CBS Cloud Voice – Microsoft Lync Configuration Guide

What is CBS Cloud Voice Business Trunking?

CBS Cloud Voice Business Trunking is the name given to Columbus Business Solutions' SIP Trunks.

What is SIP?

The Session Initiation Protocol (SIP) is used to initiate and manage Voice over IP (VoIP) communications sessions for basic telephone service and for additional real-time communication services, such as instant messaging, conferencing, presence detection, and multimedia.

What is a SIP Trunk?

A SIP trunk is an IP connection that establishes a SIP communications link between your organisation and Columbus Business Solutions. Typically, a SIP trunk is used to connect your organisation's central site to our network. In some cases, you may also opt to use SIP trunking to connect your branch sites as well.

SIP Trunking for Microsoft Lync Server

The Lync Server (2010 and 2013) SIP trunking capabilities enable the following:

- An enterprise user, whether inside or outside the corporate firewall, can make a local call or a long-distance call that is terminated on the Public Switched Telephone Network (PSTN).
- Any PSTN subscriber can contact an enterprise user inside or outside the corporate firewall by dialling a Direct Inward Dialling (DID) number that is associated with that enterprise user.

Cost Savings

The cost savings associated with SIP trunking can be substantial:

- Free site-to-site calling
- Shared connectivity for voice and data
- Scalability
- Basic rate interface (BRI) and primary rate interface (PRI) rental charges can be eliminated

Beyond Voice

Voice features are often the primary motivation for deploying SIP trunking, but voice support is just the first step. With SIP trunking, you can extend VoIP capabilities and enable Lync Server to deliver a richer set of services. For example:

- Sharing of Presence status
- Instant Messaging
- Video calling and conferencing

To implement SIP trunking, you must route the connection through a Mediation Server, which acts as a proxy for communications sessions between Lync Server clients and Columbus Business Solutions and transcodes media, when necessary.

Each Mediation Server has an internal network interface and an external network interface. The internal interface connects to the Front End Servers. The external interface is commonly called the gateway interface because it has traditionally been used to connect the Mediation Server to a PSTN gateway or an IP-PBX. A SIP trunk connects the external interface of the Mediation Server to our voice network over Columbus Business Solutions fibre.

Centralised v Distributed SIP Trunking

- Centralised SIP Trunking - Routes all Voice over Internet Protocol (VoIP) traffic, including branch site traffic, through your central site. The centralised deployment model is simple, cost-effective, and is generally the recommended approach for implementing SIP trunks with Lync Server.
- Distributed SIP Trunking - a deployment model in which you implement a local SIP trunk at one or more branch sites. VoIP traffic is then routed from the branch site directly to a service provider without going through the central site.

Distributed SIP trunking is required only in the following cases:

- The branch site requires survivable phone connectivity (for example, if the WAN goes down). This requirement should be analysed for each branch site; some of your branches may require redundancy and failover, whereas others may not.
- Resiliency is required between two central sites. You need to make sure that a SIP trunk terminates at each central site.
- The branch site and central site are in different countries/regions. For compatibility and legal reasons, you need at least one SIP trunk per country/region.

Depending on the geographical location of sites and how much traffic you anticipate within your enterprise, you may not want to route all users through the central SIP trunk, or you may opt to route some users through a SIP trunk at their branch site. To analyse your needs, answer the following questions:

- How big is each site (that is, how many users are enabled for Enterprise Voice)?
- Which Direct Inward Dialling (DID) numbers at each site get the most phone calls?

The decision whether to deploy centralised or distributed SIP trunking requires a cost-benefit analysis. In some cases, it may be advantageous to opt for the distributed deployment model even if it is not required. In a completely centralised deployment, all branch site traffic is routed over WAN links. Instead of paying for the bandwidth required for WAN linking, you may want to use distributed SIP trunking. For example, you may want to deploy a Standard Edition server at a branch site with federation to the central site, or you may want to deploy a Survivable Branch Appliance or a Survivable Branch Server with a small gateway.

The Columbus Network

CBS provides SIP Trunking over a dedicated VLAN across our Metro Ethernet network; this ensures prioritisation of voice traffic.

Bandwidth Requirements

CBS will ensure the required bandwidth to support the number of concurrent calls you require.

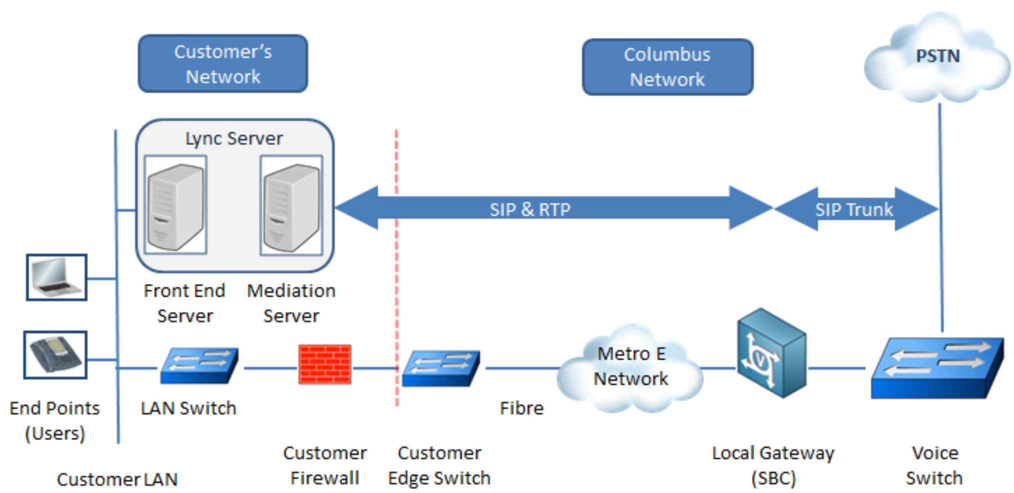
Codecs

CBS SIP Trunking and Lync Server support the following codecs:
- G.711 a-law (used primarily outside North America)
- G.711 μ-law (used in North America)

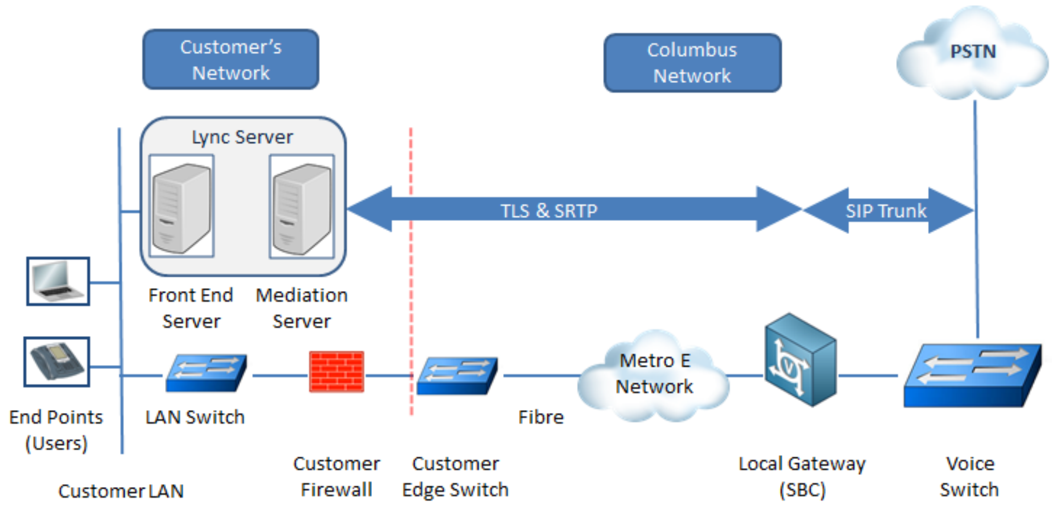
SIP Trunking Topology

The following diagram shows the SIP trunking topology options for Lync Server:

1. Standard SIP trunks:



2. Encrypted SIP trunks:



As shown in the diagram, SIP signalling traffic is transported from the Session Border Controller across the Columbus and Customer networks to the Mediation Server. If the trunk is encrypted Transport Layer Security (TLS) is used.

Real-time Transport Protocol (RTP) transports the media traffic (TCP); if the trunk is encrypted, this will be Secure Real-time Transport Protocol (SRTP).

A dedicated VLAN carries SIP signalling and media traffic from the Customer Switch across the CBS Metro E fibre network to the Session Border Controller.

A dedicated VLAN must be configured across the Local Area Network from the Lync Server environment to the Customer Edge Switch; this marks the demarcation point between the Customer and Columbus networks.

CBS Details

CBS will provide you with the following information for your connection:

- IP address for the CBS Session Border Controller
- VLAN details

Your Details

CBS will require the following information from you:

- The external IP Address for your Mediation Server
- FQDN for your Mediation Server

Security Certificate

To determine whether you need a certificate for SIP trunking, depends on your required protocol support:

1. Standard SIP trunks do not need a certificate.
2. Encrypted SIP trunks (TLS); CBS will provide you with a certificate (CBS recommends the encryption option).

Note: SIP works in conjunction with real-time transport protocol (RTP) or secure real-time transport protocol (SRTP), the protocols that manage the actual voice data in Voice over Internet Protocol (VoIP) calls.

Deployment Methodology

To implement the Lync Server side of the SIP trunk connection, follow these steps:

- Using the Lync Server Topology Builder, create and configure the SIP domain topology.
- Using the Lync Server Control Panel, configure voice routing for the new SIP domain.
- Test connectivity by using the **Test-CsPstnOutboundCall** cmdlet.

Mediation Server Component

You must deploy Lync Server Mediation Server if you deploy the Enterprise Voice workload. This section describes basic functionality, dependencies, basic topologies, and planning guidelines.

The Mediation Server translates signalling and, in some configurations, media between your internal Lync Server, Enterprise Voice infrastructure and the SIP trunk. On the Lync Server side, Mediation Server listens on a single mutual TLS (MTLS) transport address. On the gateway side, Mediation Server listens on all associated listening ports associated with trunks defined in the Topology document. All qualified gateways must support TLS, but can enable TCP as well. TCP is supported for gateways that do not support TLS.

If you also have an existing Public Branch Exchange (PBX) in your environment, Mediation Server handles calls between Enterprise Voice users and the PBX. If your PBX is an IP-PBX, you can create a direct SIP connection between the PBX and Mediation Server. If your PBX is a Time Division Multiplex (TDM) PBX, you must also deploy a PSTN gateway between Mediation Server and the PBX.

The Mediation Server is collocated with the Front End Server by default. The Mediation Server can also be deployed in a stand-alone pool for performance reasons, or if you deploy SIP trunking, in which case the stand-alone pool is strongly recommended.

We also recommend that you co-locate the Mediation Server on a Front End pool when you have deployed IP-PBXs or connect to an Internet Telephony Server Provider's Session Border Controller (SBC), as long as any of the following conditions are met:

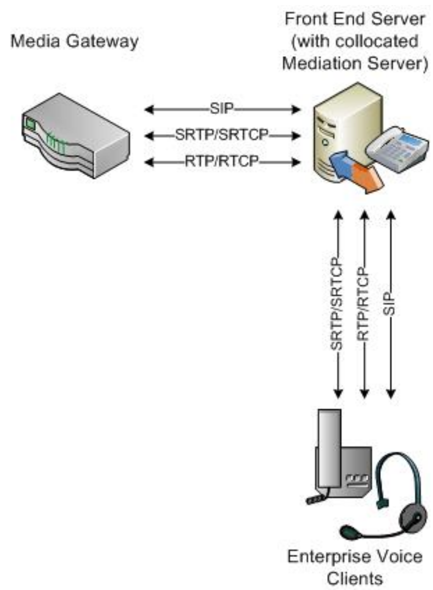
- The IP-PBX or SBC is configured to receive traffic from any Mediation Server in the pool and can route traffic uniformly to all Mediation Servers in the pool.
- The IP-PBX does not support media bypass, but the Front End pool that is hosting the Mediation Server can handle voice transcoding for calls to which media bypass does not apply.

You can use the Microsoft Lync Server Planning Tool to evaluate whether the Front End pool where you want to co-locate the Mediation Server can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

The main functions of the Mediation Server are as follows:

- Encrypting and decrypting SRTP on the Lync Server side
- Translating SIP over TCP (for gateways that do not support TLS) to SIP over mutual TLS
- Translating media streams between Lync Server and the gateway peer of the Mediation Server
- Connecting clients that are outside the network to internal ICE components, which enable media traversal of NAT and firewalls
- Acting as an intermediary for call flows that a gateway does not support, such as calls from remote workers on an Enterprise Voice client
- In deployments that include SIP trunking, working with the SIP trunking service provider to provide PSTN support, which eliminates the need for a PSTN gateway

The following figure shows the signalling and media protocols that are used by the Mediation Server when communicating with a basic PSTN gateway and the Enterprise Voice infrastructure.



Lync Server 2013 supports greater flexibility in the definition of a trunk for call routing purposes from previous releases. A trunk is a logical association between a Mediation Server and listening port number with a gateway and a listening port number. This implies several things: A Mediation Server can have multiple trunks to the same gateway; a Mediation Server can have multiple trunks to different gateways; conversely a gateway can have multiple trunks to different Mediation Servers.

A root trunk is still required to be created when a gateway is added to the Lync topology using Topology Builder. The number of gateways that a given Mediation Server can handle depends on the processing capacity of the server during peak busy hours. If you deploy a Mediation Server on hardware that exceeds the minimum hardware requirements for Lync Server 2013, then the estimate of how many active non-bypass calls a stand-alone Mediation Server can handle is approximately 1000 calls. When deployed on hardware meeting these specifications, the Mediation Server is expected to perform transcoding, but still route calls for multiple gateways even if the gateways do not support media bypass.

When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with that route. Instead, you use Topology Builder to associate trunks with Mediation Servers. In other words, routing determines which trunk to use for a call, and, subsequently, the Mediation Server associated with that trunk is sent the signalling for that call.

The Mediation Server can be deployed as a pool; this pool can be collocated with a Front End pool, or it can be deployed as a stand-alone pool. When a Mediation Server is collocated with a Front End pool, the pool size can be at most 12 (the limit of the Registrar pool size). Taken together, these new capabilities increase the reliability and deployment flexibility for Mediation Servers, but they require associated capabilities in the following peer entities:

- **PSTN Gateway.** A Lync Server qualified gateway must implement DNS load balancing, which enables a qualified public switched telephone network (PSTN) gateway to act as a load balancer for one pool of Mediation Servers, and thereby to load-balance calls across the pool.
- **Session Border Controller.** For a SIP trunk, the peer entity is the CBS Session Border Controller (SBC) in our voice network. In the direction from the Mediation Server pool to the SBC, the SBC can receive connections from any Mediation Server in the pool. In the direction from the SBC to the pool, traffic can be sent to any Mediation Server in the pool. One method of achieving this is through DNS load balancing, if supported by the service provider and SBC. An alternative is to give the service provider the IP addresses of all Mediation Servers in the pool, and the service provider will provision these in their SBC as a separate SIP trunk for each Mediation Server. The service provider will then handle the load balancing for its own servers. Not all service providers or SBCs may support these capabilities. Furthermore, the service provider may charge extra for this capability. Typically, each SIP trunk to the SBC incurs a monthly fee.
- **IP-PBX.** In the direction from the Mediation Server pool to the IP-PBX SIP termination, the IP-PBX can receive connections from any Mediation Server in the pool. In the direction from the IP-PBX to the pool, traffic can be sent to any Mediation Server in the pool. Because most IP-PBXs do not support DNS load balancing, we recommend that individual direct SIP connections be defined from the IP-PBX to each Mediation Server in the pool. The IP-PBX will then handle its own load balancing by distributing traffic over the trunk group. The assumption is that the trunk group has a consistent set of routing rules at the IP-PBX. Whether a particular IP-PBX supports this trunk group concept and how it intersects with the IP-PBX's own redundancy and clustering architecture needs to be determined before you can decide whether a Mediation Server cluster can interact correctly with an IP-PBX.

A Mediation Server pool must have a uniform view of the peer gateway with which it interacts. This means that all members of the pool access the same definition of the peer gateway from the configuration store and are equally likely to interact with it for outgoing calls. Therefore, there is no way to segment the pool so that some Mediation Servers communicate with only certain gateway peers for outgoing calls. If such segmentation is necessary, a separate pool of Mediation Servers must be used. This would be the case, for example, if the associated capabilities in PSTN gateways, SIP trunks, or IP-PBXs to interact with a pool as detailed earlier in this topic are not present.

Call Admission Control

Call admission control (CAC), first introduced in Lync Server 2010, manages real-time session establishment, based on available bandwidth, to help prevent poor Quality of Experience (QoE) for users on congested networks. To support this capability, the Mediation Server, which provides signalling and media translation between the Enterprise Voice infrastructure and a gateway or SIP trunking provider, is responsible for bandwidth management for its two interactions on the Lync Server side and on the gateway side. In call admission control, the terminating entity for a call handles the bandwidth reservation.

The gateway peers (PSTN gateway, IP-PBX, SBC) that the Mediation Server interacts with on the gateway side do not support Lync Server call admission control. Thus, the Mediation Server has to handle bandwidth interactions on behalf of its gateway peer. Whenever possible, the Mediation Server will reserve bandwidth in advance. If that is not possible (for example, if the locality of the ultimate media endpoint on the gateway side is unknown for an outgoing call to the gateway peer), bandwidth is reserved when the call is placed. This behaviour can result in oversubscription of bandwidth, but it is the only way to prevent false rings.

Configure your External Firewall

The settings configured on your firewall are unique to your firewall. You will be provided with the IP addresses and port and protocol configurations required to connect your firewall to CBS.

You must create multiple firewall rules. These rules allow inbound traffic from the CBS IP addresses to communicate with the gateway listening IP address of your Mediation Server. If your firewall restricts outbound communications as well, you need to allow the traffic to be two-way.

NB: The rules in the firewall apply to the external IP address assigned to the Pool Server or to the Lync Server Mediation Server network interface card (NIC). Depending on the configuration of your design, this may be a dedicated NIC or a shared NIC. Your firewall must support source network address translation (SNAT) and SIP proxy to perform network address translation of the external IP address of your Lync Server. The SIP proxy functionality rewrites the Session Description Protocol (SDP) packet allowing you to utilize a private IP on the Lync Server.

Modify and Publish your Lync Topology

Topology Builder is a Lync Server 2010 & 2013 tool that manages the components within your environment. By combining multiple Lync Mediation Servers with multiple CBS SIP trunks, a redundant solution can be built. For illustration purposes the example below shows a single gateway and route configuration.

- To open Topology Builder, click **Start**, click **All Programs**, click **Microsoft Lync Server**, and then click **Lync Server Topology Builder**.

Note: When configuring a Lync Pool, co-locating the Mediation Server is now an option with Lync Server 2013.

- Download an existing topology or create a new topology.
- Expand **Mediation pools** and select the Standard or Enterprise pool. Right-click the pool and select **Edit Properties**.
- Enable TCP by checking the **Enable TCP port** box, and then modify the **Listening ports value** from 5068 to 5060.
- CBS can send SIP communication over TCP/5060 or UDP/5060 but for Lync Server, TCP/5060 is preferred.
- This value enables the Mediation Server to open a listening port on the all interfaces on the Mediation Server (by default).
- Now select the **Mediation Server PTSN** gateway page; the PSTN gateways may be created as well.
- To display the **Define New IP/PSTN Gateway** dialog box, click **New.**
- Enter the IP address provided by CBS into **Gateway FQDN or IP Address**, select the SIP Transport Protocol; either **TCP** or **TLS** depending on your chosen configuration (standard or encrypted trunks) and then enter 5060 as the **Listening port**.
- Click **OK** to save the configuration.
- Click **OK** again to close the Mediation pool properties.

Note: A new PSTN gateway with the FQDN or IP Address entered in the previous step will automatically be displayed under PSTN gateways.

- After completing the addition of the configuration changes, the topology must be published.
- Select **Lync Server**, right-click and select **Publish** topology.
- In the **Publish Topology** dialog box, click **Next**.
- After publishing is complete, review the status provided and then click **Finish** to complete the process.

Create a Route in the Lync Server Control Panel

After the topology is updated, define a route in the Lync Server Control Panel. This document assumes you have a working Lync Server environment i.e. Lync Server is functioning internally and externally with the exception of Enterprise Voice.

- Launch the Lync Server Control Panel on the server or from Internet Explorer at https://<poolnameFQDN>/cscp (ex. https://lyncpool.contoso.com/cscp).
- Click on **Voice Routing**, and then click **Trunk Configuration** and select **NEW Pool Trunk**
- Set Encryption level as per your topology
  - **Not Supported** for standard trunks
  - **Required** for encrypted trunks
- Enable **Refer Support**
- Click the **Commit** drop-down menu, and then **Commit All**
- Now select **Route**.

- By default, a route named **LocalRoute** is listed. Select the route**,** click **Edit**, and then click **Delete**.
- Click **New** to create a new route.
- Enter a name in the route, such as Internet SIP Trunk, and an optional description.
- Scroll down to **Build a Pattern to Match**, and notice the default is set to '*.' - or all calls.
- The associated gateways list defines which PSTN gateways are defined in the Lync Server Topology Builder.
- Click **Add** to display the list.
- Select the previous defined gateway, and click **OK**.
- Under associated **PSTN Usages**, click Select to open the **Select PSTN Usage Record** dialog box.
- Select **Long Distance** from the list and click **OK**.
- Click **OK** to complete the creation of the new route.
- To finalize the changes, click **Commit**, and click **Commit All**.
- Click Commit at the Uncommitted Voice Configuration Settings followed by clicking Close.

Create a Dial Plan to Route Outbound Calls to Your SIP Trunk

In a pure Internet SIP trunk configuration, creation of a dial plan to CBS is simple and straightforward. All calls routed through the trunk must be in the international E.164 number format. Formatting is automated by the normalisation rules found in the Dial Plans. You may change or create additional Dial Plans, and normalise those rules to match your environment.

- Click **Dial Plan** to display the current dial plans in the environment.
- Double-click the **Global Dial Plan** to open the dial plan properties.
- Scroll down to the **Associated Normalization Rules**.
- The **Prefix All** rule, which adds a '+' to all 11-digit numbers, is present by default.
- It must be removed to create three new rules.
- Select **Prefix All**, and click **Remove**.
- Click **New** to open the **New Normalization Rule** window.
- Enter a name in the rule, such as 7-Digit Dialling for local numbers, and an optional description.
- Scroll down to **Length**, select **Exactly** from the drop-down box, and then enter 7 in the **Value** box.
- In **Digits** to add, enter the local area code with a +1 (e.g. +1868)
- Click **OK** to complete the creation of the normalization rule.
- The new rule is now listed in the rules list.
- Repeat the process to create two additional rules labelled 10-Digit Dialling and 11-Digit Dialling with the following properties:
    - Name: 10-Digit Dialling Plan
    - Length: Exactly, 10
    - Digits to add: +1

- Name: 11-Digit Dialling Plan
    - Length: Exactly, 11
    - Digits to add: +

- After the required normalization rules are created, click **OK** to complete the Dial Plan.
- Click **Commit**, and then select **Commit All** to save the normalisation rules.
- Click **Commit** again, and then click **Close** to complete the changes.
- Click **Voice Policy** to update the **Global** policy.
- Double-click **Global** to open the **Edit Voice Policy - Global** window.
- Scroll down to **Associated PSTN Usages**, and click **Select**.
- Select **Long Distance** from the **Select PSTN Usage Record** dialog box, and then click **OK**.

  Note: Notice the **Long Distance PSTN** usage record is associated with the newly created **Internet SIP** trunk route -the glue that ties the route to the policy.

- Click **OK** to close **Voice Policy**, click **Commit**, and then click **Commit All** to open the **Uncommitted Voice Configuration Settings** dialog box.
- Click **Commit**, and then click **Close** to complete the changes.
- When configuration is complete, validation is performed using the Lync Server **Control Panel**. At the top of the current window, select the down arrow to display the test case.
- In the **Dialled Number** box, enter 7, 10, or 11 digits, and then verify the normalisation rule works as expected.
- The **Results** dialog box will indicate which **Normalized Rule**, **Normalized Number**, **First PSTN Usage**, and **First Route** will be used when presented with the test number.

  Note: All numbers (local or long distance) will use the **Long Distance PSTN Usage** in this current setup. PSTN usages are used to add calling restrictions and are not used in this example configuration.

Enable Users for Enterprise Voice

The final configuration step requires that users are enabled and configured with a unique Line URI. The Direct Inward Dialing (DID) numbers, provided by CBS, must be directly associated with the user accounts' **Line URI Enterprise Voice** properties within Lync Server **Control Panel**.

Inbound communications are received in the E.164 format, so inbound call manipulation does not occur. When inbound calls are received, an automatic phone number lookup, based on the line URI of the user account is performed. If there is a match, the Mediation Server routes the call appropriately.

- Click **Users** in the Lync Server **Control Panel** to change to the users' configuration.
- The **User Search** window is blank until a query is made and results found.
- By clicking **Find** without any input, all enabled users are returned in the query.
- Double-click a user to edit the properties of the user.
- Select the **Telephony** drop-down box and pick **Enterprise Voice**.
- In the Line **URI** field, type the DID that you want to use in the E.164 format.

- This format starts with a plus sign (+) followed by the country code, area code, and phone number (e.g. +1868XXXXXXX).
- Click **Commit** to complete the changes.
- Wait for domain replication to occur.
- After the object properties replicate through Active Directory Domain Services, the system is ready for inbound and outbound test calls.

Troubleshooting Tools

1. Microsoft Network Monitor (NetMon)

NetMon is a network protocol analyser 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.

2. Wireshark

Wireshark is also a network protocol analyser 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.

3. Event Viewer

There are several locations in the event viewer where you can find valuable information to aid in troubleshooting issues with your deployment. With the requirement that there is a completely functioning Lync Server with Enterprise Voice deployment in place, there are a few areas in which one would use the Event Viewer for troubleshooting:

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

4. Lync Server Logging Tool

The Lync Server Logging Tool provides internal traces and messaging between different Lync Server elements like Front-end, Mediation server, Lync Clients, etc. The tool will need to be installed on all the Lync server components and can be downloaded from Microsoft website at http://www.microsoft.com/en-us/download/details.aspx?id=21165. File name is OCSReskit.msi. Once installed, it can be accessed from any one of the Lync Server servers by running Start/All Programs/Microsoft Lync Server/Lync Server Logging Tool.