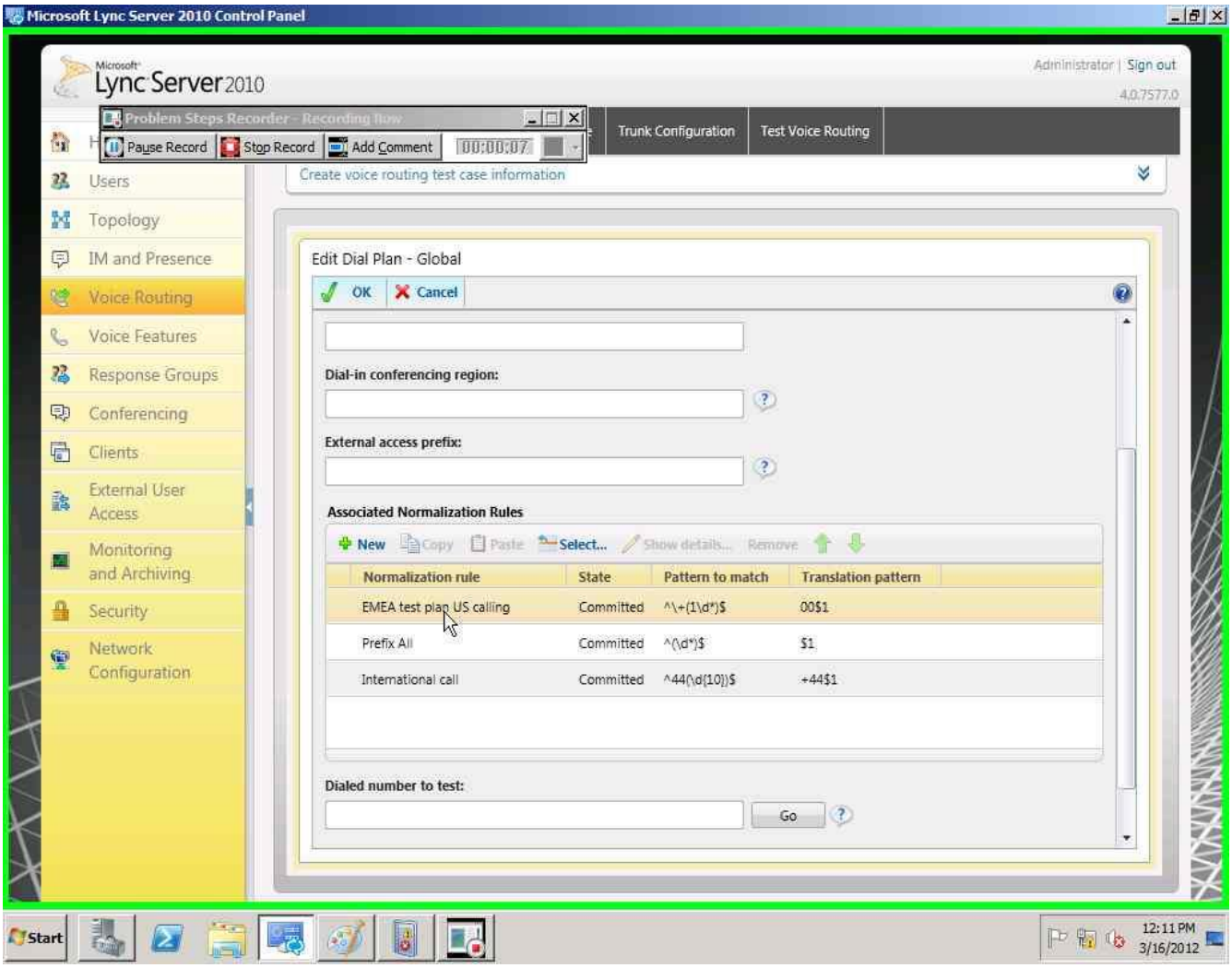
4. On the content area toolbar, click **+New**.
5. Next you build a Dial Plan and a translation rule for the phone numbers you want this route to handle. You have to create two separate dial plans for US and EMEA.

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

   International call Dial-plan
   Match this pattern: ^44(\d{10})$

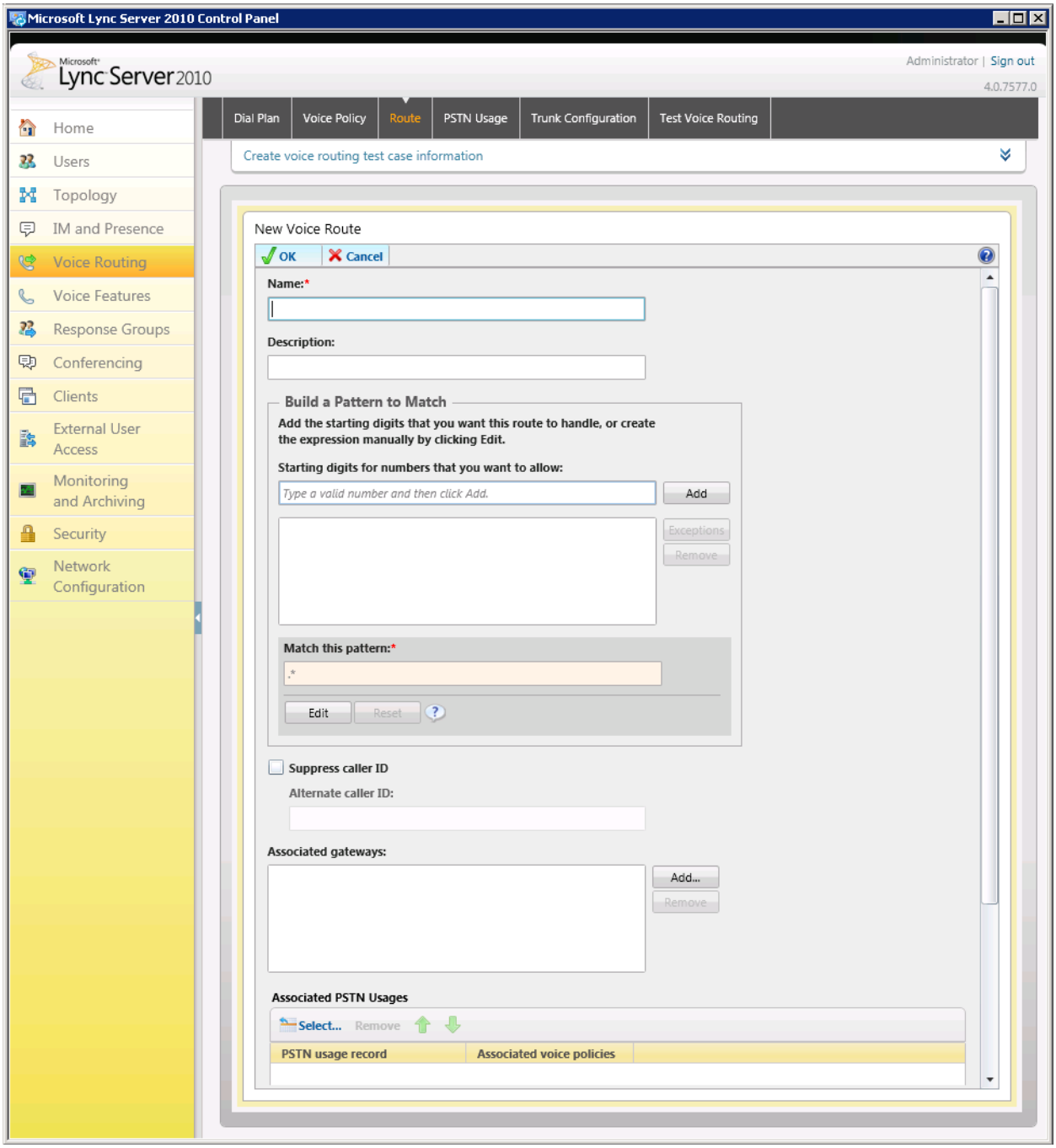
Translation rule: +44$1

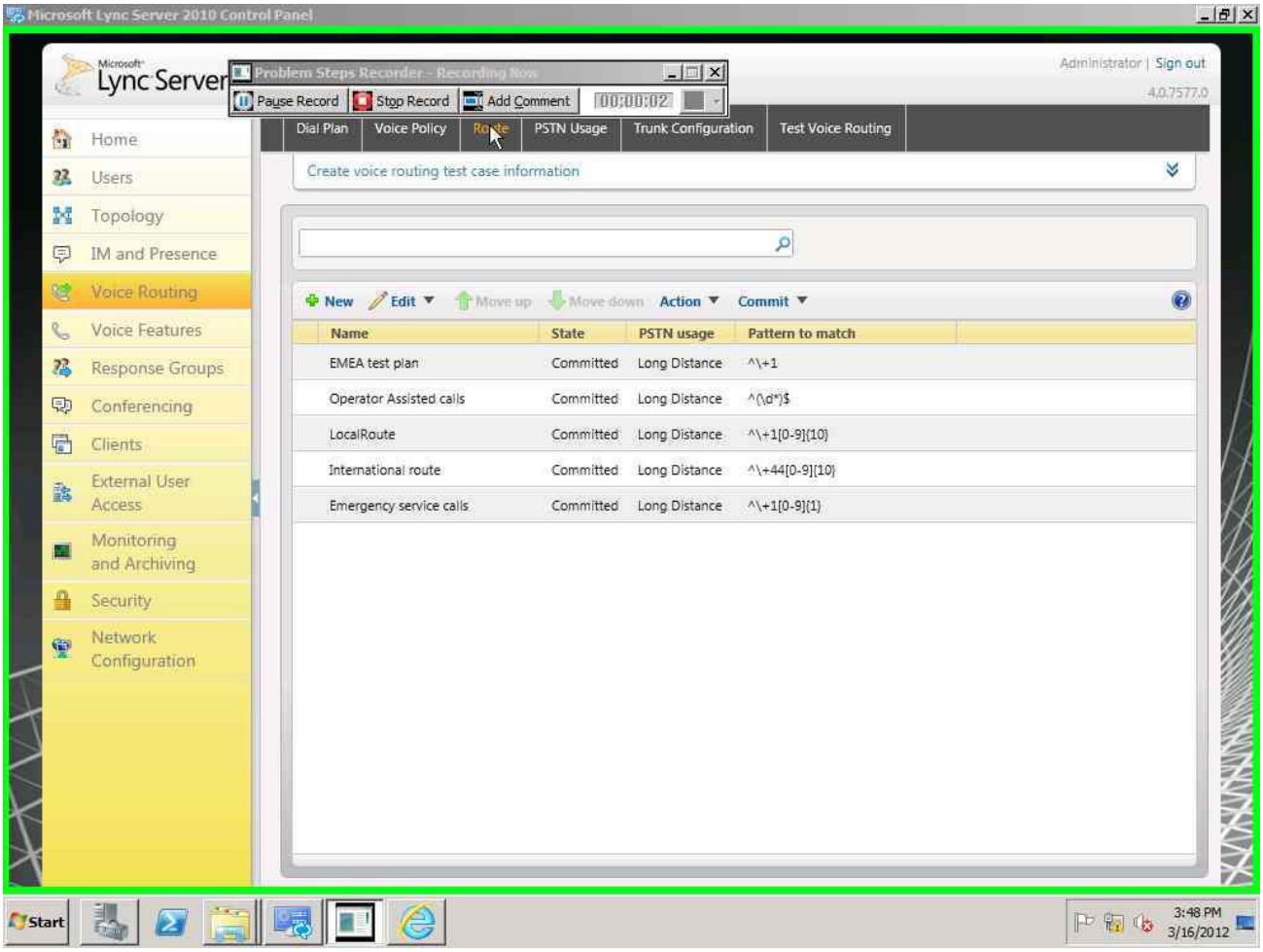
EMEA dial plan
Match this pattern: ^\+(1\d*)$
Translation rule: 00$1



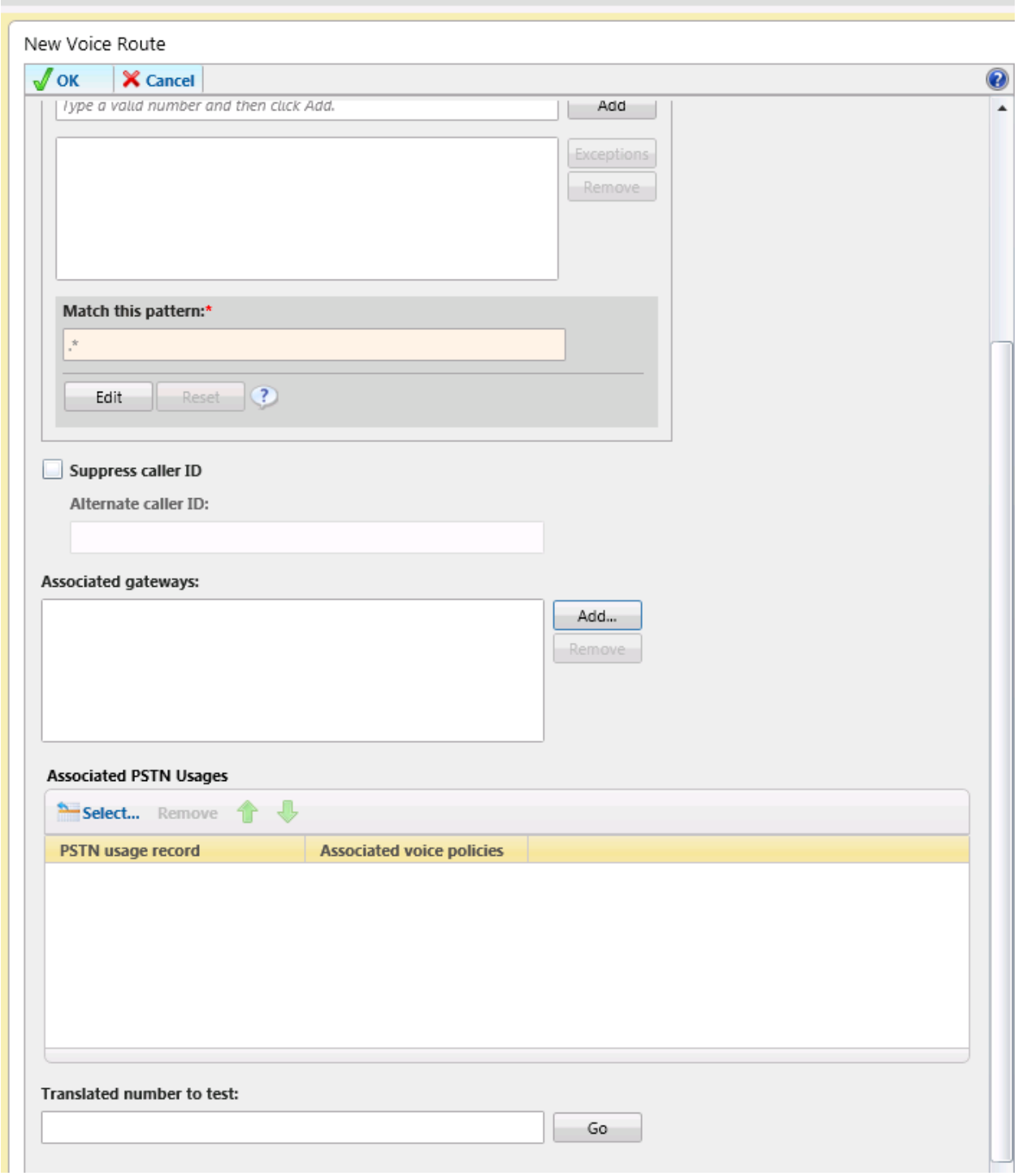
6. On the Create Voice Route page, in the Name field, enter the name you have selected for the Route. In our example, it is Test.

   The Voice Route for US would be to match this pattern: ^(\+1[0-9]{10})$
   The Voice Route for EMEA would be to match this pattern: ^(\+44[0-9]{10})$

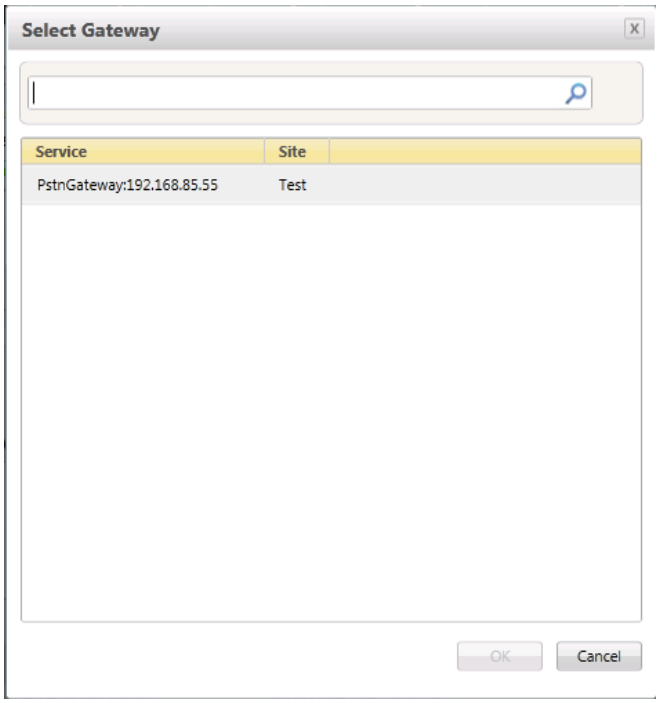

Microsoft Lync Server 2010 Control Panel
Microsoft Lync Server 2010
Administrator | Sign out
4.0.7577.0
Home
Users
Topology
IM and Presence
Voice Routing
Voice Features
Response Groups
Conferencing
Clients
External User Access
Monitoring and Archiving
Security
Network Configuration
Dial Plan
Voice Policy
Route
PSTN Usage
Trunk Configuration
Test Voice Routing
Create voice routing test case information
New Voice Route
OK
Cancel
Name:*
Description:
Build a Pattern to Match
Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.
Starting digits for numbers that you want to allow:
Type a valid number and then click Add.
Add
Exceptions
Remove
Match this pattern:*
.*
Edit
Reset
Suppress caller ID
Alternate caller ID:
Associated gateways:
Add...
Remove
Associated PSTN Usages
Select...
Remove
PSTN usage record
Associated voice policies


Microsoft Lync Server 2010 Control Panel
Problem Steps Recorder - Recording Now
Pause Record
Stop Record
Add Comment
00:00:02
Administrator | Sign out
4.0.7577.0
Lync Server
Home
Users
Topology
IM and Presence
Voice Routing
Voice Features
Response Groups
Conferencing
Clients
External User Access
Monitoring and Archiving
Security
Network Configuration
Dial Plan
Voice Policy
Route
PSTN Usage
Trunk Configuration
Test Voice Routing
Create voice routing test case information
New
Edit
Move up
Move down
Action
Commit
Name
State
PSTN usage
Pattern to match
EMEA test plan
Committed
Long Distance
^\+1
Operator Assisted calls
Committed
Long Distance
^(\d*)$
LocalRoute
Committed
Long Distance
^\+1[0-9]{10}
International route
Committed
Long Distance
^\+44[0-9]{10}
Emergency service calls
Committed
Long Distance
^\+1[0-9]{1}
Start
3:48 PM
3/16/2012

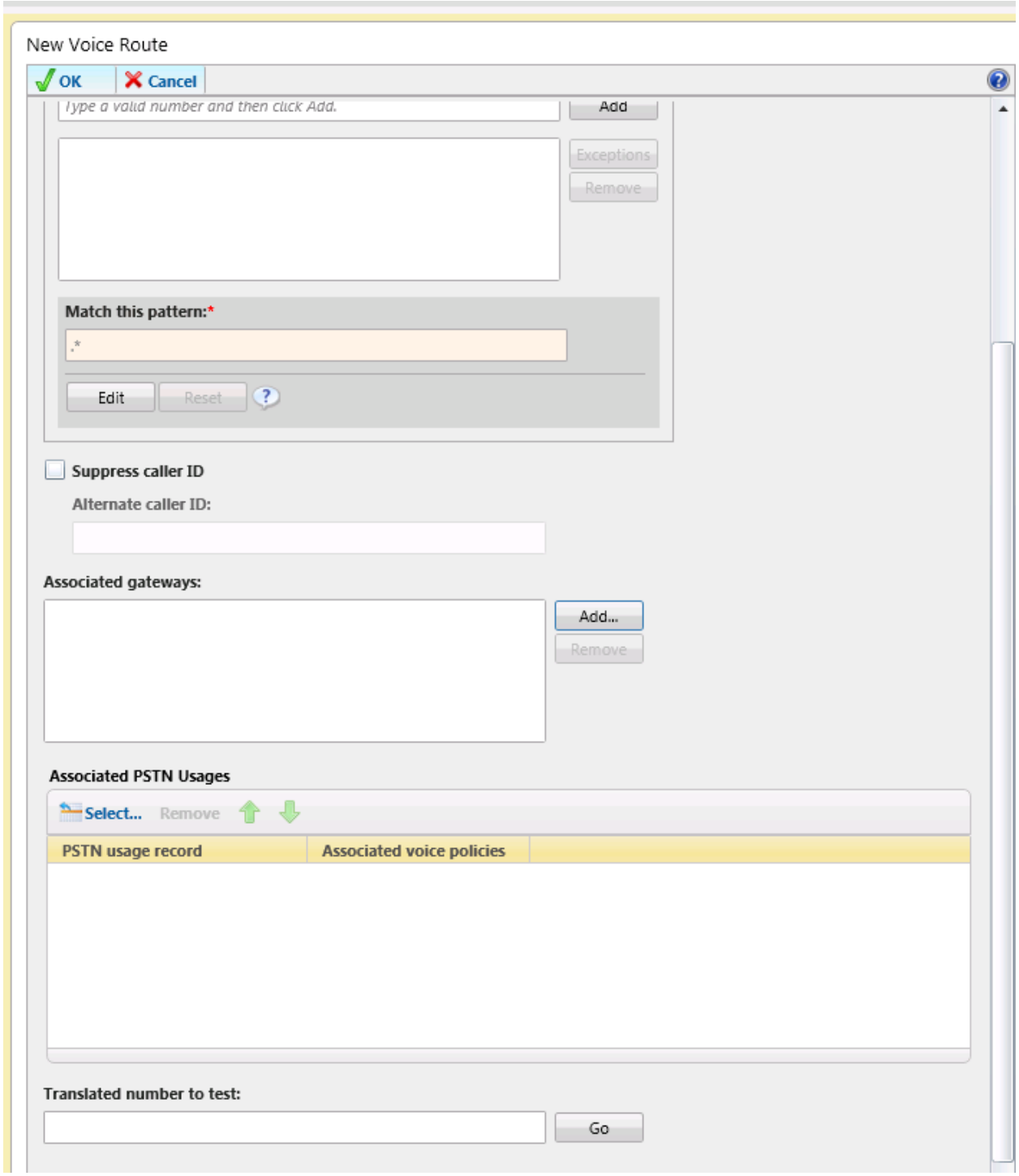
7.Next you want to associate the Voice Route with the PSTN gateway you have just created scroll down to Associated Gateways, click on the **Add** button.



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



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

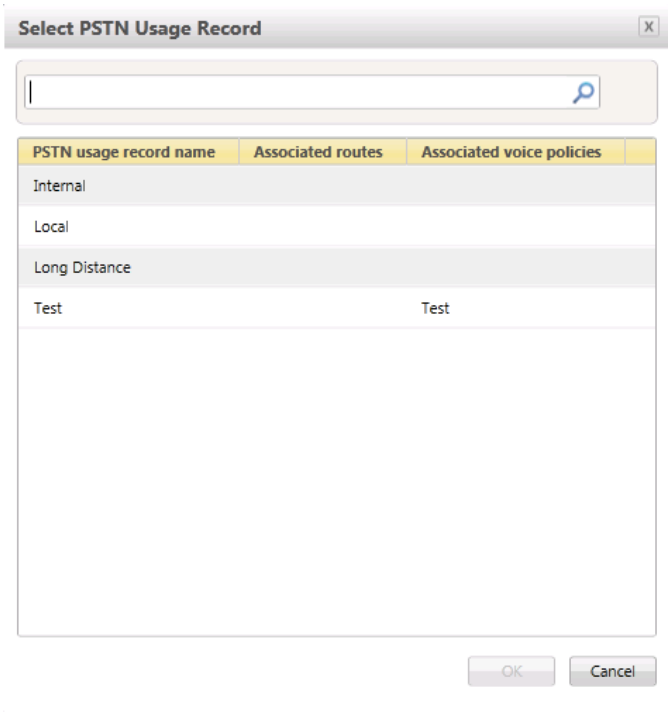


You can now see that you have associated your PSTN gateway with the route you created.

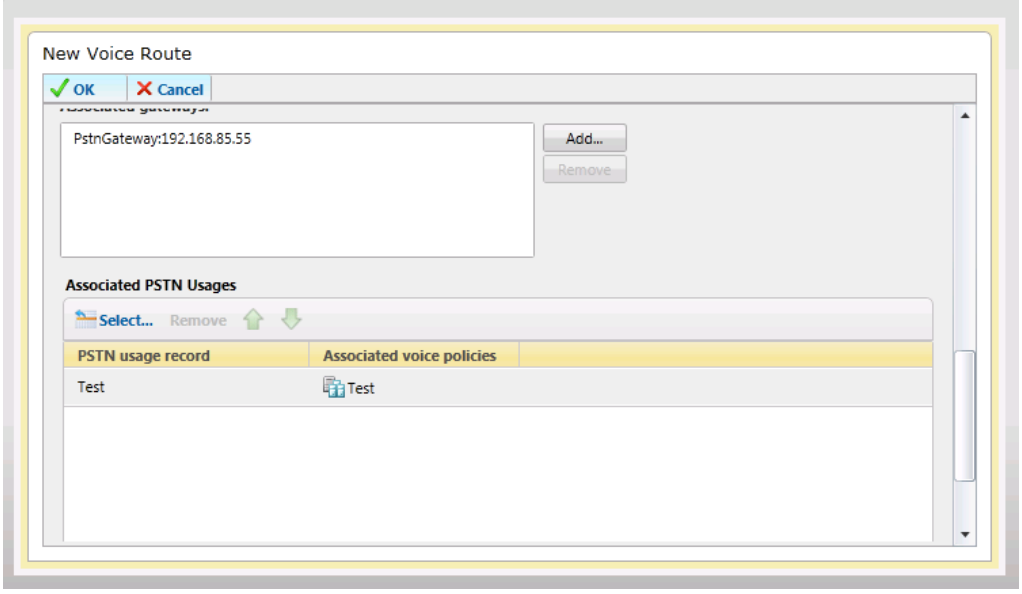
Note that the **Suppress Caller ID**: allows the manipulation of caller ID information for outbound calls, in order to mask employees' direct-dial extensions and replace them with the generic corporate or departmental numbers, this is not a necessary step for this installation, but may need to be addressed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

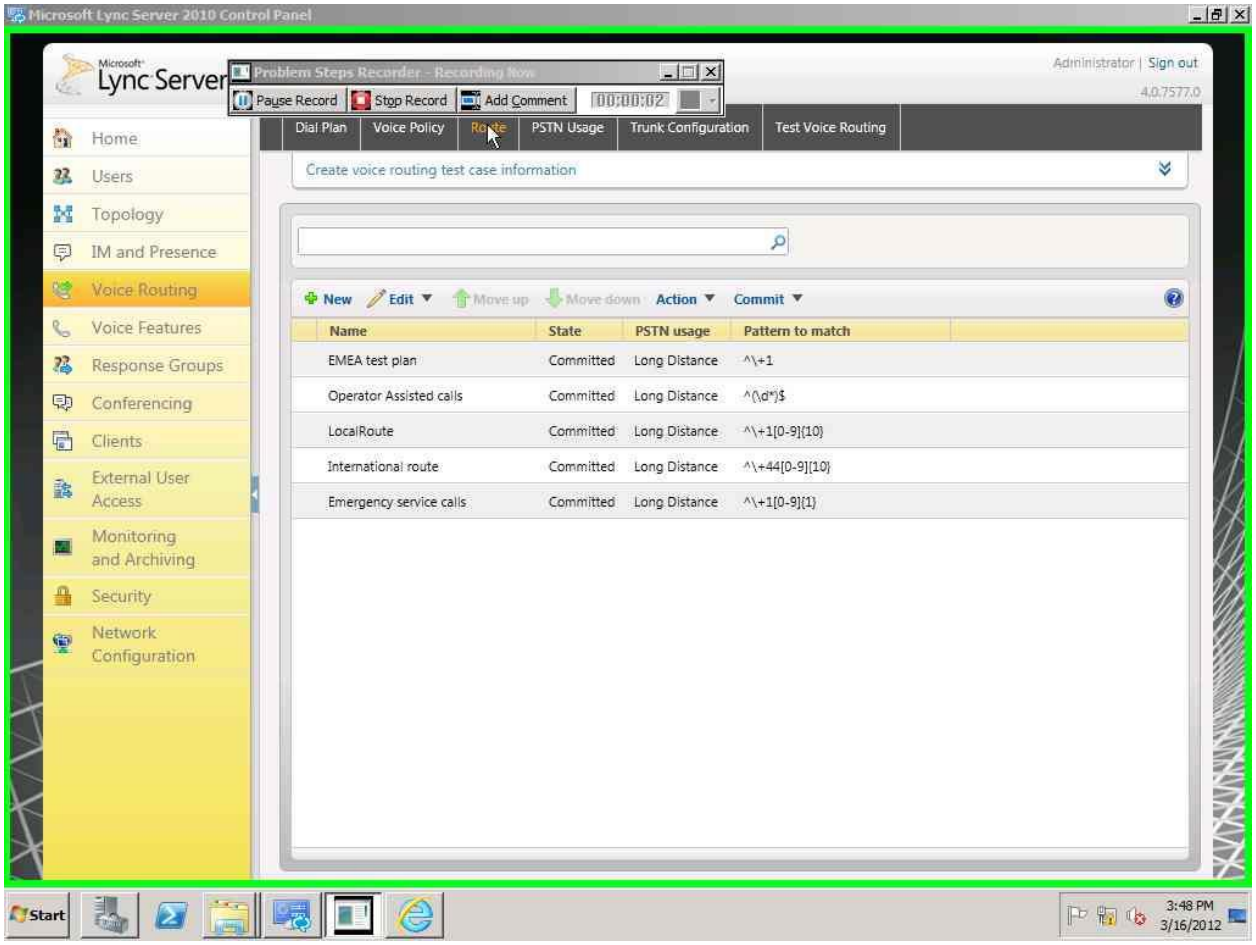
8. Click on the **Select** button under “Associated PSTN Usages”.



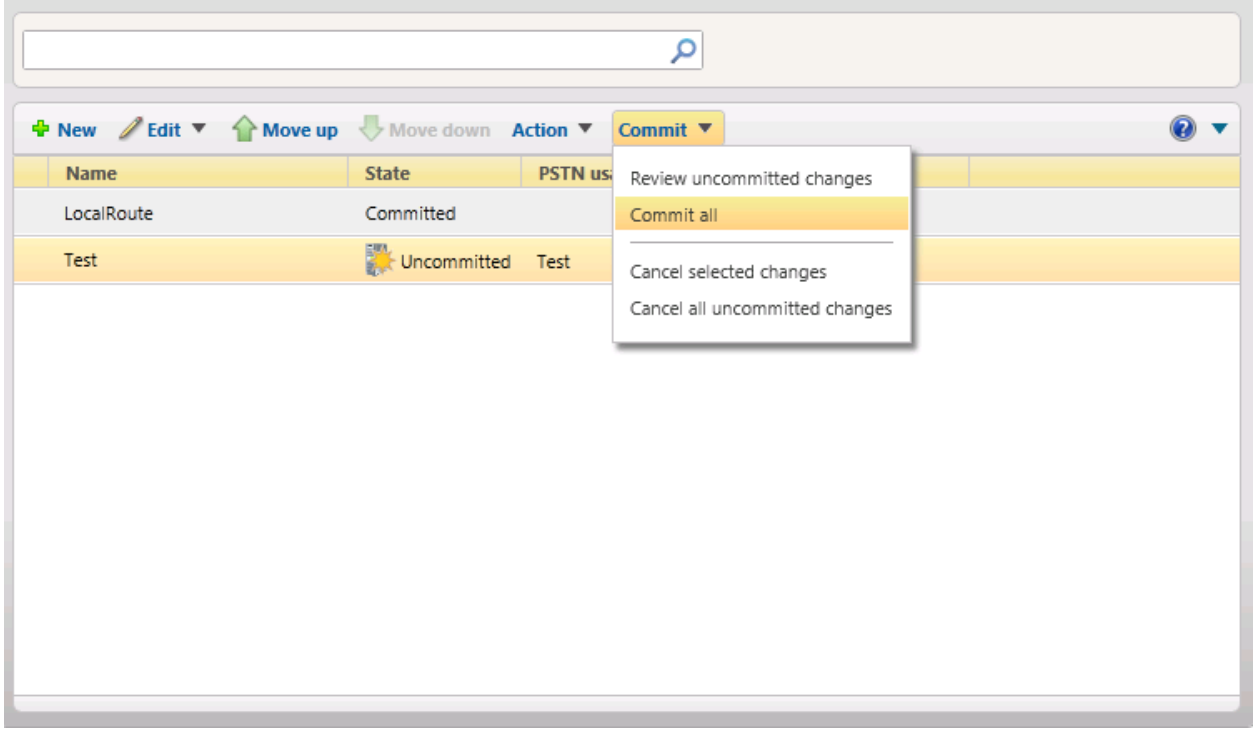
9. Select the appropriate PSTN Usage Record then click the **OK** button.



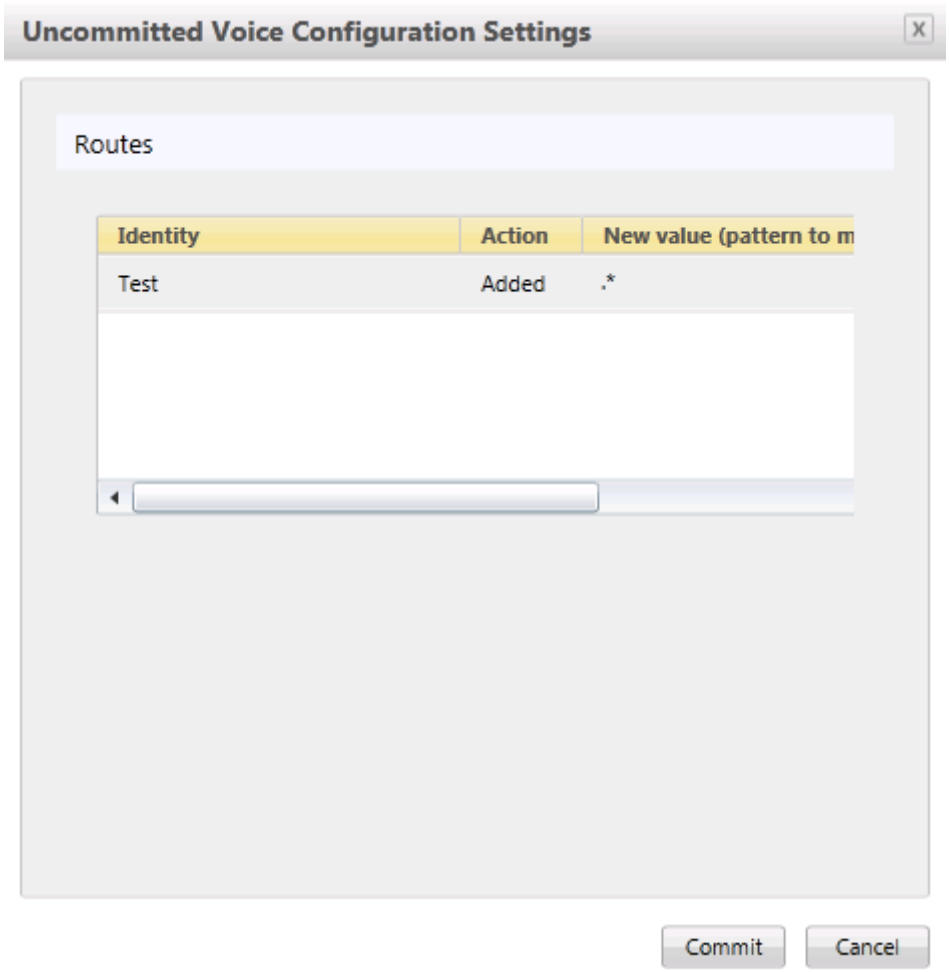
10. You will now see the Associated PSTN Gateway Usages which you have added. Click the **OK** button at the top New Voice Route screen.



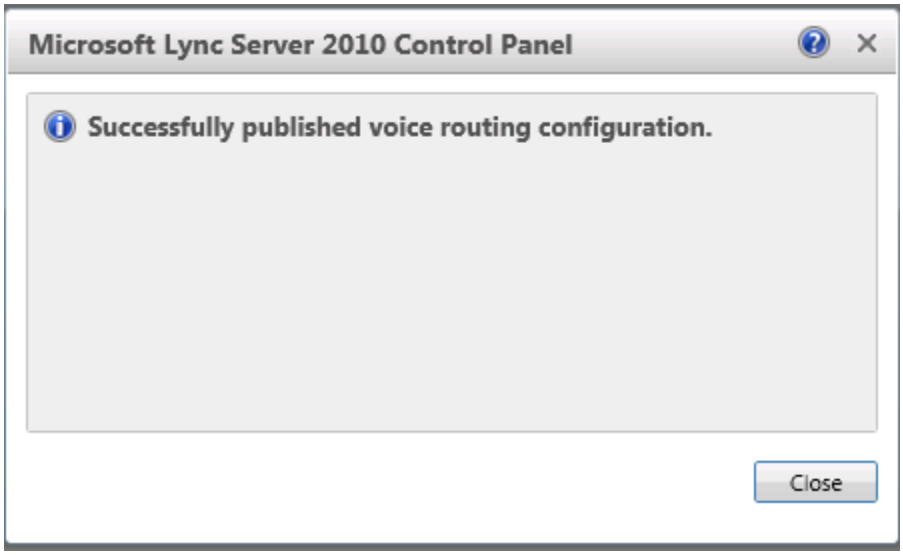
11. Click the **Commit** drop-down menu, and then **Commit All**.



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



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



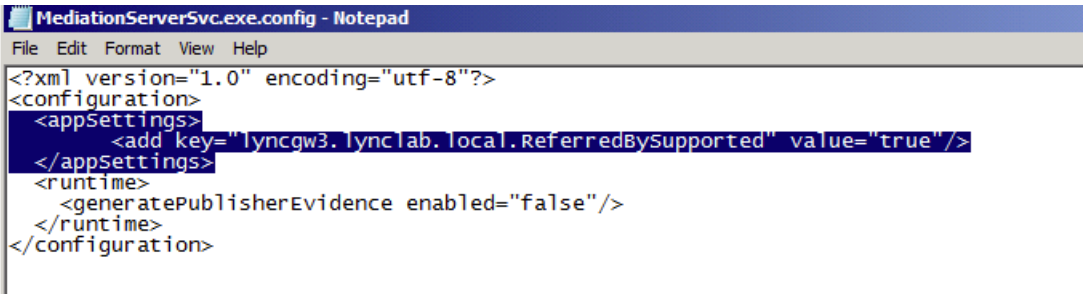
14. If there are no errors, the new Voice Route has now been successfully created and the State will show as Committed.

1.10. Additional Steps

When using a SIP trunk provider, like Verizon, Lync users may encounter problems enabling Call Transferring. By default, when transferring calls, Lync will only send the SIP FROM header which includes the originating CLID. If that CLID is not considered an on-net station for the SIP trunk, the carrier will reject the call, considering it to be unauthorized to use the trunk. This issue can be overcome through the use of a SIP REFERRED-BY header.

There is a fix which we need to implement in the mediation server which causes it to send the "Referred-by" header. This fix is based on http://support.microsoft.com/kb/2500421. Lync must be patched up to CU4 before attempting to implement this fix.

The fix is made by modifying the mediation server config file located in "C:\Program Files\Microsoft Lync Server 2010\Mediation Server". Open the config file in notepad, and add the highlighted text below (replacing lyncgw3.lynclab.local with the FQDN of your mediation server/mediation server pool):



After making the modification to the config file, restart the Lync Mediation Service, and verify it started without errors. Lync will now start sending "Referred-by" header in call transfer cases.

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 Acme Packet SBC

In this section we describe the steps for configuring an Acme Packet SBC, formally known as an Acme Packet Net-Net Session Director ("Net-Net SD"), for use with Lync Server in a SIP trunking scenario.

1.11. In Scope

The following Step-by-Step guide configuring the Net-Net SD assumes that this is a newly deployed device dedicated to a single customer. If a service provider currently has the Net-Net SD deployed and is adding Lync Server customers, then please see the appendix for a better understanding of the Acme Packet Command Line Interface (ACLI).

Note that Acme Packet offers several models of SBC. This document covers the setup for the Net-Net 3820 and 4500 series running Net-Net OS SCX 6.2.0 or later. If instructions are needed for other Acme Packet Net-Net SBC models, please contact your Acme Packet representative.

1.12. Out of Scope

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

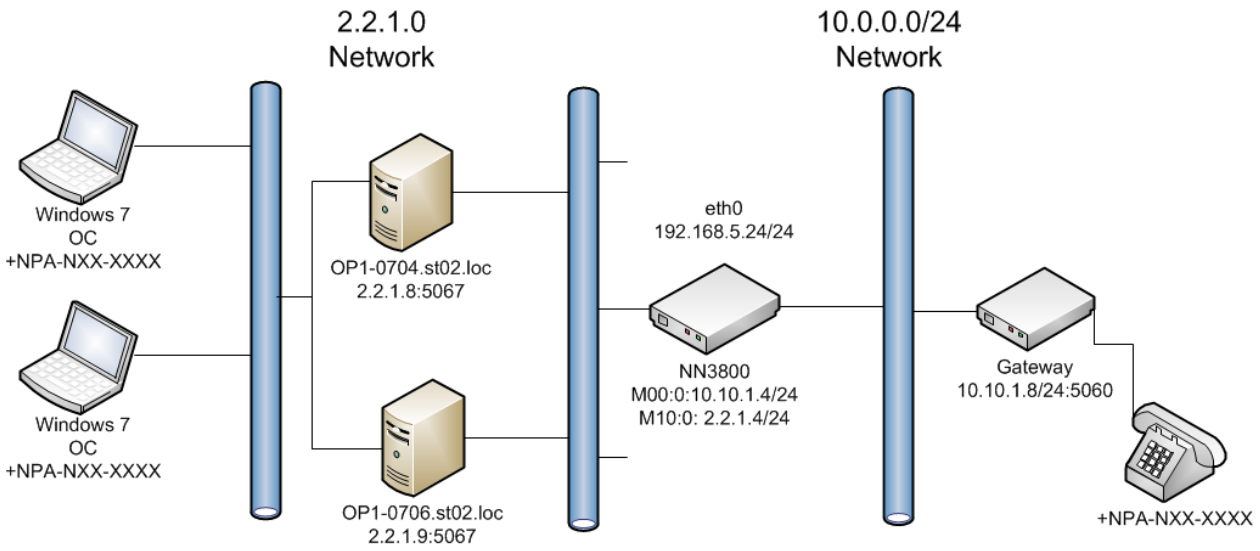
1.13. What you will need

- 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\
- IP address to be assigned to management interface (Wancom0) of the Net-Net SD

  The Wancom0 management interface MUST be connected and configured to a management network separate from the service interfaces. Otherwise the SD is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Acme Packet does not support SD configurations with management and media/service interfaces on the same subnet

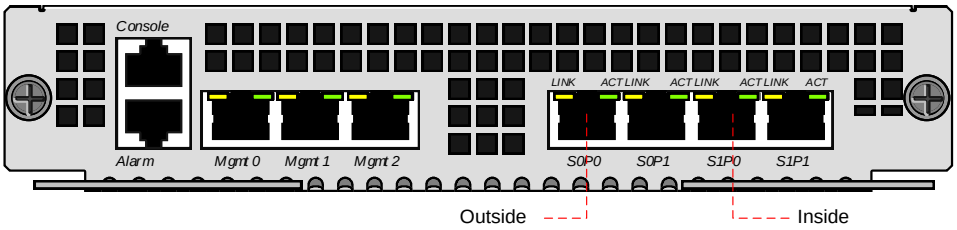
- IP address of Mediation Server external facing NIC
- IP address to be used for the Net-Net SD internal and external facing ports (Service Interfaces)
- IP address of the next hop gateway in the service provider network
- IP address of the enterprise DNS server

Lync Server 2010 Acme Packet Test Topology



1.14. 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 outside (gateway facing) network and the slot 0 port 1 (s1p0) interface into your inside (mediation server-facing) network. 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 **LYNC-VZB-IOT**are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

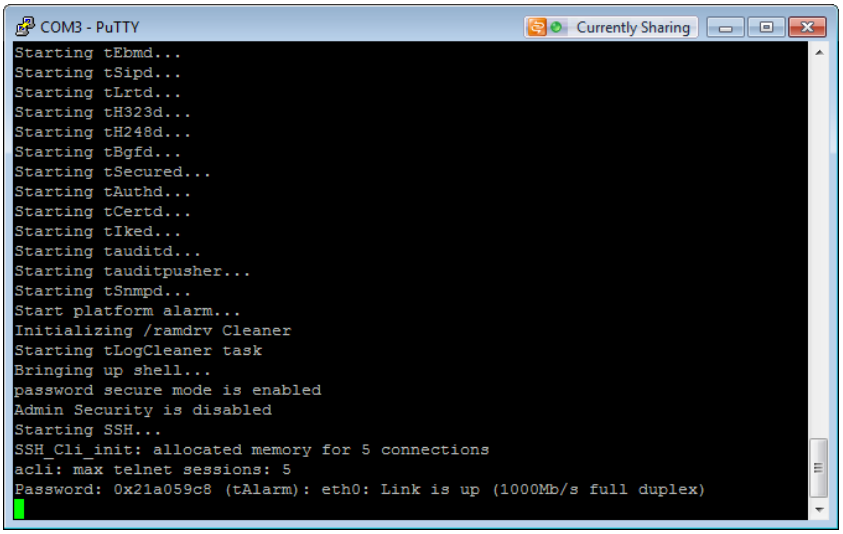
1. **Establish the serial connection to the Net-Net SD.**

   Confirm the Net-Net SD is powered off and connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port

on 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

Power on the Net-Net SD and confirm that you see the following output from the bootup sequence.

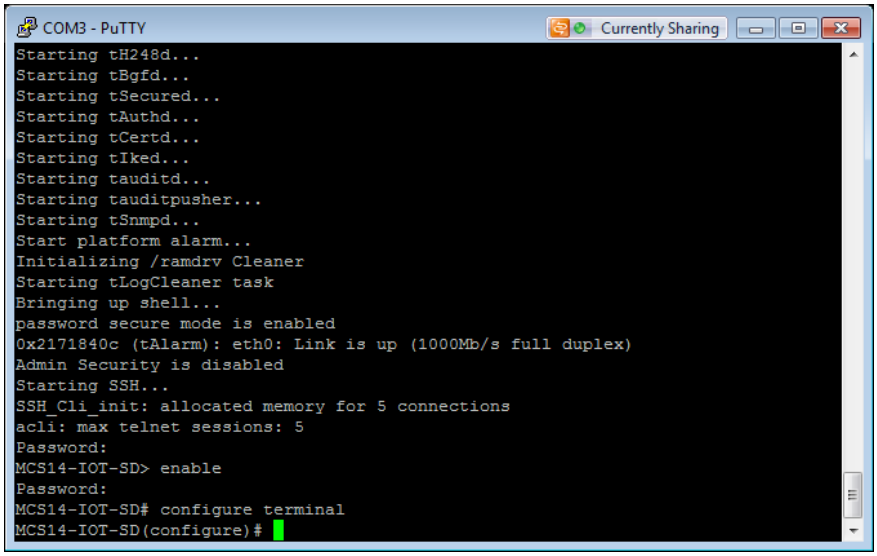


2. Login to the Net-Net SD and enter the configuration mode

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

You are now in the Global Configuration mode.



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

To assign an IP address, one has to configure the bootparams on the Net-Net SD, by going to `Lync-VZB-IOT#configure terminal --- >bootparams`

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

```
Lync-VZB-IOT#(configure)bootparam

'.' = clear field;  '-' = go to previous field;  q = quit
boot device             : eth0
processor number        : 0
host name               : acmesystem
file name               : /code/images/nnSCX637f2p4.xz --- >location where the
software is loaded on the SBC
inet on ethernet (e)    : 172.41.3.111:ffffff80 --- > This is the ip address of
the management interface of the SBC, type the IP address and mask in hex

inet on backplane (b)   :
host inet (h)           :
gateway inet (g)        : 172.41.0.1 --- > gateway address here
user (u)                : vxftp
ftp password (pw) (blank = use rsh)     : vxftp
flags (f)               :
target name (tn)        : Lync-VZB-IOT
startup script (s)      :

other (o)               :
```

4. Configure system element values

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

```
LYNC-VZB-IOT(configure)# system
LYNC-VZB-IOT(system)# system-config
LYNC-VZB-IOT(system-config)# hostname LYNC-VZB-IOT
LYNC-VZB-IOT(system-config)# description "Lync Server2010 SIP Trunking"
LYNC-VZB-IOT(system-config)# location "Redmond, WA"
LYNC-VZB-IOT(system-config)# default-gateway 172.41.0.1
LYNC-VZB-IOT(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 2010 SIP Trunking
location                        Redmond, WA
mib-system-contact
mib-system-name
mib-system-location             Redmond, WA
snmp-enabled                    enabled
enable-snmp-auth-traps          disabled
enable-snmp-syslog-notify       disabled
enable-snmp-monitor-traps       disabled
enable-env-monitor-traps        disabled
snmp-syslog-his-table-length    1
snmp-syslog-level               WARNING
system-log-level                WARNING
process-log-level               NOTICE
process-log-ip-address          0.0.0.0
process-log-port                0
collect
sample-interval                 5
push-interval                   15
boot-state                      disabled
start-time                      now
end-time                        never
red-collect-state               disabled
red-max-trans                   1000
red-sync-start-time             5000
red-sync-comp-time              1000
push-success-trap-state         disabled
```

```
call-trace                      disabled
internal-trace                  disabled
log-filter                      all
default-gateway                 172.41.0.1
restart                         enabled
exceptions
telnet-timeout                  0
console-timeout                 0
remote-control                  enabled
cli-audit-trail                 enabled
link-redundancy-state           disabled
source-routing                  disabled
cli-more                        disabled
terminal-height                 24
debug-timeout                   0
trap-event-lifetime             0
default-v6-gateway              ::
ipv6-support                    disabled
```

5. Configure Physical Interface values

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

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

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

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

```
phy-interface
name                            M00
operation-type                  Media
port                            0
slot                            0
virtual-mac
admin-state                     enabled
auto-negotiation                enabled
```

```
duplex-mode                     FULL
speed                           100
overload-protection             disabled
```

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

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

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

6. Configure Network Interface values

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

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

```
LYNC-VZB-IOT(phy-interface)# exit
LYNC-VZB-IOT(system)# network-interface
LYNC-VZB-IOT(network-interface)# name s1p0
LYNC-VZB-IOT(network-interface)# description "Mediation Server-facing
inside interface"
LYNC-VZB-IOT(network-interface)# ip-address 192.168.1.130
LYNC-VZB-IOT(network-interface)# netmask 255.255.255.0
LYNC-VZB-IOT(network-interface)# gateway 192.168.1.1
LYNC-VZB-IOT(network-interface)# pri-utility-addr 192.168.1.131
LYNC-VZB-IOT(network-interface)# sec-utility-addr 192.168.1.132
LYNC-VZB-IOT(network-interface)# add-hip-ip 192.168.1.130
LYNC-VZB-IOT(network-interface)# add-icmp-ip 192.168.1.130

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

network-interface
        name                            s1p0
```

```
        sub-port-id                     0
        description                     Mediation Server-facing inside
interface
        hostname
        ip-address                      192.168.1.130
        pri-utility-addr                192.168.1.131
        sec-utility-addr                192.168.1.132
        netmask                         255.255.255.0
        gateway                         192.168.1.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     192.168.1.130
        ftp-address
        icmp-address                    192.168.1.130
        snmp-address
        telnet-address
        ssh-address
```

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

```
LYNC-VZB-IOT(network-interface)# name s0p0
LYNC-VZB-IOT(network-interface)# description "VoIP gateway-facing
inside interface"
LYNC-VZB-IOT(network-interface)# ip-address 192.20.0.108
LYNC-VZB-IOT(network-interface)# netmask 255.255.255.0
LYNC-VZB-IOT(network-interface)# gateway 192.20.0.1
LYNC-VZB-IOT(network-interface)# pri-utility-addr 192.20.0.109
LYNC-VZB-IOT(network-interface)# sec-utility-addr 192.20.0.110
LYNC-VZB-IOT(network-interface)# dns-ip-primary 8.8.8.8
LYNC-VZB-IOT(network-interface)# dns-ip-backup1 8.8.4.4
LYNC-VZB-IOT(network-interface)# dns-domain tsengr.com
LYNC-VZB-IOT(network-interface)# add-hip-ip 192.20.0.108
LYNC-VZB-IOT(network-interface)# add-icmp-ip 192.20.0.108

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

network-interface
       name                            s0p0
       sub-port-id                     0
```

```
        description                     VoIP gateway-facing inside
interface
        hostname
        ip-address                      192.20.0.108
        pri-utility-addr                192.20.0.109
        sec-utility-addr                192.20.0.110
        netmask                         255.255.255.0
        gateway                         192.20.0.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary                  8.8.8.8
        dns-ip-backup1                  8.8.4.4
        dns-ip-backup2
        dns-domain                      tsengr.com
        dns-timeout                     11
        hip-ip-list                     192.20.0.108
        ftp-address
        icmp-address                    192.20.0.108
        snmp-address
        telnet-address
        ssh-address
```

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

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

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

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

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

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

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

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

```
        snmp-address
        telnet-address
        ssh-address
```

7. Configure Global SIP configuration

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

```
LYNC-VZB-IOT(network-interface)# exit
LYNC-VZB-IOT(system)# exit
LYNC-VZB-IOT(configure)# session-router
LYNC-VZB-IOT(session-router)# sip-config
LYNC-VZB-IOT(sip-config)# operation-mode dialog
LYNC-VZB-IOT(sip-config)# done

sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id
        egress-realm-id
        nat-mode                        None
        registrar-domain
        registrar-host
        registrar-port                  0
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
```

```
        extra-method-stats             disabled
        rph-feature                    disabled
        nsep-user-sessions-rate        0
        nsep-sa-sessions-rate          0
        registration-cache-limit       0
        register-use-to-for-lp         disabled
        refer-src-routing              disabled
        add-ucid-header                disabled
        proxy-sub-events
        pass-gruu-contact              disabled
        sag-lookup-on-redirect         disabled
        set-disconnect-time-on-bye     disabled
```

8. Configure Global Media configuration

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

By issuing the **`select`** then **`done`** commands at this level, you will be creating the media-manager element, enabling the media management functions in the Net-Net SD with the default values.

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

media-manager
state                          enabled
latching                       enabled
flow-time-limit                86400
initial-guard-timer            300
subsq-guard-timer              300
tcp-flow-time-limit            86400
tcp-initial-guard-timer        300
tcp-subsq-guard-timer          300
tcp-number-of-ports-per-flow   2
hnt-rtcp                       disabled
algd-log-level                 NOTICE
mbcd-log-level                 NOTICE
red-flow-port                  1985
red-mgcp-port                  1986
red-max-trans                  10000
red-sync-start-time            5000
red-sync-comp-time             1000
media-policing                 enabled
max-signaling-bandwidth        10000000
max-untrusted-signaling        100
```

```
min-untrusted-signaling        30
app-signaling-bandwidth        0
tolerance-window               30
rtcp-rate-limit                0
trap-on-demote-to-deny         disabled
min-media-allocation           2000
min-trusted-allocation         4000
deny-allocation                64000
anonymous-sdp                  disabled
arp-msg-bandwidth              32000
fragment-msg-bandwidth         0
rfc2833-timestamp              disabled
default-2833-duration          100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event    disabled
media-supervision-traps        disabled
dnsalg-server-failover         disabled
```

9. Configure Realms configuration

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

You will create two realms:

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

```
LYNC-VZB-IOT(media-manager-config)# exit
LYNC-VZB-IOT(media-manager)# realm-config
LYNC-VZB-IOT(realm-config)# identifier MS-Lync-Peer
LYNC-VZB-IOT(realm-config)# description "Mediation Server-facing
(Outside)"
LYNC-VZB-IOT(realm-config)# network-interfaces s1p0:0
LYNC-VZB-IOT(realm-config)# done

realm-config
        identifier                     MS-Lync-Peer
        description                    Mediation Server-facing(Outside)
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s1p0:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
```

```
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        fallback-bandwidth             0
        max-priority-bandwidth         0
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        cac-failure-threshold          0
        untrust-cac-failure-threshold  0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
```

```
        codec-policy
        codec-manip-in-realm            disabled
        codec-manip-in-network          disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@console
        last-modified-date              2012-02-02 16:36:03
```

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

```
LYNC-VZB-IOT(realm-config)# identifier VZB-SIP-trunk
LYNC-VZB-IOT(realm-config)# description "Gateway (outside)"
LYNC-VZB-IOT(realm-config)# network-interfaces s0p0:0
LYNC-VZB-IOT(realm-config)# done

realm-config
        identifier                      VZB-SIP-trunk
        description                     Gateway (outside)
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
```

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

```
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@172.41.0.11
        last-modified-date              2012-03-06 13:31:20
```

10. Configure SBC redundancy configuration

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

```
LYNC-VZB-IOT(realm-config)# exit
LYNC-VZB-IOT(media-manager)# exit
LYNC-VZB-IOT(configure)# system
LYNC-VZB-IOT(system)# redundancy
LYNC-VZB-IOT(redundancy)# state enabled
LYNC-VZB-IOT(redundancy)# peer
LYNC-VZB-IOT(rdncy-peer)# name Lync-VZB-IOT
LYNC-VZB-IOT(rdncy-peer)# state enabled
LYNC-VZB-IOT(rdncy-peer)# type Primary
LYNC-VZB-IOT(rdncy-peer)# destination
LYNC-VZB-IOT(rdncy-peer-dest)# address 169.254.1.1:9090
LYNC-VZB-IOT(rdncy-peer-dest)# network-interface wancom1:0
LYNC-VZB-IOT(rdncy-peer-dest)# done
destination
    address                         169.254.1.1:9090
    network-interface               wancom1:0
LYNC-VZB-IOT(rdncy-peer-dest)# address 169.254.2.1:9090
LYNC-VZB-IOT(rdncy-peer-dest)# network-interface wancom2:0
LYNC-VZB-IOT(rdncy-peer-dest)# done
destination
    address                         169.254.2.1:9090
    network-interface               wancom2:0
LYNC-VZB-IOT(rdncy-peer-dest)# exit
LYNC-VZB-IOT(rdncy-peer)# done
peer
    name                            Lync-VZB-IOT
    state                           enabled
    type                            Primary
```

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

```
        cfg-sync-comp-time             1000
        gateway-heartbeat-interval     10
        gateway-heartbeat-retry        3
        gateway-heartbeat-timeout      1
        gateway-heartbeat-health       1
        media-if-peercheck-time        0
        peer
                name                           SN1Secondary
                state                          enabled
                type                           Secondary
                destination
                        address                        169.254.1.2:9090
                        network-interface              wancom1:0
                destination
                        address                        169.254.2.2:9090
                        network-interface              wancom2:0
        peer
                name                           Lync-VZB-IOT
                state                          enabled
                type                           Primary
                destination
                        address                        169.254.1.1:9090
                        network-interface              wancom1:0
                destination
                        address                        169.254.2.1:9090
                        network-interface              wancom2:0
        last-modified-by               admin@console
        last-modified-date             2012-01-06 17:23:25
LYNC-VZB-IOT(redundancy)# exit
```

11. Configure SIP signaling configuration

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

Here you will be configuring the IP addresses and TCP ports on which the 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.

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

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

LYNC-VZB-IOT(sip-port)# exit
LYNC-VZB-IOT(sip-interface)# options dropResponse=183
LYNC-VZB-IOT(sip-interface)# done

sip-interface
        state                           enabled
        realm-id                        VZB-SIP-trunk
        description                     SIP Trunk-facing (Outside)
        sip-port
                address                         192.20.0.108
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
```

```
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        options                         dropResponse=183
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode  pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 101
        rfc2833-mode                    transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
```

```
        sip-profile
        sip-isup-profile
        last-modified-by                admin@console
        last-modified-date              2012-03-06 17:46:57
```

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

```
LYNC-VZB-IOT(sip-interface)# realm-id MS-Lync-Peer
LYNC-VZB-IOT(sip-interface)# description "Mediation Server-Facing
(Outside)"
LYNC-VZB-IOT(sip-interface)# sip-ports
LYNC-VZB-IOT(sip-port)# address 192.168.1.130
LYNC-VZB-IOT(sip-port)# transport-protocol TCP
LYNC-VZB-IOT(sip-port)# done
sip-port
address                         192.168.1.130
port                            5060
transport-protocol              TCP
tls-profile
allow-anonymous                 all
ims-aka-profile

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

sip-interface
        state                           enabled
        realm-id                        MS-Lync-Peer
        description                     Mediation Server-Facing(Outside)
        sip-port
                address                         192.168.1.130
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
```

```
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@10.0.221.199
        last-modified-date             2012-02-03 15:01:24
```

12. Configure next-hop signaling elements

To configure the next-hop signaling elements (i.e., the mediation server and PSTN gateway) you define session-agents. Use the **session-agent** command under the session-router branch. To enter the session-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 2010 Gateway specification outlines the need for the SBC to have capability to do DNS load balancing among a pool of mediation servers. This is currently supported by the Acme Packet SBC via A or SRV records, however not necessarily in a round-robin manner. In this document and testing, the SBC load balances between two mediation servers that are defined in a group (session-group) with round-robin algorithm configured. It is assumed that when using this kind of a configuration at any point another mediation server is added to the pool of servers, it will need to be explicitly configured on the SBC and added to the session-group which will be the responsibility of the enterprise network administrator.

We will first configure the PSTN gateway.

```
LYNC-VZB-IOTLYNC-VZB-IOT(sip-interface)# exit
LYNC-VZB-IOT(session-router)# hostname icrcn1n0001.customer07.tsengr.com
LYNC-VZB-IOT(session-router)# port 0
LYNC-VZB-IOT(session-router)# realm-id VZB-SIP-trunk
LYNC-VZB-IOT(session-router)# done

session-agent
        hostname                        icrcn1n0001.customer07.tsengr.com
        ip-address
        port                            0
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        VZB-SIP-trunk
        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                   0
        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              2012-01-26 13:42:47
```

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

```
LYNC-VZB-IOT(session-agent)# exit
LYNC-VZB-IOT(session-router)# session-group
Lync-VZB-IOT(session-group)# group-name MediationServerGroup
Lync-VZB-IOT(session-group)#description "Group for Mediation servers 1
and 2"
Lync-VZB-IOT(session-group)# strategy RoundRobin
Lync-VZB-IOT(session-group)# dest LyncMedSrv1.selab.com
Lync-VZB-IOT(session-group)# dest +LyncMedSrv2.selab.com
Lync-VZB-IOT(session-group)# done
session-group
        group-name                      MediationServerGroup
        description                     Group for Mediation servers 1 &2
        state                           enabled
        app-protocol                    SIP
        strategy                        RoundRobin
        dest
                                        LyncMedSrv1.selab.com
                                        LyncMedSrv2.selab.com
        trunk-group
        sag-recursion                   disabled
        stop-sag-recurse                401,407
```

Defining Mediation Server 1

```
LYNC-VZB-IOT(session-group)exit
LYNC-VZB-IOT(session-router)session-agent
LYNC-VZB-IOT(session-agent)# hostname LyncMedSrv1.selab.com
LYNC-VZB-IOT(session-agent)# ip-address 192.168.1.119
LYNC-VZB-IOT(session-agent)# port 5066
LYNC-VZB-IOT(session-agent)# app-protocol sip
LYNC-VZB-IOT(session-agent)# transport-method statictcp
LYNC-VZB-IOT(session-agent)# realm-id MS-Lync-Peer
LYNC-VZB-IOT(session-agent)# ping-method OPTIONS+hops=0
Lync-VZB-IOT(session-agent)# refer-call-transfer enabled
LYNC-VZB-IOT(session-agent)# done

session-agent
        hostname                        LyncMedSrv1.selab.com
        ip-address                      192.168.1.119
        port                            5066
        state                           enabled
```

```
        app-protocol                    SIP
        app-type
        transport-method                StaticTCP
        realm-id                        MS-Lync-Peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
```

```
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            enabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        last-modified-by               admin@10.0.221.199
        last-modified-date             2012-03-02 15:57:44
```

Defining Mediation Server 2

```
LYNC-VZB-IOT(session-agent)# hostname LyncMedSrv2.selab.com
LYNC-VZB-IOT(session-agent)# ip-address 192.168.1.120
LYNC-VZB-IOT(session-agent)# port 5066
LYNC-VZB-IOT(session-agent)# app-protocol sip
LYNC-VZB-IOT(session-agent)# transport-method statictcp
LYNC-VZB-IOT(session-agent)# realm-id MS-Lync-Peer
LYNC-VZB-IOT(session-agent)# ping-method OPTIONS+hops=0
Lync-VZB-IOT(session-agent)# refer-call-transfer enabled
LYNC-VZB-IOT(session-agent)# done

session-agent
        hostname                       LyncMedSrv2.selab.com
        ip-address                     192.168.1.120
        port                           5066
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               StaticTCP
        realm-id                       MS-Lync-Peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
```

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

```
        refer-call-transfer            enabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        last-modified-by               admin@10.0.221.199
        last-modified-date             2012-03-02 15:57:51
```

13. Configure SIP routing

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

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

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

policy-attribute
            next-hop                        SAG:MediationServerGroup
            realm                           MS-Lync-Peer
            action                          none
            terminate-recursion             disabled
            carrier
            start-time                      0000
            end-time                        2400
            days-of-week                    U-S
            cost                            0
            app-protocol                    SIP
            state                           enabled
            methods
            media-profiles
            lookup                          single
            next-key
            eloc-str-lkup                   disabled
            eloc-str-match

LYNC-VZB-IOT(local-policy-attributes)# exit
```

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

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

```
LYNC-VZB-IOT(local-policy)# from-address *
LYNC-VZB-IOT(local-policy)# to-address *
LYNC-VZB-IOT(local-policy)# source-realm MS-Lync-Peer
LYNC-VZB-IOT(local-policy)# policy-attributes
LYNC-VZB-IOT(local-policy-attributes)# next-hop
icrcn1n0001.customer07.tsengr.com
LYNC-VZB-IOT(local-policy-attributes)# realm VZB-SIP-trunk
LYNC-VZB-IOT(local-policy-attributes)# app-protocol sip
LYNC-VZB-IOT(local-policy-attributes)# done
policy-attribute
next-hop                        icrcn1n0001.customer07.tsengr.com
realm                           VZB-SIP-trunk
action                          none
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

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

local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        MS-Lync-Peer
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@172.41.0.11
        last-modified-date              2012-03-06 11:43:03
        policy-attribute
                next-hop               icrcn1n0001.customer07.tsengr.com
                realm                           VZB-SIP-trunk
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

To handle call transfer and refer scenarios (local refer handling by the SBC) when Lync client 1 refers/transfers the call to Lync Client 2, we will need two routes to route to the two mediation servers depending on the referred party

```
local-policy
        from-address
                                        *
        to-address
                                        LyncMedSrv1.selab.com
        source-realm
                                        VZB-SIP-trunk
        description                     For referred party header
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@console
        last-modified-date              2012-02-28 13:05:51
        policy-attribute
                next-hop                        LyncMedSrv1.selab.com
                realm                           MS-Lync-Peer
                action                          replace-uri
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol                    SIP
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
local-policy
        from-address
                                        *
        to-address
                                        LyncMedSrv2.selab.com
        source-realm
                                        VZB-SIP-trunk
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
```

```
        last-modified-by                admin@console
        last-modified-date              2012-02-28 13:07:58
        policy-attribute
                next-hop                        LyncMedSrv2.selab.com
                realm                           MS-Lync-Peer
                action                          replace-uri
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol                    SIP
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

14. Configure media handling

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

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

```
LYNC-VZB-IOT(local-policy)# exit
LYNC-VZB-IOT(session-router)# exit
LYNC-VZB-IOT(configure)# media-manager
LYNC-VZB-IOT(media-manager)# steering-pool
LYNC-VZB-IOT(steering-pool)# ip-address 192.168.1.130
LYNC-VZB-IOT(steering-pool)# start-port 30000
LYNC-VZB-IOT(steering-pool)# end-port 40000
LYNC-VZB-IOT(steering-pool)# realm-id MS-Lync-Peer
LYNC-VZB-IOT(steering-pool)# network-interface s1p0:0
LYNC-VZB-IOT(steering-pool)# done
steering-pool
        ip-address                      192.168.1.130
        start-port                      30000
        end-port                        40000
        realm-id                        MS-Lync-Peer
        network-interface               s1p0:0
        last-modified-by                admin@console
```

```
        last-modified-date              2012-01-05 14:34:29
```

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

```
LYNC-VZB-IOT(steering-pool)# ip-address 192.20.0.108
LYNC-VZB-IOT(steering-pool)# start-port 40000
LYNC-VZB-IOT(steering-pool)# end-port 50000
LYNC-VZB-IOT(steering-pool)# realm-id VZB-SIP-trunk
LYNC-VZB-IOT(steering-pool)# network-interface s0p0:0
LYNC-VZB-IOT(steering-pool)# done
steering-pool
        ip-address                      192.20.0.108
        start-port                      40000
        end-port                        50000
        realm-id                        VZB-SIP-trunk
        network-interface               s0p0:0
        last-modified-by                admin@172.41.0.11
        last-modified-date              2012-03-06 15:03:19
```

15. Transcoding

Transcoding requires a transcoding module to be installed in the SBC. In order to check if the module is present in your SBC, use command “show prom-info phy” and you should see the following output “**ID: 4 Port GiGE w/QoS & DSP**”. The transcoding module requires a minimum bootloader version compiled on “06/21/2011”. Using command “show version boot” should confirm the compilation date. Transcoding is required to interwork with Verizon SIP trunk. Microsoft Lync requires a minimum codec of G711 and Verizon SIP uses G.729 as a preferred codec, in order for a call to function between MS Lync and Verizon SIP trunk transcoding of the RTP stream is a must. Also, if you have a customer who supports G711 as well, then we need to edit the codec-policy to allow G711. Here is how you setup the SBC to support transcoding.

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

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

media-profile
```

```
        name                            G729
        subname                         vadoff
        media-type                      audio
        payload-type                    18
        transport                       RTP/AVP
        req-bandwidth                   0
        frames-per-packet               0
        parameters                      annexb=no
        average-rate-limit              0
        peak-rate-limit                 0
        max-burst-size                  0
        sdp-rate-limit-headroom         0
        sdp-bandwidth                   disabled
        police-rate                     0
        standard-pkt-rate               0
        last-modified-by                admin@console
        last-modified-date              2012-01-24 14:51:19

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

codec-policy
        name                            AllowG711
        allow-codecs                    PCMU PCMA telephone-event
        add-codecs-on-egress            PCMU PCMA telephone-event
        order-codecs
        force-ptime                     disabled
        packetization-time              20
        dtmf-in-audio                   disabled
        last-modified-by                admin@console
        last-modified-date              2012-01-24 14:52:21

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

```
codec-policy
        name                    remRED&CN
        allow-codecs            G729::vadoff telephone-event RED:no CN:no
        add-codecs-on-egress    G729::vadoff PCMU PCMA telephone-event
        order-codecs            G729::vadoff PCMU PCMA telephone-event
        force-ptime             disabled
        packetization-time      20
        dtmf-in-audio           disabled
        last-modified-by        admin@console
        last-modified-date      2012-02-01 18:04:54

LYNC-VZB-IOT(codec-policy)# exit
LYNC-VZB-IOT(media-manager)# realm-config
LYNC-VZB-IOT(realm-config)# sel
identifier:
1: VZB-SIP-trunk s0p0:0           0.0.0.0
2: MS-Lync-Peer s1p0:0           0.0.0.0
selection: 1
LYNC-VZB-IOT(realm-config)#codec-policy remRED&CN
LYNC-VZB-IOT(realm-config)# done
realm-config
        identifier                      VZB-SIP-trunk
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy                    voip-default
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
```

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

```
        hide-egress-media-update       disabled
        last-modified-by               admin@172.41.0.11
        last-modified-date             2012-03-06 13:31:20


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

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

```
        nat-trust-threshold            0
        deny-period                    30
        cac-failure-threshold          0
        untrust-cac-failure-threshold  0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
        codec-policy                   AllowG711
        codec-manip-in-realm           disabled
        codec-manip-in-network         disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
        last-modified-by               admin@console
        last-modified-date             2012-02-02 16:36:03
```

For customers who support G711, we need to simply edit the codec-policy to allow G711:

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

codec-policy
   name                  remRED&CN
   allow-codecs          PCMU PCMA G729::vadoff telephone-event RED:no
CN:no
   add-codecs-on-egress  PCMU PCMA G729::vadoff telephone-event
   order-codecs          PCMU PCMA G729::vadoff telephone-event
   force-ptime           disabled
   packetization-time    20
   dtmf-in-audio         disabled
   last-modified-by      admin@console
   last-modified-date    2012-02-01 18:04:54
```

16. Configure Sip-manipulations and translation rules

In order to cater to VZ's call flow standards, we need to configure certain header manipulation rules (HMR). There is a header rule to add user part to the Contact header and host part to the From header. Also, Lync does not send a Referred-by message on the REFER message for call transfer scenarios. It sends a Referred-by on the re-INVITE send to the SBC. We have a HMR in place to check if an INVITE message has a Referred-by header, and if it has then we take that value and put it in the Contact header of the new INVITE message going towards VZ. Also, since Lync does not send a P-Asserted-ID header, we insert that header in the request messages going towards VZ trunk. The sip-manipulation element can be found under the session-router element. The following are the sip-manipulation rules which you will need to configure:

```
sip-manipulation
        name                            ModContact
        description                     Modify Contact and From header
        split-headers
        join-headers
        header-rule
                name                            AddUserPart
                header-name                     Contact
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
```

```
                element-rule
                        name                            AddUserPart
                        parameter-name
                        type                            uri-user
                        action                          add
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $FROM_USER.$0
        header-rule
                name                            ModFrom
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            ModFrom
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rule
                name                            Add_privacy_HMR
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value                       PrivacyRequestedCalls
        header-rule
                name                            CheckForReferredBy
                header-name                     Referred-By
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            CheckforReferred
                        parameter-name
                        type                            uri-user
                        action                          store
```

```
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value                     (\+1)(.*)
                        new-value
        header-rule
                name                            OverwriteContact
                header-name                     Contact
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value             $CheckForReferredBy.$CheckforReferred
                new-value
                element-rule
                        name                            OverwriteUser
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $FROM_USER.$0
        header-rule
                name                            Add_P_Asserted_ID_new
                header-name                     P-Asserted-Identity
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value             $CheckForReferredBy.$CheckforReferred
                new-value
"<sip:"+$CheckForReferredBy.$CheckforReferred.$2+"@"+$LOCAL_IP+">"
        header-rule
                name                            RemoveReferredBy
                header-name                     Referred-By
                action                          delete
                comparison-type                 case-sensitive
                msg-type                        any
                methods
                match-value
                new-value
        header-rule
                name                            check_ms_source
                header-name                     ms-call-source
                action                          store
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
```

```
        header-rule
                name                            addDiv
                header-name                     Diversion
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value
$CheckForReferredBy.$CheckforReferred&!$check_ms_source
                new-value
                element-rule
                        name                            addDiv_er
                        parameter-name
                        type                            header-value
                        action                          add
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value
"<sip:"+$CheckForReferredBy.$CheckforReferred.$2+"@"+$LOCAL_IP+">"
        header-rule
                name                            DelmsSource
                header-name                     ms-call-source
                action                          delete
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
        header-rule
                name                            storeTo
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            storeTo_er
                        parameter-name
                        type                            uri-user
                        action                          store
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value                     ^(99)(.*)
                        new-value
        header-rule
                name                            ReplaceFromHeader
                header-name                     From
```

```
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            ReplaceFromHostPart
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       anonymous.invalid
                element-rule
                        name                            ReplaceDisplayURI
                        parameter-name
                        type                            uri-display
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       \"Anonymous\"
                element-rule
                        name                            ReplaceFromUserPart
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       anonymous
        header-rule
                name                            ReplaceContactHeader
                header-name                     Contact
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            ReplaceContactUserPart
                        parameter-name
                        type                            uri-user
                        action                          add
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
```

```
                        new-value                       anonymous
        header-rule
                name                            AddPrivacyHeader
                header-name                     Privacy
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value                       "id"
        header-rule
                name                            fixTo
                header-name                     To
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            fixTo_er
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                      $storeTo.$storeTo_er.$2
        header-rule
                name                            fixRURI
                header-name                     request-uri
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            fixRURI_er
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                      $storeTo.$storeTo_er.$2
        last-modified-by                admin@10.0.221.199
        last-modified-date              2012-03-02 16:08:52
sip-manipulation
        name                            PrivacyRequestedCalls
```

```
        description                     Inserts a Privacy id field for privacy
requested calls
        split-headers
        join-headers
        header-rule
                name                            storeTo
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            storeTo_er
                        parameter-name
                        type                            uri-user
                        action                          store
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value                     (991)(.*)
                        new-value
        header-rule
                name                            ReplaceFromHeader
                header-name                     From
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            ReplaceFromHostPart
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       anonymous.invalid
                element-rule
                        name                            ReplaceDisplayURI
                        parameter-name
                        type                            uri-display
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       \"Anonymous\"
                element-rule
```

```
                        name                            ReplaceFromUserPart
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       anonymous
        header-rule
                name                            ReplaceContactHeader
                header-name                     Contact
                action                           manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            ReplaceContactUserPart
                        parameter-name
                        type                            uri-user
                        action                          add
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       anonymous
        header-rule
                name                            AddPrivacyHeader
                header-name                     Privacy
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value                       "id"
        header-rule
                name                            fixTo
                header-name                     To
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            fixTo_er
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
```

```
                        comparison-type                case-sensitive
                        match-value
                        new-value
$storeTo.$storeTo_er.$2
        header-rule
                name                            fixRURI
                header-name                     request-uri
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $storeTo.$storeTo_er
                new-value
                element-rule
                        name                            fixRURI_er
                        parameter-name
                        type                            uri-user
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                     $storeTo.$storeTo_er.$2
        last-modified-by                admin@10.0.221.199
```

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

```
LYNC-VZB-IOT(session-router)# sip-interface
Lync-VZB-IOT(sip-interface)# sel
<realm-id>:
1: MS-Lync-Peer  192.168.1.130:5060
2: VZB-SIP-trunk 192.20.0.108:5060

selection: 2
Lync-VZB-IOT(sip-interface)# out-manipulationid ModContact
Lync-VZB-IOT(sip-interface)# done

sip-interface
        state                           enabled
        realm-id                        VZB-SIP-trunk
        description                     SIP Trunk-facing (Outside)
        sip-port
                address                         192.20.0.108
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
```

```
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        options                         dropResponse=183
        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              ModContact
        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              2012-03-06 17:46:57
```

Lync does send E164 numbers in the To and From headers whereas VZ does not accept E164 numbers. Hence we need a translation rule on the SBC to translate the E164 phone numbers into a regular one by stripping off the +1 from the phone numbers. The translation rule then needs to be added on the session-translation which then gets called from the VZ session-agent.

```
Lync-VZB-IOT(sip-interface)# exit
Lync-VZB-IOT(session-router)# translation-rules
Lync-VZB-IOT(translation-rules)# id stripplus1
Lync-VZB-IOT(translation-rules)# type delete
Lync-VZB-IOT(translation-rules)# delete-string +1
Lync-VZB-IOT(translation-rules)# done

translation-rules
        id                              stripplus1
        type                            delete
        add-string
        add-index                       0
        delete-string                   +1
        delete-index                    0
        last-modified-by                admin@console
        last-modified-date              2012-01-26 16:27:25

Lync-VZB-IOT(translation-rules)# exit
Lync-VZB-IOT(session-router)# session-translation
Lync-VZB-IOT(session-translation)# id stripplus1
Lync-VZB-IOT(session-translation)# rules-calling stripplus1
Lync-VZB-IOT(session-translation)# rules-called stripplus1
Lync-VZB-IOT(session-translation)# done

session-translation
        id                              stripplus1
        rules-calling                   stripplus1
        rules-called                    stripplus1
        last-modified-by                admin@console
        last-modified-date              2012-01-26 18:28:59
```

```
Lync-VZB-IOT(session-translation)# exit
Lync-VZB-IOT(session-router)# session-agent
Lync-VZB-IOT(session-agent)# sel
<hostname>:
1: icrcn1n0001.customer07.tsengr.com realm=VZB-SIP-trunk ip=
2: LyncMedSrv2.selab.com             realm=MS-Lync-Peer  ip=192.168.1.120
3: LyncMedSrv1.selab.com             realm=MS-Lync-Peer  ip=192.168.1.119

selection: 1
Lync-VZB-IOT(session-agent)# out-translationid stripplus1
Lync-VZB-IOT(session-agent)# done

session-agent
        hostname                        icrcn1n0001.customer07.tsengr.com
        ip-address
        port                            0
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        VZB-SIP-trunk
        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                   0
```

```
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid               stripplus1
        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              2012-01-26 13:42:47
```

4. Verify configuration integrity

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

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

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

15. Save and activate your configuration

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

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

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

Configuration is now complete.

For the EMEA configuration we have to change a couple of things like the session-agent and the local-policy to reflect the new EMEA SIP trunk domain address. Also, for the Referred-by sip-manipulation needs to be changed since the EMEA phone numbers will be different than the NA ones.

```
session-agent
        hostname                        icrcn1n0001.customer31.tsengr.com
        ip-address
        port                             0
        state                            enabled
        app-protocol                     SIP
        app-type
        transport-method                 UDP
        realm-id                         VZB-SIP-trunk
        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                    0
        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              2012-03-12 14:16:50

local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        MS-Lync-Peer
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@console
        last-modified-date              2012-03-07 15:01:30
        policy-attribute
                next-hop               icrcn1n0001.customer31.tsengr.com
                realm                          VZB-SIP-trunk
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
```

```
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

We also need to change a couple of header rules to make it work with the EMEA trunk.

```
header-rule
                name                            CheckForReferredBy
                header-name                     Referred-By
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            CheckforReferred
                        parameter-name
                        type                            uri-user
                        action                          store
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value                     (.*)
                        new-value

header-rule
                name                            Add_P_Asserted_ID_new
                header-name                     P-Asserted-Identity
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value       $CheckForReferredBy.$CheckforReferred
                new-value
"<sip:"+$CheckForReferredBy.$CheckforReferred.$0+"@"+$LOCAL_IP+">"

header-rule
                name                            addDiv
                header-name                     Diversion
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value
$CheckForReferredBy.$CheckforReferred&!$check_ms_source
```

```
                  new-value
                  element-rule
                          name                            addDiv_er
                          parameter-name
                          type                            header-value
                          action                          add
                          match-val-type                  any
                          comparison-type                 case-sensitive
                          match-value
                          new-value
"<sip:"+$CheckForReferredBy.$CheckforReferred.$0+"@"+$LOCAL_IP+">"
```

A basic configuration on the SBC to route calls to and from the Lync Server 2010 environment is now complete. The following sections highlight some of the useful tips to configure the SBC in order to successfully resolve and overcome interoperability challenges in a SIP trunking environment between the Lync Server 2010 and Service provider network. It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

Phase III – Test the Interface

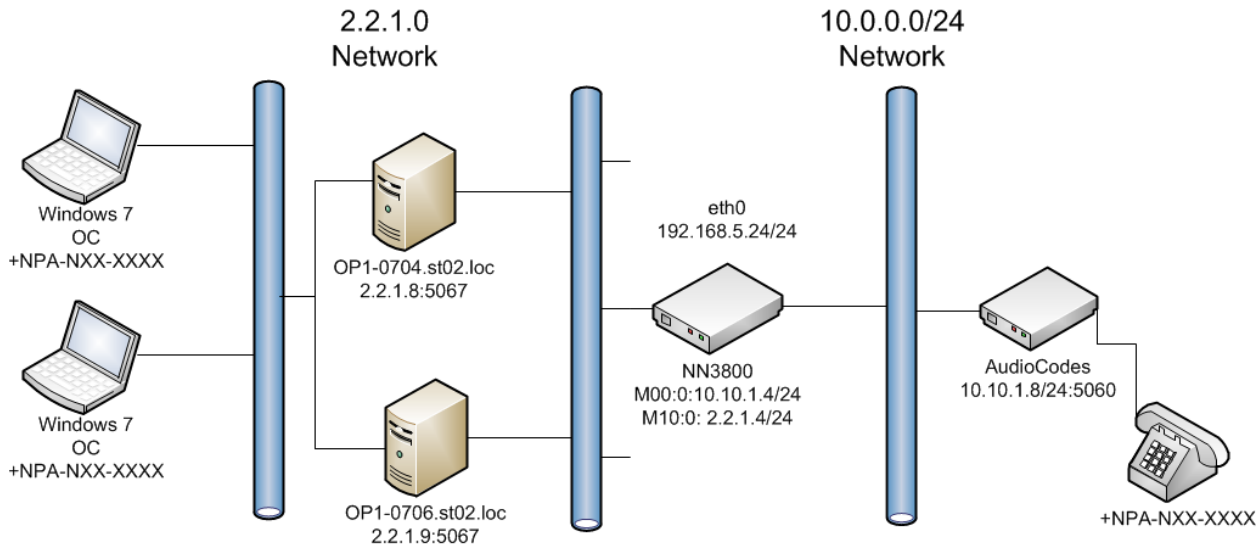
1.16. Overview

Once the Mediation Server and Net-Net Session Director have been configured, the final phase is to test the SIP trunk interface. The Microsoft Unified Communications Partner Engineering team has published a SIP Trunking Test Plan document. This section of provides a subset of the SIP Trunking Test Plan which is sufficient to assess that the deployment was successful. It is highly recommended that you use this test plan as a baseline in addition to any other tests you wish to run.

1.17. Testing

The following diagram shows the as built test topology. An analog VoIP gateway was used to represent the PSTN gateway on the service provider-side of the Net-Net SD.

Lync Server 2010 Acme Test Topology



1.18. Test Results

The following table lists a summary of our test case results. The test case number refers to the test case documented in the Microsoft SIP Trunking Test Plan.

Basic Calls

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
	Security			
TC1	Layer 2 IPSec Authentication	Pass		IPSec Tunnel established and working
	DNS SRV			
TC2	Service Protocols/Port Adherence	Pass		Capture Received and verified to be correct.
	Inbound			
TC3	Inbound Call Loop Avoidance	Pass		Capture received, verified that 480 error message sent to Proxy.
TC4	Inbound call with originator (PSTN) release	Pass		Capture received, verified results are as expected.
TC5	Inbound call with terminator (CPE) release	Pass		Capture received, verified results are as expected.
TC6	Inbound call - Hang-up during Ring phase	Pass		Capture received, verified results are as expected.
TC7	Inbound Call - vendor phone not registered/online	Pass		Capture received, verified that 404 error message sent to proxy.
TC8	Inbound Calling Line Identification (Caller-ID)	Pass	Caller-ID matches the Calling party number of the PSTN phone.	
TC9	Inbound Call Waiting	Pass		
TC10	Inbound G.711 Fax	NA		
TC11	Inbound T.38 Fax	NA		
TC12	Inbound Call from PSTN with Privacy Restricted	Pass		
	Outbound			

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC13	Unscreened ANI using Diversion Header	Pass	CLI in the FROM header displayed as Caller ID on the PSTN phone	
TC14	Unscreened ANI using P-Asserted Identity	Pass	CLI in the FROM header displayed as Caller ID on the PSTN phone	
TC15	Outbound call with Originator (CPE) release	Pass		
TC16	Outbound call with Terminator (PSTN) release	Pass		
TC17	Outbound call - Hangup during ring phase	Pass		
TC18	Outbound 1+10digit call	Pass		
TC19	Outbound International Call	Pass		
TC20	Outbound 311 Non-Emergency call	Pass		
TC21	Outbound 555-1212 Directory Assistance	Pass		
TC22	Outbound 411 Directory Assistance	Pass	Got an error message “Please dial a 0 or 1 before the number and try the call again.”	
TC23	Outbound 1411 Directory Assistance	Pass		
TC24	Outbound 711 Telephone Relay Services (Hearing Impaired)	Pass		
TC25	911 Emergency Service	Pass		
TC26	Outbound 511 Information Line	Pass	Got an error message “The number you have dialed is not in service, please check the number and dial again”.	
TC27	Outbound Toll-Free Call	Pass		
TC28	Operator assistance (0+ Local)	Pass		

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC29	Operator assistance (0+ Toll)	Pass		
TC30	Operator assistance (0 Minus)	Pass		
TC31	Operator assistance (00 Minus)	Pass		
TC32	Operator assistance (01+ international)	Pass		
TC33	Outbound G.711 Fax	NA		
TC34	Outbound T.38 Fax	NA		
TC35	Outbound Calling Line Identifier (Caller ID)	Pass	Caller ID correctly displayed on the PSTN phone	
TC36	Outbound Fast Answer	Pass		
TC37	Outbound Call to PSTN with Privacy Requested	Pass		
TC38	Calling Party Number not provisioned	Pass		
	Protocols			
TC39	UDP for SIP	Pass		
TC40	SDP support (RFC 2327)	Pass		
TC41	RTP and RTCP support (RFC 3550)	Fail		
TC42	SIP Headers	Pass		
TC43	18x Behavior	Pass		
TC44	302 Behavior	Pass	SIP messaging from previous tests used to verify results	
TC45	Diversion Header	Pass		
TC46	DTMF RFC 2833—Outbound	Fail		
TC47	DTMF RFC 2833—Inbound	Pass		

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC48	Offer/Answer with SDP (RFC3264)	Pass	SIP messaging from previous tests used to verify results	
TC49	Call Hold (RFC 3264)	Pass		
TC50	Media Inactivity	Pass	Kept on hold for more than 3 minutes	
TC51	FQDN	Pass		
	Media			
TC52	G.711 ulaw	Pass		
TC53	G.729 and G.729a	Pass		
TC54	Codec Negotiation	Pass		
TC55	Early Media Support	Pass		
	Diffserv			
TC56	RTP	Pass		
TC57	SIP	Pass		
	Attended Call Transfer **Re-INVITE Method**			
TC58	IPPBX-PSTN-IPPBX	Pass		
TC59	IPPBX-PSTN-PSTN	Pass		
TC60	PSTN-IPPBX-IPPBX	Pass		
TC61	PSTN-IPPBX-PSTN	Pass		
	Semi-Attended Call Transfer **Re-INVITE Method**			
TC62	IPPBX-PSTN-IPPBX	Pass		
TC63	IPPBX-PSTN-PSTN	Pass		
TC64	PSTN-IPPBX-IPPBX	Pass		
TC65	PSTN-IPPBX-PSTN	Pass		
	Blind Call Transfer **Re-INVITE Method**			

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC66	IPPBX-PSTN-IPPBX	Pass		
TC67	IPPBX-PSTN-PSTN	Pass		
TC68	PSTN-IPPBX-IPPBX	Pass		
TC69	PSTN-IPPBX-PSTN	Pass		
	Attended Call Transfer **REFER Method**			
TC70	IPPBX-PSTN-IPPBX	Not Supported		
TC71	IPPBX-PSTN-PSTN	Not Supported		
TC72	PSTN-IPPBX-IPPBX	Not Supported		
TC73	PSTN-IPPBX-PSTN	Not Supported		
	Semi-Attended Call Transfer **REFER Method**			
TC74	IPPBX-PSTN-IPPBX	Not Supported		
TC75	IPPBX-PSTN-PSTN	Not Supported		
TC76	PSTN-IPPBX-IPPBX	Not Supported		
TC77	PSTN-IPPBX-PSTN	Not Supported		
	Blind Call Transfer **REFER Method**			
TC78	IPPBX-PSTN-IPPBX	Not Supported		
TC79	IPPBX-PSTN-PSTN	Not Supported		
TC80	PSTN-IPPBX-IPPBX	Not Supported		
TC81	PSTN-IPPBX-PSTN	Not Supported		
	Call Conference			
TC82	IPPBX-PSTN-IPPBX	Pass		
TC83	IPPBX-PSTN-PSTN	Pass		

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC84	PSTN-IPPBX-IPPBX	Pass		
TC85	PSTN-IPPBX-PSTN	Pass		
	CPE Failover Behavior			
TC86	Options method request and response	Pass		
TC87	Round-Robin (Load share 50/50 between the two CPEs	Pass		
TC88	Primary/Secondary failover (Hunt)	Pass		
TC89	Both CPE Fail behavior	Pass		
TC90	Verizon Alternate Route using DNS/SRV query	NA		**This is a future requirement that is not supported at this time.**
TC91	Verizon Alternate Route using IP:port assignment	NA		**This is a future requirement that is not supported at this time.**
	Ambient Noise			
TC92	Ambient Noise – CPE to PSTN	Pass		
TC93	Ambient Noise – PSTN to CPE	Pass		
	EMEA Retail Interop			
	Inbound – Calls From Verizon PSTN to the Vendor VoIP			
TC94	Inbound Fax	NA		
TC95	Inbound - G.711 CODEC Negotiation	Pass		
TC96	Inbound - G.729 CODEC Negotiation	Pass		

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
	Outbound – Vendor VOIP TO Verizon PSTN CALL DIRECTION			
TC97	Outbound - FAX	NA		
TC98	Outbound - G711 CODEC Negotiation	Pass		
TC99	Outbound - G729 CODEC Negotiation	Pass		
TC100	Outbound - Call Redial	Pass		
	Re-Invite Call Test Cases			
	Attended Call Transfers			
TC101	IP-PBX calls PSTN attended transfer to IP-PBX	Pass		
TC102	IP-PBX calls PSTN attended transfer to PSTN	Pass		
TC103	PSTN calls IP-PBX attended transfer to IP-PBX	Pass		
TC104	PSTN calls IP-PBX attended transfer to PSTN	Pass		
	Semi-Attended Call Transfers			
TC105	IP-PBX calls PSTN semi-attended transfer to IP-PBX	Pass		
TC106	IP-PBX calls PSTN semi-attended transfer to PSTN	Pass		
TC107	PSTN calls IP-PBX semi-attended transfer to IP-PBX	Pass		
TC108	PSTN calls IP-PBX semi-attended transfer to PSTN	Pass		
	Blind Call Transfers			
TC109	IP-PBX calls PSTN with blind transfer to IP-PBX	Pass		
TC110	IP-PBX calls PSTN with blind transfer to PSTN	Pass		

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC111	PSTN calls IP-PBX with blind transfer to IP-PBX	Pass		
TC112	PSTN calls IP-PBX with blind transfer to PSTN	Pass		
	REFER Call Transfer Test Cases			
	Attended Call Transfers			
TC113	IP-PBX calls PSTN attended transfer to IP-PBX	Not Supported		
TC114	IP-PBX calls PSTN attended transfer to PSTN	Not Supported		
TC115	PSTN calls IP-PBX attended transfer to IP-PBX	Not Supported		
TC116	PSTN calls IP-PBX attended transfer to PSTN	Not Supported		
	Semi-Attended Call Transfers			
TC117	IP-PBX calls PSTN semi-attended transfer to IP-PBX	Not Supported		
TC118	IP-PBX calls PSTN semi-attended transfer to PSTN	Not Supported		
TC119	PSTN calls IP-PBX semi-attended transfer to IP-PBX	Not Supported		
TC120	PSTN calls IP-PBX semi-attended transfer to PSTN	Not Supported		
	Blind Call Transfers			
TC121	IP-PBX calls PSTN with blind transfer to IP-PBX	Not Supported		
TC122	IP-PBX calls PSTN with blind transfer to PSTN	Not Supported		
TC123	PSTN calls IP-PBX with blind transfer to IP-PBX	Not Supported		
TC124	PSTN calls IP-PBX with blind transfer to PSTN	Not Supported		
	Conference Call Test Cases			

Test Case ID	Requirement	Result	Vendor Comments	Verizon Comments
TC125	IP-PBX calls PSTN conference to IP-PBX	Pass		
TC126	IP-PBX calls PSTN conference to PSTN	Pass		
TC127	PSTN calls IP-PBX conference to IP-PBX	Pass		
TC128	PSTN calls IP-PBX conference to PSTN	Pass		

Troubleshooting Tools

If you find that you are not able to complete calls or have problems with the test cases, there are a few tools available for Windows Server, Lync Server, and the Net-Net SD 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 any issues you may encounter.

Since we are concerned with communication between the Lync Server mediation server and the Net-Net SD we will focus on the troubleshooting tools to use between those devices if calls are not working or tests are not passing.

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 only a few areas in which one would use the Event Viewer for troubleshooting:

- The Enterprise Voice client;
- The Lync Server Front End server;
- An Lync Server Standard Edition Server; and
- An Lync Server Mediation Server.

On the Net-Net SD

The Net-Net SD 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 SD Console:

```
LYNC-VZB-IOT# reset sipd

LYNC-VZB-IOT# notify sipd debug

LYNC-VZB-IOT#

enabled SIP Debugging

LYNC-VZB-IOT# 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\akonar>ftp 192.168.5.24

Connected to 192.168.85.55.

220 LYNC-VZB-IOTFTP 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.

TELNET

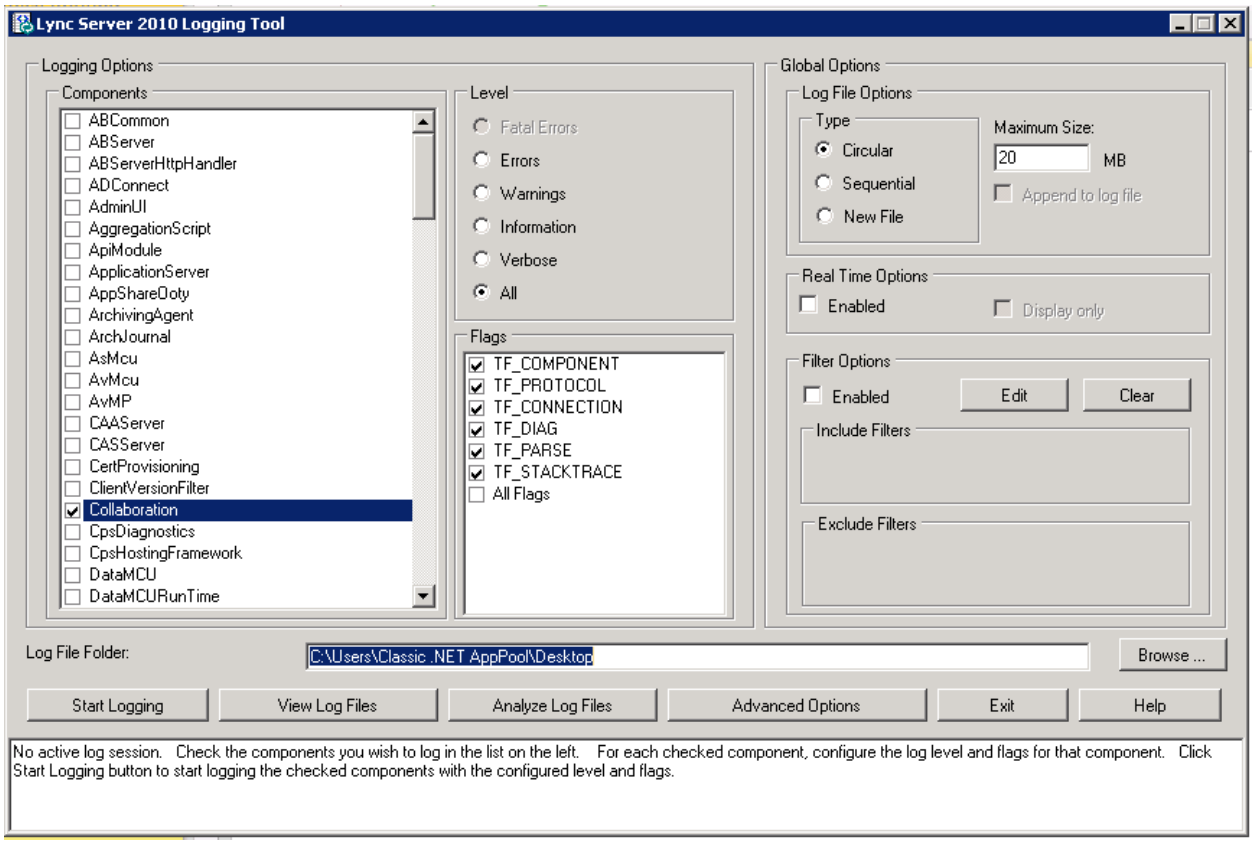
Since we are working within an architecture which uses bound TCP listening ports for functionality, the simplest form of troubleshooting can be seeing if the devices are listening on a particular port, as well as confirming that the there is nothing blocking them such as firewalls. Ensure that you have a TELNET client available on a workstation as well as on the Lync Server mediation server.

The Lync Server mediation server will listen on TCP port 5067 by default for SIP signaling. In our example we are listening on 5060 on the PSTN facing NIC. From the Standard Edition pool or Enterprise Edition pool the Mediation Server would be listening on port 5061. Tests may include:

- Client to pool server: **telnet <servername> 5061**
- Pool server to Mediation Server: **telnet <servername> 5061**

Lync Server Logging Tool

The Communications Server Logging Tool provides deeper information then one would get from the Event Viewer. The logging tool is extremely powerful with great depth and breadth. Please use the help information available with this tool. This can be accessed from any one of the Lync Server servers by running Start/All Programs/Microsoft Communications Server 2010/Communications Server Logging Tool.


Lync Server 2010 Logging Tool
Logging Options
Components
ABCommon
ABServer
ABServerHttpHandler
ADConnect
AdminUI
AggregationScript
ApiModule
ApplicationServer
AppShareOoty
ArchivingAgent
ArchJournal
AsMcu
AvMcu
AvMP
CAAServer
CASServer
CertProvisioning
ClientVersionFilter
Collaboration
CpsDiagnostics
CpsHostingFramework
DataMCU
DataMCURunTime
Level
Fatal Errors
Errors
Warnings
Information
Verbose
All
Flags
TF_COMPONENT
TF_PROTOCOL
TF_CONNECTION
TF_DIAG
TF_PARSE
TF_STACKTRACE
All Flags
Global Options
Log File Options
Type
Circular
Sequential
New File
Maximum Size:
20
MB
Append to log file
Real Time Options
Enabled
Display only
Filter Options
Enabled
Edit
Clear
Include Filters
Exclude Filters
Log File Folder:
C:\Users\Classic .NET AppPool\Desktop
Browse ...
Start Logging
View Log Files
Analyze Log Files
Advanced Options
Exit
Help
No active log session. Check the components you wish to log in the list on the left. For each checked component, configure the log level and flags for that component. Click Start Logging button to start logging the checked components with the configured level and flags.

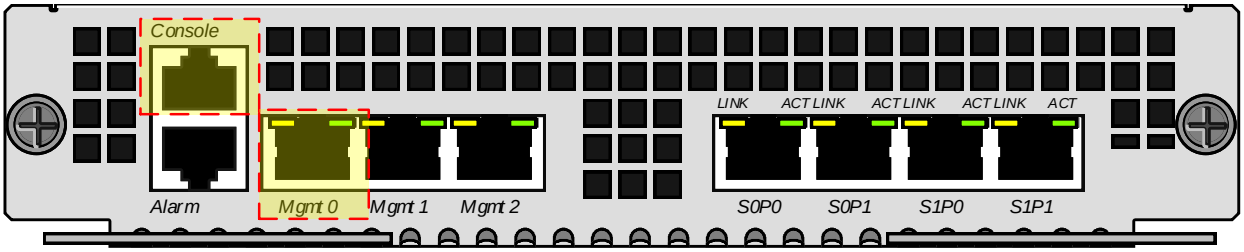
Appendix – Acme Packet Command Line Interface

a. Accessing the ACLI

Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH, which must be explicitly configured.

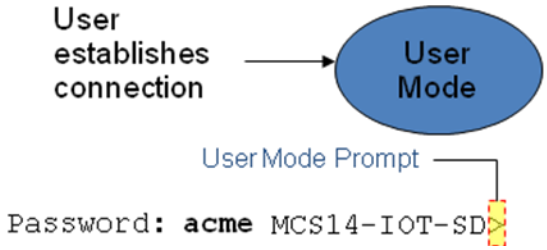
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the Net-Net SD.



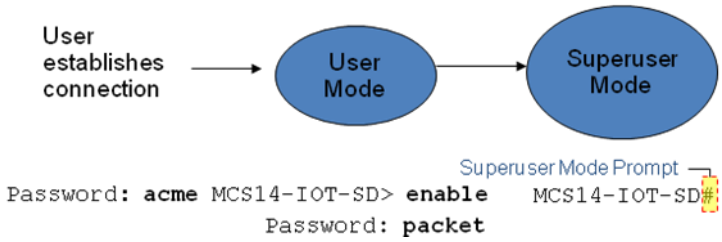
ACLI Basics

There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the Net-Net SD, the prompt for the User mode password appears. The default password is **acme**.



User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.

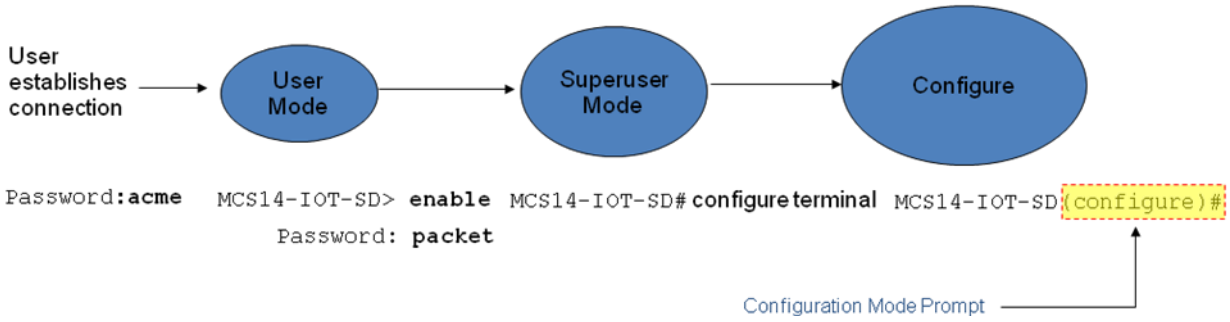


The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the **`enable`** command in the User mode.

From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the **`exit`** command.

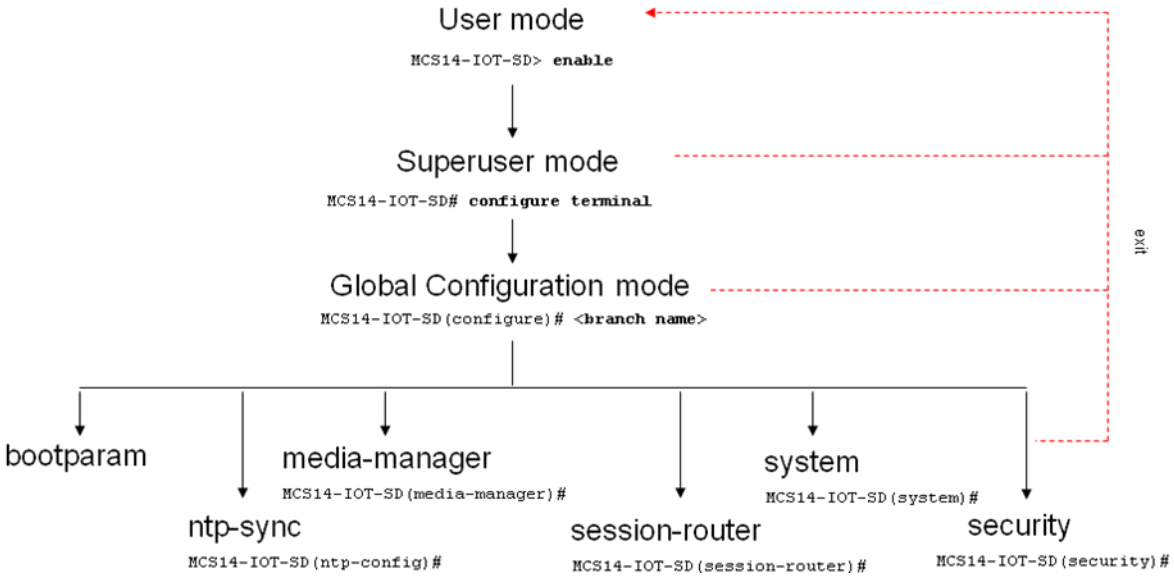
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **LYNC-VZB-IOT(configure)#**. To return to the Superuser mode, issue the **`exit`** command.



In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.



The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to Net-Net SD boot parameters. Key boot parameters include:

```
'.' = clear field;  '-' = go to previous field;  q = quit
boot device             : eth0
processor number        : 0
host name               :
file name               : /tffs0/nnSCX620.gz
inet on ethernet (e)    : 10.0.3.11:ffff0000
inet on backplane (b)   :
host inet (h)           : 10.0.3.100
gateway inet (g)        : 10.0.0.1
user (u)                : anonymous
ftp password (pw) (blank = rsh)       : anonymous
flags (f)               : 0x8
target name (tn)        : MCS14-IOT-SD
startup script (s)      :
other (o)
```

- boot device – The global management port, usually eth0
- file name – The boot path and the image file.
- inet on ethernet – The IP address and subnet mask (in hex) of the management port of the SD.
- host inet –The IP address of external server where image file resides.
- user and ftp password – Used to boot from the external FTP server.
- gateway inet – The gateway IP address for reaching the external server, if the server is located in a different network.

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the Net-Net SD time and date.

The security branch provides access to security configuration.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, iwf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media-manager, and so forth.

You will use media-manager, session-router, and system branches for most of your working configuration.

Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element. For example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- SIP-ports - are children of the sip-interface element
- peers – are children of the redundancy element
- destinations – are children of the peer element

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.

   When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.

2. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the **`show`** command before issuing the **`done`** command. The parameters that you did not configure are filled with either default values or left empty.

3. On completion, you must issue the **`done`** command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.

4. Issue the **`exit`** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the Net-Net SD reboots, your configurations will be lost.

Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

1. Enter the element that you will edit at the correct level of the ACLI path.

2. Select the element that you will edit, and view it before editing it.
   The **`select`** command loads the element to the volatile memory for editing. The **`show`** command allows you to view the element to ensure that it is the right one that you want to edit.

3. Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.

4. It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the **`show`** command before issuing the **`done`** command.

5. On completion, you must issue the **`done`** command.

6. Issue the **`exit`** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the Net-Net SD reboots, your configurations will be lost.

Deleting an Element

The **no** command deletes an element from the configuration in editing.

To delete a single-instance element,

1. Enter the **`no`** command from within the path for that specific element
2. Issue the **`exit`** command.

To delete a multiple-instance element,

1. Enter the **`no`** command from within the path for that particular element.
   The key field prompt, such as <name>:<sub-port-id>, appears.
2. Use the <Enter> key to display a list of the existing configured elements.
3. Enter the number corresponding to the element you wish to delete.
4. Issue the **`select`** command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the Net-Net SD reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the Net-Net SD: the edited configuration, the saved configuration, and the running configuration.

- The **edited configuration** – this is the version that you are making changes to. This version of the configuration is stored in the Net-Net SD's volatile memory and will be lost on a reboot. To view the editing configuration, issue the **`show configuration`** command.
- The **saved configuration –** on issuing the **`save-config`** command, the edited configuration is copied into the non-volatile memory on the Net-Net SD and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.
- The **running configuration** is the saved then activated configuration. On issuing the **`activate-config`** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect. To view the running configuration, issue command show **`running-config`**.

Saving the Configuration

The **`save-config`** command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the **save-config** command, the Net-Net SD displays a reminder on screen stating that you must use the **activate-config** command if you want the configurations to be updated.

```
MCS14-IOT-SD# save-config
Save-Config received, processing.
waiting 1200 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'.
MCS14-IOT-SD#
```

Activating the Configuration

On issuing the **activate-config** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration.

Some configuration changes are service affecting when activated. For these configurations, the Net-Net SD warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
MCS14-IOT-SD# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
MCS14-IOT-SD#
```