



Microsoft Lync and Cisco Expressway

Deployment Guide

Cisco Expressway X8.5
Microsoft Lync 2010, Lync 2013

September 2015

Contents

Introduction	5
Objectives and intended audience	5
Deployment scenario	5
Clustered "Lync gateway" Expressway	6
Why add a "Lync gateway" Expressway?	7
Features and capabilities	8
Client support	9
Interoperability with different versions of Lync Server	9
Microsoft Lync B2BUA interoperating capabilities	9
Summary of configuration objectives	10
Lync environments	10
Prerequisites prior to configuring Expressway and Lync to interoperate	14
Check that calls between Lync clients registered on Lync Server operate as expected	15
Unified CM configuration	15
Enabling users for Lync	15
Registering Lync clients to the Lync Server	17
Lync client configuration	17
Testing the configuration	18
Enabling endpoints registered on the video network to call clients registered on Lync	19
Video network: Unified CM configuration	19
Prerequisites	19
Configuring the SIP Profile for Expressway	19
Configuring the region with an appropriate session bit rate for video calls	22
Configuring the SIP Trunk security profile	22
Configuring the SIP Trunk device	23
Configuring the clusterwide domain enterprise parameters	26
Allowing dialing to Expressway domain from Cisco phones	27
Checking the message size limit on Unified CM	28
"Lync gateway" Expressway configuration (part 1)	28
"Lync gateway" Expressway: Load CA certificate and server certificate (if using TLS to Lync)	29
"Lync gateway" Expressway: Configure DNS and local hostname	29
"Lync gateway" Expressway: Ensure that cluster name is configured	30
"Lync gateway" Expressway: Configure an NTP server	30
"Lync gateway" Expressway: Ensure that TLS is enabled in SIP configuration	31
Lync Server configuration	31
Trust a "Lync gateway" Expressway	31
Configure Lync Server media encryption capabilities	33
"Lync gateway" Expressway configuration (part 2)	34
Configure the B2BUA on the "Lync gateway" Expressway	34
Set up a search rule to route calls to the Lync domain to Lync	35
Set up search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync	37
Testing the configuration	37
Enabling Lync clients registered on Lync Server to call endpoints registered on the video network	38
"Lync gateway" Expressway configuration	38

Configuring the B2BUA trusted hosts on the “Lync gateway” Expressway	38
Configuring the “Lync gateway” Expressway with a neighbor zone that contains the video network	39
Creating a search rule to route calls to the Unified CM neighbor zone	41
Creating a transform to strip port information from URIs	43
Configuring Lync Server domain static routes	44
Configuring static routes to route calls to the “Lync gateway” Expressway	44
Testing the configuration	45
Enabling Microsoft Edge Server and Expressway TURN capabilities	46
Connecting Expressway to Unified CM using TLS	47
Ensuring certificate trust between Unified CM and Expressway	47
Loading server and trust certificates on Expressway	47
Loading server and trust certificates on Unified CM	48
Configuring a SIP trunk security profile on Unified CM	48
Updating the Unified CM trunk to Expressway to use TLS	49
Updating the Expressway neighbor zone to Unified CM to use TLS	49
Verifying that the TLS connection is operational	50
Network of Expressways	50
Encrypted calls to endpoints registered to Unified CM	50
Appendix 1: Federation	51
Solution overview	51
Configuring the directory Expressway	52
Modifying the Lync static route configuration	53
Appendix 2: Troubleshooting	54
Troubleshooting checklist	54
Check for errors in the Event Log	54
Tracing calls	54
Video endpoint reports that it does not support the Lync client SDP	54
TLS neighbor zone to Lync Server is active and messaging is sent from Expressway to Lync Server, but Lync debug says Lync fails to open a connection to Expressway	55
Lync client initiated call fails to connect	55
Lync responds to INVITE with ‘488 Not acceptable here’	55
Call connects but clears after about 30 seconds	55
Media problems in calls involving external Lync clients connecting via an Edge server	56
One way media: Lync client to Expressway-registered endpoint	57
Lync rejects Expressway zone OPTIONS checks with ‘401 Unauthorized’ and INFO messages with ‘400 Missing Correct Via Header’	57
Lync client stays in ‘Connecting ...’ state	58
Call to PSTN or other devices requiring caller to be authorized fails with 404 not found	58
Lync clients try to register with Expressway-E	58
B2BUA problems	58
B2BUA Lync Server status reports “Unknown” or “Unknown failure”	58
Lync problems	58
Problems with certificates	59
Appendix 3: Debugging on Lync	60
Use of Lync Server Logging Tool	60
Enabling debug on Lync client	61
Appendix 4: Interoperating capabilities and limitations	62

Known interoperating capabilities	62
Upspeeding from a voice call to a video call	62
Maximum call resolution	62
Known interoperating limitations	62
Video codecs	62
MXP endpoints	62
Joining a Lync conference (AV MCU)	62
Upspeeding from a voice call to a video call	63
Microsoft Mediation Server	63
Lync client reports no audio device	64
Appendix 5: Port reference	65
Appendix 6: Media paths and license usage for calls through B2BUA	67
Lync client call to SIP video endpoint	67
An external Lync client calls an internal SIP video endpoint	68
Appendix 7: Additional information	69
TEL URI handling for Expressway to Lync calls	69
Document revision history	70

Introduction

Objectives and intended audience

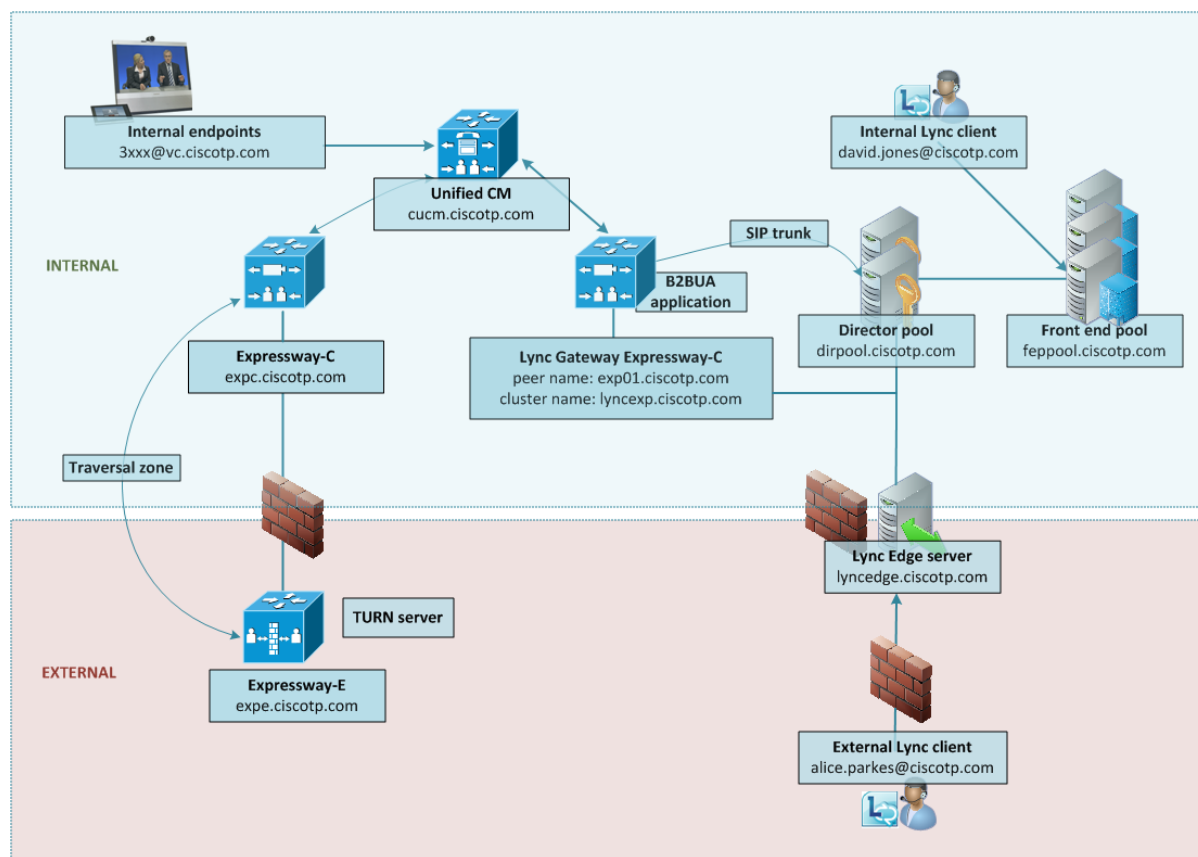
This deployment guide describes how to configure a Cisco Expressway (Expressway) using the Back-2-Back-User-Agent (B2BUA) and Microsoft Lync 2010 / 2013 (Lync) to interwork.

It also highlights the capabilities and limitations of interoperation of Expressway and Lync.

Deployment scenario

A company is introducing a Lync environment into their network and is installing Microsoft Lync clients to provide messaging and presence capabilities for all staff. Integrating this with their existing video network, which handles their video conferencing, provides the ability for video endpoints to make calls to and receive calls from Lync clients.

This deployment guide uses the example environment depicted below:



This guide describes how to configure:

- static routes to route calls from Lync to a "Lync gateway" Expressway
- the Expressway B2BUA to route calls to Lync
- a SIP trunk between the "Lync gateway" Expressway and Unified CM

The basic configuration environment consists of the following elements:

Lync deployment with:

- a pool of Front End Processors with FQDN feppool.ciscotp.com
- a pool of Directors with FQDN dirpool.ciscotp.com
- an Edge server with FQDN lyncedge.ciscotp.com
- users david.jones@ciscotp.com and alice.parkes@ciscotp.com (among others)

Cisco video deployment with:

- Lync gateway Cisco Expressway-C (referred to as the "Lync gateway" Expressway) with peer FQDN exp01.ciscotp.com and cluster FQDN lyncexp.ciscotp.com. The cluster FQDN must resolve to a list of DNS A-records including the IP addresses of all cluster peers (for round-robin operation).
- Unified CM with FQDN cucm.ciscotp.com
- Cisco Expressway-C with FQDN expc.ciscotp.com and Cisco Expressway-E with FQDN expe.ciscotp.com for TURN server support
- Internal video endpoints for video users david.jones and alice.parkes

In this scenario, dialing is typically carried out by users clicking on one of their buddies in the Lync contact list or by selecting a destination from an electronic address book on the video endpoint.

This guide describes how to connect Lync and a Unified CM via a "Lync gateway" Expressway using a SIP trunk across an IP network and static routes from Lync to the "Lync gateway" Expressway. The example presented uses the following setup:

- A Unified CM (or cluster of Unified CM peers) – the "Lync gateway" Expressway – to act as the link between the existing video network and Lync.
- The Lync's SIP domain is ciscotp.com. The SIP domain for Lync need not be the same as the AD domain of Lync clients (the Lync login domain used in the login user name may be different from the SIP domain used in the sign-in address).
- The Cisco video network's domain is vc.ciscotp.com (used for video device registrations).
- Endpoints registered to the video network are provisioned by Unified CM and register with a DN in the format 3xxx.
- Lync clients registered to Lync are identified by URIs, for example:
 - David with a URI david.jones@ciscotp.com
 - Alice with a URI alice.parkes@ciscotp.com
- Lync Front End Server is configured with a static domain route which routes URIs with the Expressway's video network domain (vc.ciscotp.com) to the Expressway. Care must be taken when using domain static routes; any traffic for that domain that Lync cannot handle locally will be routed to Expressway.

Clustered "Lync gateway" Expressway

When this document refers to a "Lync gateway" Expressway, a cluster of Expressways can also be used. The operation is functionally the same, but there is more capacity available.

Calls from Lync Server will typically arrive at a single Expressway in the cluster, as Lync Server will use the static domain routes, which has a single IP address for TCP connectivity and a single FQDN for TLS connectivity.

If you use a DNS A record to map the peers' IP addresses to the FQDN of the cluster, the DNS server typically returns the IP addresses in a different order each time the Lync Server queries DNS (round-robin).

The Lync Server selects one IP address to use, based on its own logic (outside of this document's scope). If the TTL of the record has not expired when the Lync Server makes a new DNS query, the Lync Server will use the same IP address it used the previous time. If the Lync Server cannot connect to the IP address it selected, it will try another of the IP addresses returned by the DNS server.

Why add a “Lync gateway” Expressway?

The “Lync gateway” Expressway is an interface between an existing working video network and the Microsoft Lync environment. Using this gateway minimizes the changes that need to be made in the video network so as to introduce as few artifacts as possible when adding Lync interoperability to the video network.

Having dedicated Expressways for this “Lync gateway” operation limits the number of Expressways for which the **Microsoft Interoperability** option key needs to be purchased and enabled.

Lync Server can only send calls to a single FQDN (though this may have a round robin DNS address to support a cluster of Expressways for resilience) for calls via a static domain route defined in Lync Server.

Lync Server will only accept messages received from peers that it has been configured to trust. Having a dedicated “Lync gateway” Expressway or Expressway cluster also limits the number of trusted devices that need to be configured in Lync, as every device that sends SIP messages to Lync Server needs to be explicitly listed as a trusted host in Lync Server.

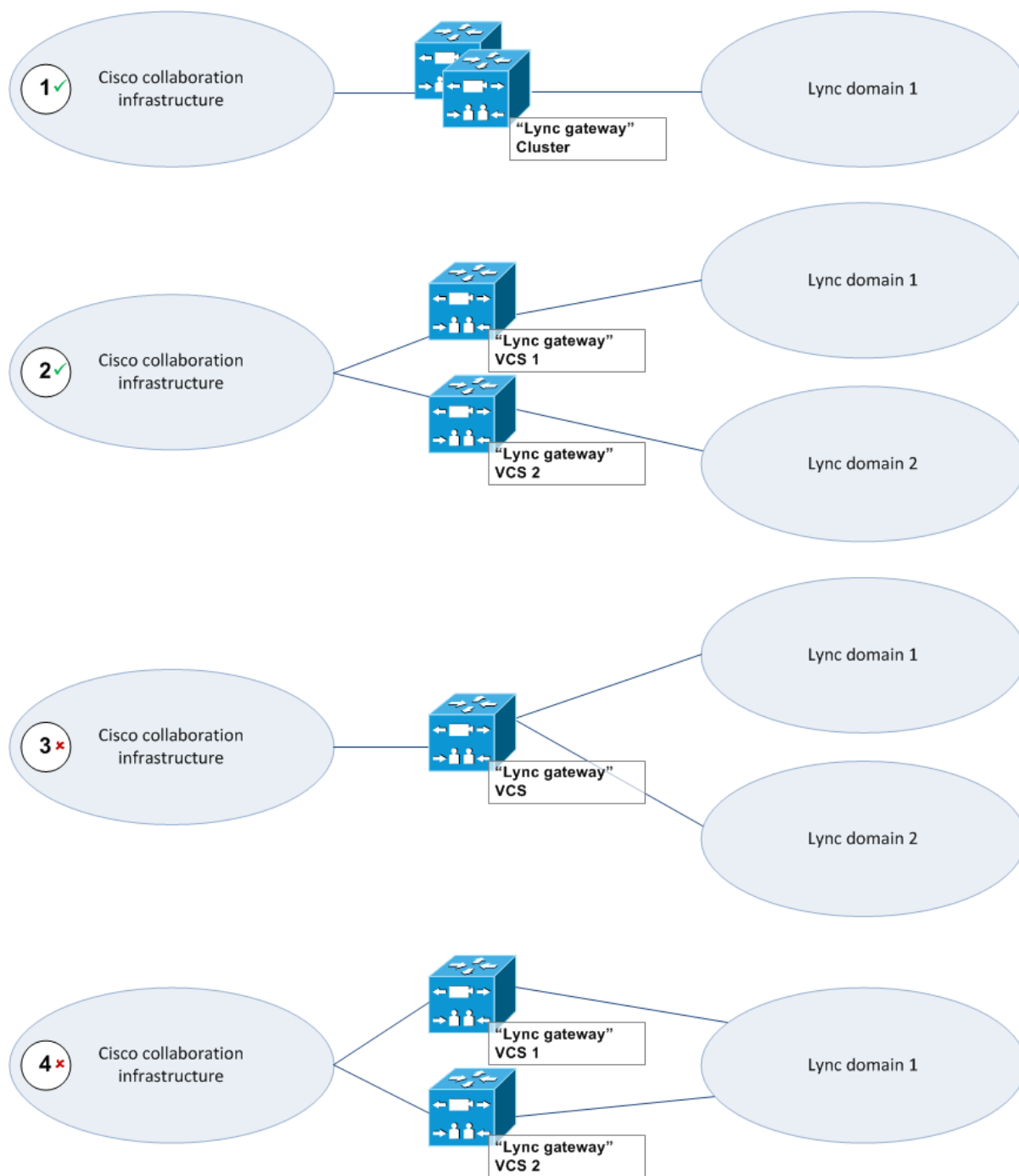
Multiple Lync domains and relationships to multiple Lync gateway Expressway

You can integrate Cisco collaboration infrastructure with more than one Lync domain if required, but you need to set up a “Lync gateway” Expressway into each Lync domain. Wherever you put a single Expressway as a gateway, you could use a cluster instead.

Take care when you design your deployment that you don't have more than one gateway per Lync domain, or more than one Lync domain per gateway. See the diagram below which shows the following different options:

1. This option is used in this document; there is one gateway Expressway (or cluster) into a single Lync domain.
2. It is possible to configure multiple Lync domains, provided you have an independent gateway serving each. This option is not exhaustively tested, nor is it described in this document.
3. You cannot configure multiple Lync domains with only one Lync gateway Expressway serving all of them.
4. You should avoid configuring multiple gateways to serve one Lync domain. With this deployment, calls from one video endpoint to another video endpoint that is called via its Lync domain will get routed via Lync rather than directly through the collaboration infrastructure; users could lose duo video, far end camera control, and possibly encryption and video quality.

Figure 1: Lync gateway Expressway deployment options, showing potential misconfigurations



Features and capabilities

Expressway X8.1 or later is compatible with Lync 2010 and Lync 2013 clients, registered to Lync 2010 or Lync 2013 front end servers.

Client support

Expressway is generally compatible with Lync 2010 and Lync 2013 clients, including mobile clients. When specific issues are discovered, they are recorded on the [TelePresence Interoperability database](#).

Interoperability with different versions of Lync Server

The known differences in interoperability when Expressway integrates with Microsoft Lync Server 2013 or Lync Server 2010 are summarized below:

Microsoft Lync Server 2010

The **Microsoft Interoperability** option key must be installed to enable encrypted calls to and from Microsoft Lync 2010 Server (for both native SIP calls and calls interworked from H.323). It is also required by the B2BUA when establishing ICE calls to Lync 2010 clients.

The B2BUA can use the Cisco AM GW to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio to allow high definition calls between Microsoft Lync 2010 clients and Cisco endpoints.

Microsoft Lync Server 2013

The B2BUA provides interworking between standard H.264 AVC and Lync 2013's H.264UC SVC codec. You can still configure the B2BUA to use Cisco AM GW transcoders with Lync 2013, but it is not necessary and we recommend that they are not deployed with Lync 2013.

Lync 2013 no longer supports H.263, so X8.1 or later software is required to interoperate successfully with Lync 2013.

The **Microsoft Interoperability** option key is required for all types of communication with Lync 2013.

Microsoft Lync B2BUA interoperating capabilities

When using the Microsoft Lync B2BUA:

- Domain static routes are set up on Lync Server to route calls to domains in the video network.
- Search rules are set up on Expressway to route calls to Lync domains.
- Lync Server accepts and handles call hold (and resume) requests.
- Lync clients can be the object of a transfer (even if there is an AM gateway involved in the call).
- Calls to Microsoft Mediation Servers work from endpoints in the Expressway video network for SIP initiated calls, but do not work for calls interworked from H.323 (unless the workaround specified in [Appendix 4: Interoperating capabilities and limitations \[p.62\]](#) is implemented).
- Lync systems may use hardware load balancers for resilience and capacity.
- A “Lync gateway” Expressway (or Expressway cluster) can communicate to Lync via Lync Director.
- Media encryption (SRTP) is supported when TLS is used between Expressway and Lync and the **Microsoft Interoperability** option key is added to the “Lync gateway” Expressway.
- SIP signaling and RTP media is always routed via the B2BUA application for calls involving Lync clients. Each B2BUA application (one application per Expressway) can handle 100 simultaneous calls between Lync and the Expressway video environment. However, a call involving Cisco AM GW will consume two B2BUA call resources.

Summary of configuration objectives

This document describes how to configure Lync and the Expressway in B2BUA mode to enable calls from:

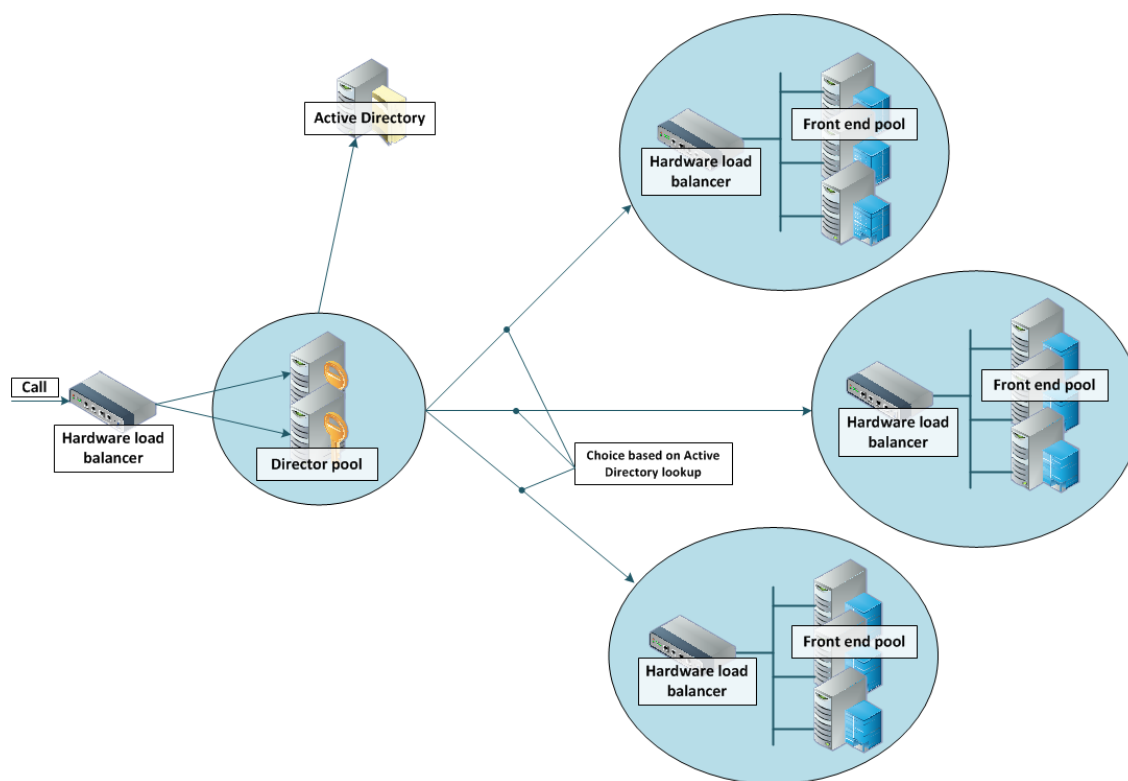
- Microsoft Lync clients registered on Lync Server to other Lync clients registered on that Lync Server.
- SIP video endpoints registered to Unified CM in the video network to Lync clients registered on Lync.
- Lync clients registered on Lync Server to video endpoints registered in the video network.

Lync environments

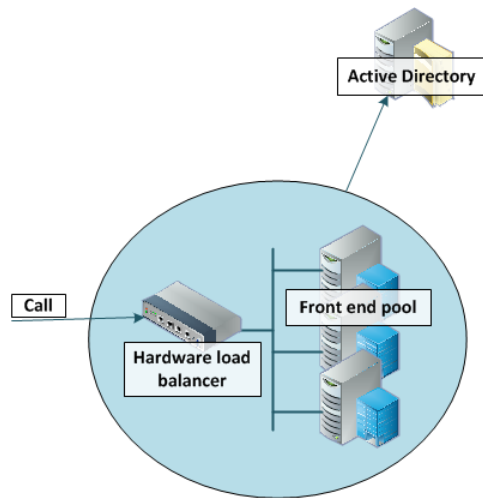
Lync environments have a number of building blocks, and so they may be constructed in many ways. A full scale Lync deployment is likely to use Lync Director, Hardware Load Balancers (HLBs), Front End Processors (FEPs) in enterprise pools, and a redundant AD server.

For Lync installations, Microsoft recommend that DNS may be used in place of hardware load balancing for routing SIP traffic. Microsoft guidance can be found at <http://technet.microsoft.com/en-us/library/gg398634.aspx>.

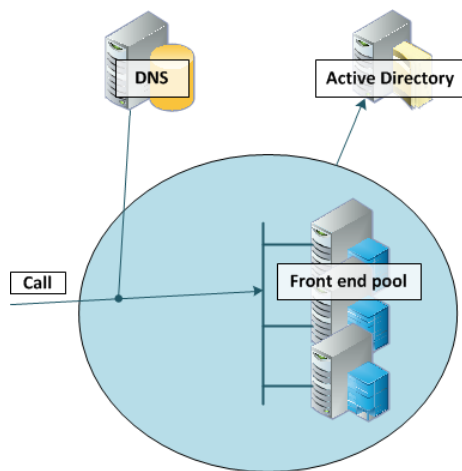
An example architecture is shown below:



A smaller deployment may not use Lync Director servers, but may just use a Hardware Load Balancer in front of a set of Front End Processors.

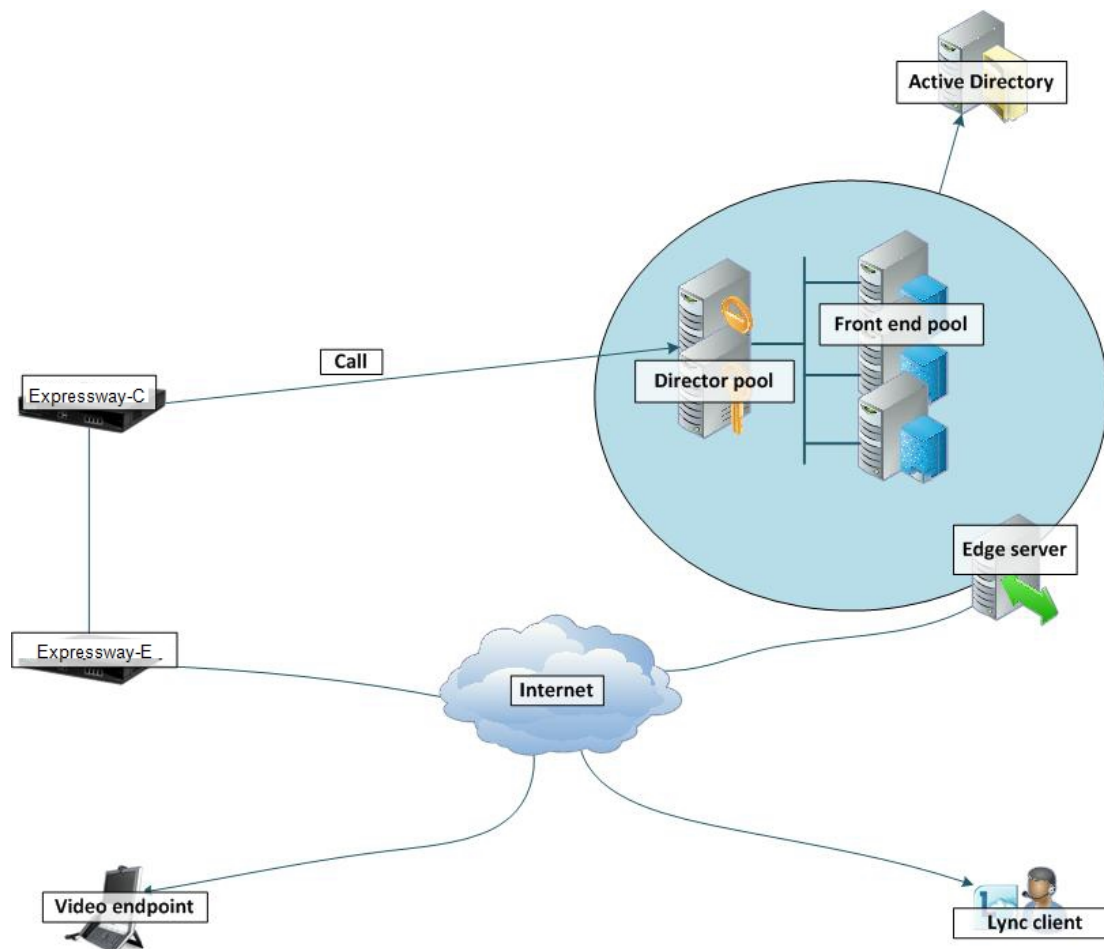


A Lync environment may use DNS instead of the Hardware Load Balancer, for example:



Note that Lync requires that the AD server and FEP are on separate machines.

Lync deployments may also contain Edge servers to allow Lync clients to register from outside the local network through the Edge server to Lync. Communicating with Lync devices outside the edge server requires both the Edge Server and the Expressway-E connecting to the public Internet. (Calls involving a Microsoft Edge server require the Expressway to have the **Microsoft Interoperability** option key installed, as this key allows for ICE to be used for media connectivity, which is required in the following scenario.)



In any deployment with Expressway and Lync:

- In Lync, traffic sent via a static SIP route is either sent directly from a FEP to the Expressway, or from a FEP via a Director and to the Expressway.
- If the Lync environment is fronted by a Hardware Load Balancer in front of Lync Directors then calls to and from the video network will go via the Directors; they will not be routed directly to or from the FEPs:
 - Lync Directors should trust the “Lync gateway” Expressway(s).
 - Lync Directors should route the video network domain (vc.ciscotp.com) to the “Lync gateway” Expressway cluster FQDN.
 - Depending on Lync configuration, FEPs may route SIP traffic directly to the Expressway, or they may route the traffic through a Director pool.
- If the Lync environment is fronted by a single Lync Director then calls to and from the video network will go via that Director; they will not be routed directly to or from the FEPs:
 - Lync Directors should trust the “Lync gateway” Expressway(s).
 - Lync Directors should route the video network domain (vc.ciscotp.com) to the “Lync gateway” Expressway cluster FQDN.

- Depending on Lync configuration, FEPs may route SIP traffic directly to the Expressway, or they may route the traffic through a Director pool.
- If the Lync environment has no Lync Director but a Hardware Load Balancer in front of Front End Processor pool(s) then configure the pool(s) (not each FEP):
 - The FEP pools should trust the “Lync gateway” Expressway(s).
 - All FEP pools should route the video network domain (vc.ciscotp.com) to the “Lync gateway” Expressway cluster FQDN.Configuring the pool ensures that the same configuration is applied to every FEP in the pool.
- If Lync is a single FEP then that FEP should be configured:
 - The single FEP should trust the “Lync gateway” Expressway(s).
 - The single FEP should route the video network domain (vc.ciscotp.com) to the “Lync gateway” Expressway cluster FQDN.

We recommend that you use a Expressway cluster FQDN (e.g. lyncexp.ciscotp.com) rather than an individual Expressway peer (even if it is a "cluster" of one). If you configure a Trusted Application Pool (Cluster FQDN), you can always add peer FQDNs (Expressway peers) to the Application pool later without requiring to remove the existing search rules, static routes or Trusted Applications in the Lync Server.

“Lync gateway” Expressway should be configured such that:

- If the Lync environment is fronted by a Hardware Load Balancer in front of Lync Directors then the B2BUA should be configured to route calls for Lync to the Hardware Load Balancer, and receive calls from either of the Lync Directors:
 - The “Lync gateway” B2BUA needs to specify the Hardware Load Balancer as the Lync signaling destination address.
 - The “Lync gateway” B2BUA needs to include the addresses of both Lync Directors as trusted hosts (and any FEPs which might send traffic directly to the B2BUA).
 - Search rules that route calls to Lync will target the B2BUA neighbor zone.
- If the Lync environment is fronted by a Lync Director or a pool of directors, then the B2BUA should be configured to route calls for Lync to the Lync Director, and receive calls from the Lync Director:
 - The “Lync gateway” B2BUA needs to specify the Lync Director (pool) as the Lync signaling destination address.
 - The “Lync gateway” B2BUA needs to include the address of each individual Lync Director as a trusted host (and any FEPs which might send traffic directly to the B2BUA).
 - Search rules that route calls to Lync will target the B2BUA neighbor zone.
- If the Lync environment has no Lync Director but a Hardware Load Balancer in front of Front End Processors then the B2BUA should be configured to route calls for Lync to the Hardware Load Balancer, and receive calls from any of the FEPs:
 - The “Lync gateway” B2BUA needs to specify the Hardware Load Balancer as the Lync signaling destination address.
 - The “Lync gateway” B2BUA needs to include the addresses all of the Lync FEPs as trusted hosts.
 - Search rules that route calls to Lync will target the B2BUA neighbor zone.
- If Lync is a single FEP then the B2BUA should be configured to route calls for Lync to the single FEP directly, and receive calls from that FEP:
 - The “Lync gateway” B2BUA needs to specify the FEP as the Lync signaling destination address.
 - The “Lync gateway” B2BUA needs to include the address of the FEP as a trusted host.
 - Search rules that route calls to Lync will target the B2BUA neighbor zone.

Prerequisites prior to configuring Expressway and Lync to interoperate

Before configuring the video network and the Lync environment to interwork, make sure that:

- The “Lync gateway” Expressway (cluster peers) are running X8.1 code (or later)
- The “Lync gateway” Expressway (cluster peers) have a rich media sessions option key applied.
- The version of Lync is Lync 2010 or Lync 2013.
- Lync is configured and operational and access is available to Active Directory for managing users.
- The FQDN of all Lync servers is resolvable via the DNS server that the “Lync gateway” Expressway is configured to use (this should be the DNS server used by Lync).
- The FQDNs of each of the “Lync gateway” Expressways and if clustered, the FQDN of the “Lync gateway” cluster must be resolvable via DNS (with round-robin A-records).
- Validation of the Front End Servers on all Lync Directors and Lync FEPs must show no errors. Use the Topology Validation Tool which can be found in the Lync Resource Toolkit.
- If TLS is to be used (recommended) ensure that the DNS server supports reverse DNS lookup (often supported using PTR records).

Check that calls between Lync clients registered on Lync Server operate as expected

The configuration described in this section should already be in place and operational.

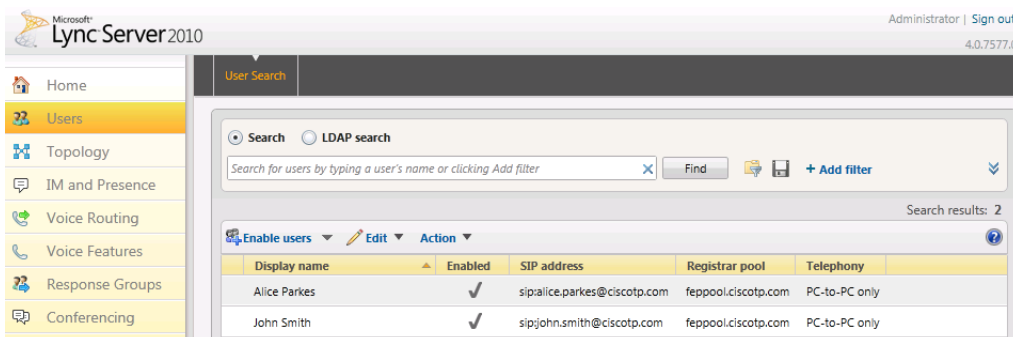
Unified CM configuration

No configuration is required on Unified CM for endpoints registered on Lync to call other endpoints registered on Lync Server.

Enabling users for Lync

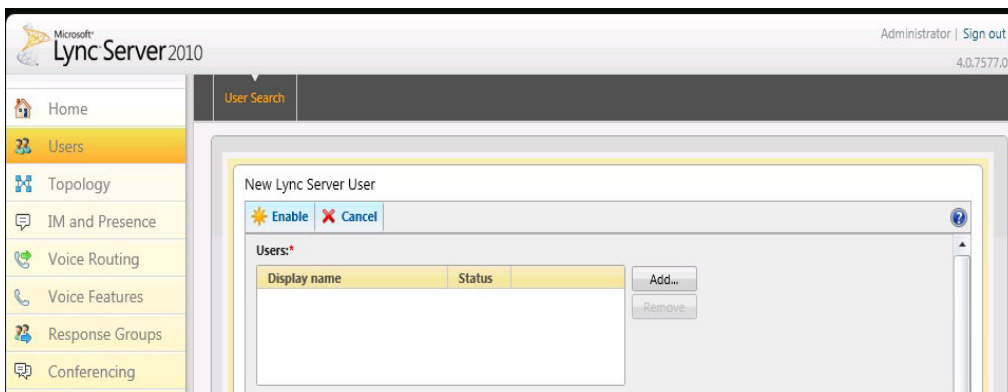
By default, Active Directory users are not Lync enabled. Check that users required to support Lync are enabled to do so, and if not enable them. This can be done both by Lync Server Control Panel or through Windows PowerShell commands (using Lync 2010 as an example):

1. Bring up the Lync Server Control Panel (either from the start menu select Lync Server Control Panel, or if there is a desktop icon double click it).
2. On Lync Server Control Panel go to the **Users** menu: you can see users already enabled for communication server.

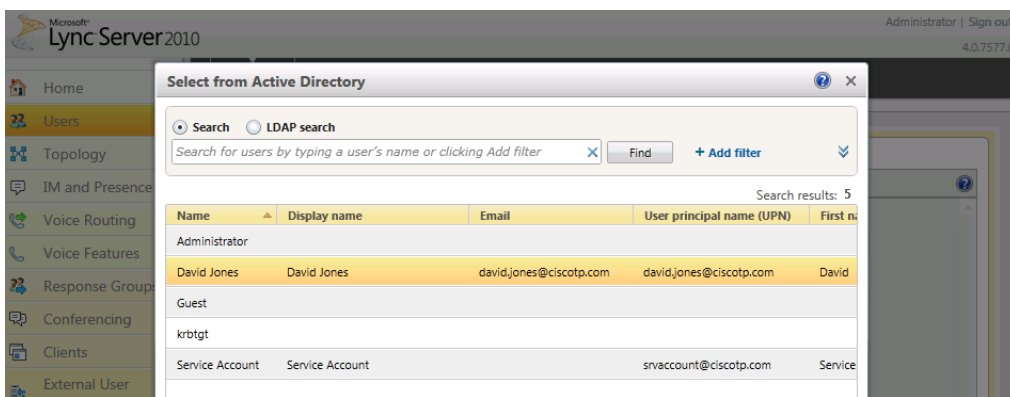


To add a new user:

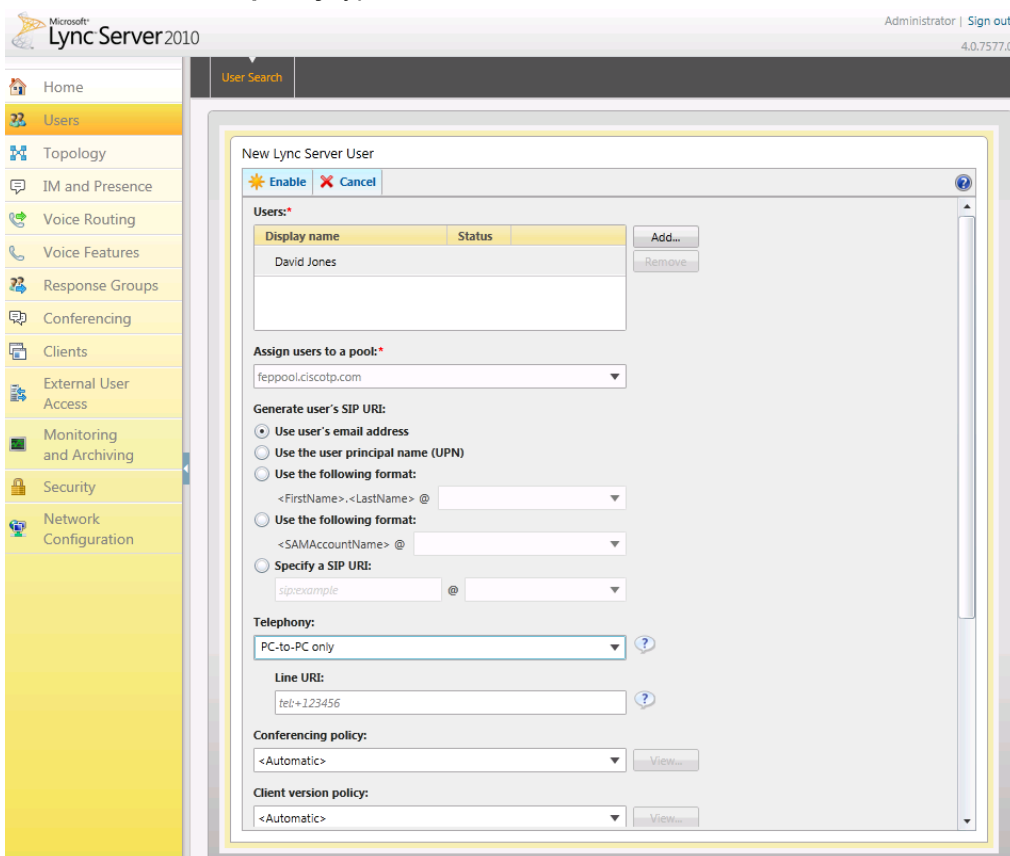
1. Select **Enable users** and click **Add**.



2. Search for and select the user (in this example, David Jones)
Note: to find the user it must already have been defined in Active Directory.



3. Select the communication server pool to assign to the user.
4. Select your preferred method to **Generate user's SIP URI**.
5. Select the user's **Telephony** type.




This can be done in single command by CSPS using the command “**enable-csuser**”

For example:

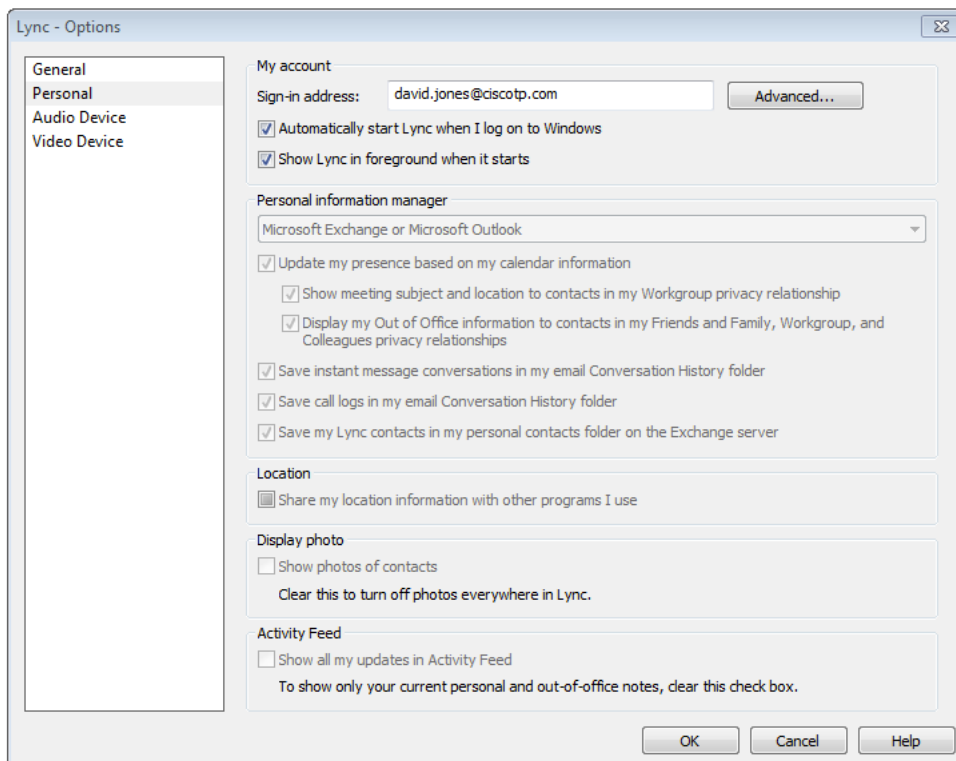
```
enable-csuser -identity "ciscotp\david.jones" -registrarpool
"feppool.ciscotp.com" -sipaddress sip:david.jones@ciscotp.com
```

Registering Lync clients to the Lync Server

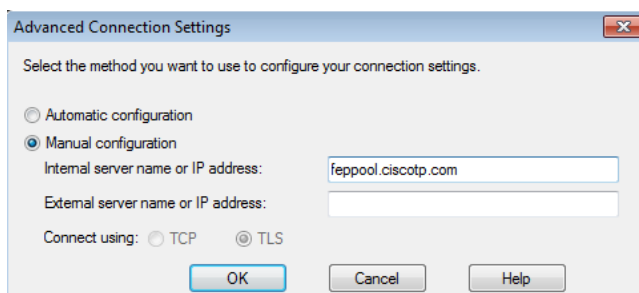
Lync client configuration

1. Install and start the Lync client.
2. On the Sign in screen, click on the  icon or select the menu arrow beside it and select **Tools > Options**.
3. Select **Personal**.
4. Set up **Sign-in address** as required.

This is the SIP URI of the Lync user, for example david.jones@ciscotp.com:

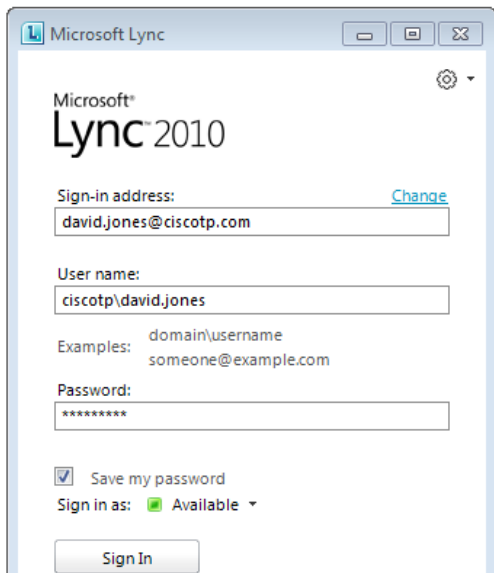


5. Click **Advanced**.

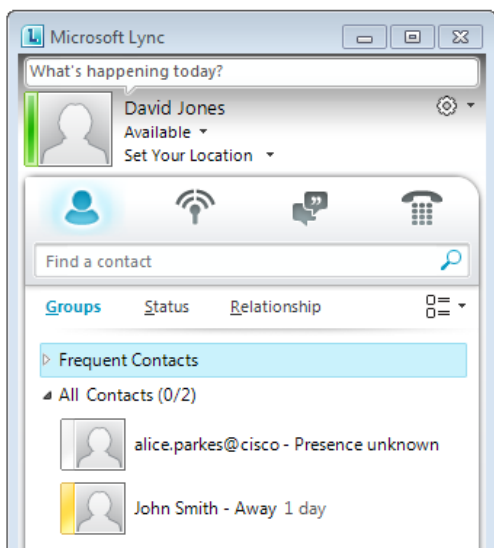


6. In a production environment ensure *Automatic configuration* is selected.
If this does not work, select *Manual configuration* and set **Internal server name or IP address** to the FQDN of the Lync Server.
7. Click **OK** to return to the **Lync - Options** panel.
8. Click **OK** to return to the Lync client.

9. Click **Sign In**.
10. Enter the **User name** and **Password**.
This is the Active Directory name and password of the user. The user name may or may not be the same as the sign in address. Depending on how the network is configured, the **User name** may need to be in the form <domain>\<user> rather than <user>@<domain> for example ciscotp\david.jones instead of david.jones@ciscotp.com.



11. Click **Sign In**.



Testing the configuration

To make a video call between Lync endpoints:

1. Double-click on the buddy you want to call.
2. Click **Start a Video Call**.
3. Answer the call on the receiving Lync client.

Enabling endpoints registered on the video network to call clients registered on Lync

This is configured in 4 stages:

1. Video network: Unified CM configuration
2. "Lync gateway" Expressway configuration (part 1)
3. Lync Server configuration
4. "Lync gateway" Expressway configuration (part 2)

Video network: Unified CM configuration

Prerequisites




Ensure that Unified CM contains a basic configuration and has already set up at least:

- System > Server
- System > Cisco Unified CM
- System > Cisco Unified CM Group
- System > Date / Time Group
- System > Presence Group
- System > Region Information
- System > Device Pool
- System > DHCP
- System > Location
- System > Physical location
- System > Enterprise parameters
- System > Licensing

Configuring the SIP Profile for Expressway

Note that you can skip this step if you are using version 9.x as a "Standard SIP Profile For Cisco VCS" will already exist (the Cisco VCS profile may be used with Expressway).

1. On Unified CM, go to **Device > Device Settings > SIP Profile**.
2. Click **Copy** against the **Standard SIP Profile**.

Find SIP Profile where Name begins with <input type="text"/> Find Clear Filter  			
<input type="checkbox"/>	Name ^	Description	Copy
<input type="checkbox"/>	Standard SIP Profile	Default SIP Profile	

3. Configure the fields as follows (leave other fields as default values):

Name	"Standard SIP Profile For Cisco VCS" (the profile is named "for Cisco VCS" for consistency with other Unified CM versions)
-------------	--

Default MTP Telephony Event Payload Type	101
Redirect by Application	Select the check box
Use Fully Qualified Domain in SIP Requests	Select the check box
Allow Presentation Sharing using BFCP	Select the check box (in Unified CM 8.6.1 or later)
Timer Invite Expires	180
Timer Register Delta	5
Timer Register Expires	3600
Timer T1	500
Timer T2	Leave as default (typically 4000 or 5000)
Retry INVITE	6
Retry non-INVITE	10
Start Media Port	16384
Stop Media Port	32766
Call Pickup URI	x-cisco-serviceuri-pickup
Call Pickup Group Other URI	x-cisco-serviceuri-opickup
Call Pickup Group URI	x-cisco-serviceuri-gpickup
Meet Me Service URI	x-cisco-serviceuri-meetme
Timer Keep Alive Expires	120
Timer Subscribe Expires	120
Timer Subscribe Delta	5
Maximum Redirections	70
Off Hook To First Digit Timer	15000
Call Forward URI	x-cisco-serviceuri-cfwdall
Abbreviated Dial URI	x-cisco-serviceuri-abbrdial
Reroute Incoming Request to new Trunk based on	Never

- Click **Save**.

SIP Profile Configuration Related Links: [Back To Find/List](#) [Go](#)

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name* Standard SIP Profile For Cisco VCS

Description Default SIP Profile

Default MTP Telephony Event Payload Type* 101

Resource Priority Namespace List < None >

Early Offer for G.Clear Calls* Disabled

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites* TIAS and AS

User-Agent and Server header information* Send Unified CM Version Information as User-Agen

☒ Redirect by Application

☐ Disable Early Media on 180

☐ Outgoing T.38 INVITE include audio mline

☐ Enable ANAT

☐ Require SDP Inactive Exchange for Mid-Call Media Change

☒ Use Fully Qualified Domain Name in SIP Requests

☒ Allow Presentation Sharing using BFCP

Parameters used in Phone

Timer Invite Expires (seconds)* 180

Timer Register Delta (seconds)* 5

Timer Register Expires (seconds)* 3600

Timer T1 (msec)* 500

Timer T2 (msec)* 4000

Retry INVITE* 6

Retry Non-INVITE* 10

Start Media Port* 16384

Stop Media Port* 32766

Call Pickup URI* x-cisco-serviceuri-pickup

Call Pickup Group Other URI* x-cisco-serviceuri-opickup

Call Pickup Group URI* x-cisco-serviceuri-gpickup

Meet Me Service URI* x-cisco-serviceuri-meetme

User Info* None

DTMF DB Level* Nominal

Call Hold Ring Back* Off

Anonymous Call Block* Off

Caller ID Blocking* Off

Do Not Disturb Control* User

Telnet Level for 7940 and 7960* Disabled

Timer Keep Alive Expires (seconds)* 120

Timer Subscribe Expires (seconds)* 120

Timer Subscribe Delta (seconds)* 5

Maximum Redirections* 70

Off Hook To First Digit Timer (milliseconds)* 15000

Call Forward URI* x-cisco-serviceuri-cfwdall

Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial

☒ Conference Join Enabled

☐ RFC 2543 Hold

☒ Semi Attended Transfer

☐ Enable VAD

☐ Stutter Message Waiting

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on* Never

RSVP Over SIP* Local RSVP

☒ Fall back to local RSVP

SIP Rel1XX Options* Disabled

☐ Deliver Conference Bridge Identifier

☐ Early Offer support for voice and video calls (insert MTP if needed)

☐ Send send-receive SDP in mid-call INVITE

SIP OPTIONS Ping

☐ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)* 60

Ping Interval for Out-of-service Trunks (seconds)* 120

Ping Retry Timer (milliseconds)* 500

Ping Retry Count* 6

Save Delete Copy Reset Apply Config Add New

Configuring the region with an appropriate session bit rate for video calls

Ensure that your regions have an appropriate session bit rate for video calls:

1. Go to **System > Region Information > Region**.
2. Select the region (for example the **Default** region).
3. Set **Maximum Session Bit Rate for Video Calls** to a suitable upper limit for your system, for example 6000 kbps.
4. Click **Save** and then click **Apply Config**.

Configuring the SIP Trunk security profile

Version 8.6.x

1. Go to **System > Security > SIP Trunk Security Profile**.
2. Click **Add New**.
3. Configure the fields as follows:

Name	Non Secure SIP Trunk Profile
Device Security Mode	Non Secure
Incoming Transport Type	TCP+UDP
Outgoing Transport Type	TCP
Incoming Port	5060
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box

4. Click **Save**.

Version 9.x

In version 9.x, the Non Secure SIP Trunk Profile will already exist, but **it must be modified**.

1. On Unified CM, go to **System > Security > SIP Trunk Security Profile**.
2. Select **Non Secure SIP Trunk Profile**.
3. Modify the fields as follows:

Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box

4. Click **Save**.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

SIP Trunk Security Profile Configuration Related Links: Back To Find/List | Go

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

SIP Trunk Security Profile Information

Name* Non Secure SIP Trunk Profile
Description Non Secure SIP Trunk Profile authenticated by null Stri
Device Security Mode Non Secure
Incoming Transport Type* TCP+UDP
Outgoing Transport Type TCP
☐ Enable Digest Authentication
Nonce Validity Time (mins)* 600
X.509 Subject Name
Incoming Port* 5060
☐ Enable Application Level Authorization
☐ Accept Presence Subscription
☐ Accept Out-of-Dialog REFER**
☒ Accept Unsolicited Notification
☒ Accept Replaces Header
☐ Transmit Security Status
SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

Save Delete Copy Reset Apply Config Add New

Configuring the SIP Trunk device

1. On Unified CM, go to **Device > Trunk**.
2. Click **Add New**.
3. Select a **Trunk Type** of *SIP Trunk*.
 - **Device Protocol** displays *SIP*.
 - If asked for a **Trunk Service Type**, select *None (Default)*.
4. Click **Next**.
5. Configure the **Device Information** fields as follows:

Device Name	As required, such as Expressway_system
Device Pool	(As set up in System > Device Pool)
Call classification	OnNet
Location	(As set up in System > Location)
Packet Capture Mode	None
Media Termination Point Required	Clear this check box if any video phones registered to Unified CM are to make or receive video calls with endpoints routed via Expressway. Select this check box if audio devices only are registered to Unified CM.
SRTP Allowed	Select this check box
Run On All Active Unified CM Nodes	Select this check box


6. Configure the **Call Routing Information > Inbound Calls** fields as follows:

Significant digits	All
Connected Line ID Presentation	Default
Connected Name Presentation	Default
Calling Search Space	(As set up in Call Routing > Class of Control > Calling Search Space)
Prefix DN	<blank>
Redirecting Diversion Header Delivery – Inbound	Select this check box

7. Configure the **Call Routing Information > Outbound Calls** fields as follows:

Calling Party Selection	Originator
Calling Line ID Presentation	Default
Calling Name Presentation	Default
Caller ID DN	<blank>
Caller Name	<blank>

8. Configure the **SIP Information** fields as follows:

Destination address is an SRV	Select this check box if a domain is specified for the destination address, and the DNS server uses DNS SRV records to direct the domain to a cluster of Expressways. Do not select this check box if an IP address is specified as the Destination address .
Destination address	<FQDN of Expressway / Expressway cluster>. Alternatively you can enter the <IP address of Expressway>. If you are not using SRV records and need to specify multiple peers, click  to add extra Destination address rows.
Destination port	5060 (this displays as zero if you are using SRV records)
Presence Group	Standard Presence Group (or whichever presence group has been configured in System > Presence Group)
SIP Trunk Security Profile	Non Secure SIP Trunk Profile
SIP Profile	Standard SIP Profile for Cisco VCS
DTMF Signaling Method	RFC 2833
Normalization Script	vcs-interop (if available, the vcs-interop script may be used with Expressway)

9. Click **Save**.
10. Click **Reset**.
11. Click **Reset**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration Related Links: [Back To Find/List](#) [Go](#)

Save

Status

Status: Ready

Device Information

Product: SIP Trunk
 Device Protocol: SIP
 Trunk Service Type: None(Default)
 Device Name*: Expressway_system
 Description: Expressway system location
 Device Pool*: Default ▾
 Common Device Configuration: LABC6 ▾
 Call Classification*: OnNet ▾
 Media Resource Group List: < None > ▾
 Location*: Reston LABC6 A51 ▾
 AAR Group: < None > ▾
 Tunneled Protocol*: None ▾
 QSIG Variant*: No Changes ▾
 ASN.1 ROSE OID Encoding*: No Changes ▾
 Packet Capture Mode*: None ▾
 Packet Capture Duration: 0
☐ Media Termination Point Required
☒ Retry Video Call as Audio
☐ Path Replacement Support
☐ Transmit UTF-8 for Calling Party Name
☐ Transmit UTF-8 Names in QSIG APDU
☐ Unattended Port
☒ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure*: When using both sRTP and TLS ▾
 Route Class Signaling Enabled*: Default ▾
 Use Trusted Relay Point*: Default ▾
☒ PSTN Access
☒ Run On All Active Unified CM Nodes

Intercompany Media Engine (IME)

E.164 Transformation Profile: < None > ▾

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain: < None > ▾

Call Routing Information

☒ Remote-Party-Id
☒ Asserted-Identity
 Asserted-Type*: Default ▾
 SIP Privacy*: Default ▾

Inbound Calls

Significant Digits*: All ▾
 Connected Line ID Presentation*: Default ▾
 Connected Name Presentation*: Default ▾
 Calling Search Space: LABC6 ▾
 AAR Calling Search Space: < None > ▾
 Prefix DN:
☒ Redirecting Diversion Header Delivery - Inbound

Incoming Calling Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

[Clear Prefix Settings](#) [Default Prefix Settings](#)

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default		< None > ▾	<input checked="" type="checkbox"/>

Connected Party Settings

Connected Party Transformation CSS: < None > ▾
☒ Use Device Pool Connected Party Transformation CSS

Outbound Calls		
Called Party Transformation CSS	< None >	
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS		
Calling Party Transformation CSS	< None >	
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS		
Calling Party Selection*	Originator	
Calling Line ID Presentation*	Default	
Calling Name Presentation*	Default	
Caller ID DN		
Caller Name		
<input type="checkbox"/> Redirecting Diversion Header Delivery - Outbound		
Redirecting Party Transformation CSS	< None >	
<input checked="" type="checkbox"/> Use Device Pool Redirecting Party Transformation CSS		

SIP Information		
Destination		
<input checked="" type="checkbox"/> Destination Address is an SRV		
Destination Address	Destination Address IPv6	Destination Port
1 * <input type="text" value="[[Undefined variable]]"/>	<input type="text"/>	<input type="text" value="0"/>
MTP Preferred Originating Codec*	711ulaw	
Presence Group*	Standard Presence group	
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile	
Rerouting Calling Search Space	< None >	
Out-Of-Dialog Refer Calling Search Space	< None >	
SUBSCRIBE Calling Search Space	< None >	
SIP Profile*	Standard SIP Profile For Cisco VCS	
DTMF Signaling Method*	RFC 2833	
Normalization Script		
Normalization Script <input type="text" value="vcs-interop"/>		
<input type="checkbox"/> Enable Trace		
Parameter Name	Parameter Value	
1 <input type="text"/>	<input type="text"/>	

Geolocation Configuration	
Geolocation	< None >
Geolocation Filter	< None >
<input type="checkbox"/> Send Geolocation Information	

- Save

Configuring the clusterwide domain enterprise parameters

Unified CM must be configured with a **Cluster Fully Qualified Domain Name** so that it can receive calls to addresses in the format <address>@domain. (It is also required when Unified CM is clustered so that Expressway can send the call to any Unified CM node.)

1. Go to **System > Enterprise parameters**, and find the **Clusterwide Domain Configuration** section.
2. Set the **Organization Top Level Domain** to the same domain as the video network, for example vc.ciscotp.com.
This ensures that the correct domain of the calling party is displayed to the called party.
3. Set the **Cluster Fully Qualified Domain Name** to the same domain as the video network, for example vc.ciscotp.com.
This parameter defines one or more Fully Qualified Domain Names (FQDNs) for this cluster. Multiple FQDNs must be separated by a space. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter will be recognized as a request destined for this cluster and/or devices attached to it.
4. Click **Save**.

Clusterwide Domain Configuration[Organization Top Level Domain](#)

vc.ciscotcp.com

[Cluster Fully Qualified Domain Name](#)

vc.ciscotcp.com

Allowing dialing to Expressway domain from Cisco phones

Configure a SIP route pattern that tells Unified CM that anything with, for example, a domain vc.ciscotcp.com needs to be sent down the Expressway SIP trunk. This is required to permit dialing from endpoints that support SIP URIs with domains, and also for enabling the reverse path to the Expressway for certain signaling.

1. On Unified CM, go to **Call Routing > SIP Route Pattern**.
2. Click **Add New**.
3. Configure the fields as follows:

Pattern Usage	Domain Routing
IPv4 Pattern	Domain for calls, for example ciscotcp.com
Route Partition	Default is "<None>"; set according to dial plan restrictions
SIP Trunk	Required Trunk to route calls to the Unified CM

4. Click **Save**.

Pattern Definition

Pattern Usage Domain Routing

IPv4 Pattern*

ciscotcp.com

IPv6 Pattern

Description

Expressway system domain

Route Partition

LABCM6

SIP Trunk/Route List*

Expressway_system

[\(Edit\)](#)☐ Block Pattern**Calling Party Transformations**☐ Use Calling Party's External Phone Mask

Calling Party Transformation Mask

Prefix Digits (Outgoing Calls)

Calling Line ID Presentation*

Default

Calling Line Name Presentation*

Default

Connected Party Transformations

Connected Line ID Presentation*

Default

Connected Line Name Presentation*

Default

Save

Delete

Copy

Add New

When <name>@ciscotcp.com is dialed by an endpoint registered to Unified CM, Unified CM will route the call to the Expressway as <name>@<FQDN of Expressway>:5060 (TCP) or <name>@<FQDN of Expressway>:5061 (TLS). (The domain may alternatively be the IP address of Expressway, depending on what is configured as the SIP Trunk **Destination Address**.)

Checking the message size limit on Unified CM

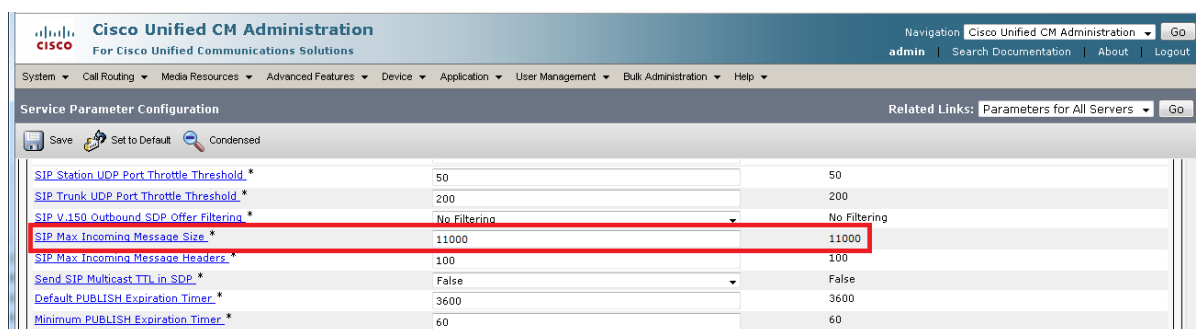
SIP messages for video are considerably larger than SIP messages for audio calls, in particular, when a Cisco TelePresence Server is used in the video network.

Ensure that the **SIP Max Incoming Message Size** on Unified CM is set to 11000:

1. Go to **System > Service Parameters**.
2. Select the appropriate server.
3. Select *Cisco CallManager (Active)* as the service.
4. Select **Advanced**.
5. In the **Clusterwide Parameters (Device – SIP)** configure the field as follows:

SIP Max Incoming Message Size	11000
--------------------------------------	-------

6. Click **Save**.



"Lync gateway" Expressway configuration (part 1)

This comprises the following steps:

1. Load CA certificate and server certificate onto Expressway for TLS connectivity with Lync.
2. Configure DNS.
3. Ensure that a cluster name is configured.
4. Configure an NTP server.
5. Ensure that TLS is enabled in SIP configuration.

We recommend that you use TLS connectivity between Expressway and Lync. (TCP may not work for Lync configurations that include HLBs and / or Lync Director and the use of TCP prevents the use of encryption).

If the "Lync gateway" is a cluster, unless this guide states that configuration is required on each peer, configure the master "Lync gateway" Expressway in the cluster and allow the configuration to be replicated to the other peers automatically. If the "Lync gateway" is just a single Expressway then set up the configuration on that "Lync gateway" Expressway.

"Lync gateway" Expressway: Load CA certificate and server certificate (if using TLS to Lync)

Obtain and load the CA certificate, server certificate and private key onto the Expressway. Note that for mutual TLS authentication the server certificate must be capable of being used as a client certificate as well.

A certificate must be created for each "Lync gateway" Expressway; the certificate must specify:

- **Subject Name:** the Expressway peer's FQDN e.g. exp01.ciscotlp.com
and if it is part of a cluster:
- **Subject Alternate Name:** a comma separated list of the Expressway cluster's FQDN and the Expressway peer's routable FQDN, e.g. lyncexp.ciscotlp.com, exp01.ciscotlp.com

You may also want to set up the SIP trunk between Expressway and Unified CM to use TLS. We recommend that you set up a working TCP trunk first and then convert it to TLS. Full instructions for doing this and for managing certificates on Expressway and Unified CM are in section [Connecting Expressway to Unified CM using TLS \[p.47\]](#).

"Lync gateway" Expressway: Configure DNS and local hostname

Configure the DNS server details

The "Lync gateway" Expressway(s) should be configured to use the same DNS server(s) as Lync Server.

On a machine running Lync Server:

1. From the Windows **Start** menu choose **Run**.
2. Type `cmd` into the **Open** field and click **OK**. A command window opens.
3. In the cmd.exe window type:
`ipconfig /all`
4. Note down the DNS server(s).

Note: a DNS server IP address of 127.0.0.1 means that Lync Server is using a DNS server on its own hardware. Instead of entering 127.0.0.1 on the Expressway, use the IP address of the Lync Server platform instead.

On each "Lync gateway" Expressway peer:

1. Go to **System > DNS**.
2. If the DNS server that Lync Server uses can provide all DNS lookups needed by Expressway:
 - a. Set **Default DNS Server Address 1** to the IP address of DNS server noted earlier.
 - b. If Lync Server has more than one DNS server defined, configure the additional default DNS server fields (**Address 2**, **Address 3** and so on) with the IP addresses of the additional servers.
3. If the Expressway must use other DNS servers for normal calls and only the Lync DNS server for Lync access:
Configure the **Default DNS servers** with the servers which will be used for normal, non-Lync related DNS operation and configure the **Per-domain DNS servers** section as follows:

Address 1	IP address of the DNS server used by Lync Server
------------------	--

Domain names	Domain shared with Lync
Address 2 ... 5	Use these fields only if Lync Server uses more than one DNS server
Domain names 2 ... 5	Use these fields only if Lync Server uses more than one DNS server; configure with the domain shared with Lync

4. Configure the next available **Per-domain DNS server address** to contain the IP address of the Lync Front End Processor, and specify the Lync domain e.g. ciscotp.com as the associated **Domain name**. (This is required in some network setups: Lync frequently embeds hostnames inside contact headers and sometimes these can be unresolvable outside of the Windows domain.)
5. Click **Save**.

Ensure that Local hostname and DNS domain are configured

For each "Lync gateway" Expressway peer, ensure that a unique Local host name is set up and that the DNS Domain name is set up:

1. Go to **System > DNS** and set:
 - a. **Local host name** to a unique hostname for this Expressway.
 - b. **Domain name** to the domain name for this Expressway.
2. Click **Save**.

Note that:

- the **Local host name** concatenated with DNS **Domain name** is the routable FQDN of this Expressway.
- if these items are not configured and the connection between Lync Server and Expressway is TLS, then although the neighbor zone goes active and Expressway can send messaging to Lync Server, Lync Server will never open a TLS connection back to Expressway, resulting in no calls from Lync to Expressway and other strange behavior.

"Lync gateway" Expressway: Ensure that cluster name is configured

Lync will be configured with a static route that uses the "Lync gateway" Expressway's cluster name / FQDN (e.g. lyncexp.ciscotp.com) regardless of whether the "Lync gateway" Expressway is part of a cluster or not.

For each "Lync gateway" Expressway peer, ensure that **Cluster name (System > Clustering)** is the same, and is set up to be the FQDN of the cluster. Note that this should have been set up when the cluster was created – see *Expressway Cluster Creation and Maintenance Deployment Guide*. If the cluster name needs changing follow the procedure in that document.

"Lync gateway" Expressway: Configure an NTP server

On each "Lync gateway" Expressway peer:

1. Go to **System > Time**.
2. Set **NTP server 1** to the IP address of an NTP server.
3. Optionally set **NTP server 2** to the IP address of an additional NTP server.
4. Set **Time zone** as appropriate to the location of the Expressway.

You can find out which time server that the Windows server (the Lync Server) is using by typing 'net time /queryntp' from the windows command line.

"Lync gateway" Expressway: Ensure that TLS is enabled in SIP configuration

1. Go to **Configuration > Protocols > SIP**.
2. Ensure that **TLS mode** is *On*.

Lync Server configuration

The configuration will vary depending upon the architecture of the Lync Server installation.

- If a Lync Director is in use, then configure the Lync Director (pool) to trust the "Lync gateway" Expressway and to route traffic to Expressway. Other FEPs receiving calls for the video domain may not know how to route them (depending on Lync SIP routing configuration), and may pass the calls to the Director pool for routing.
- If there is just a hardware load balancer in front of a set of FEP pools, configure each FEP pool.
- If there is just a single FEP, configure it.

To allow the "Lync gateway" Expressway to communicate with Lync Server:

1. For a TLS (encrypted signaling) connection between the "Lync gateway" Expressway and Lync Server (recommended), TLS must be allowed on Lync Server.
For a TCP connection (not recommended), TCP must be allowed on Lync Server .
2. Configure Lync Server to trust the "Lync gateway" Expressway(s).
3. Configure Lync Server media encryption capabilities.

Trust a "Lync gateway" Expressway

Lync trust can either be set up for a single "Lync gateway" Expressway or multiple Expressways (for example when using a cluster for "Lync gateway" Expressway).

On Lync Server (using Lync 2010 as an example):

1. Select **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Management Shell**.
2. Set one or more "Lync gateway" Expressways as a trusted application for Lync Server (Expressway is treated as an application by Lync Server).
Use the command **New-CsTrustedApplicationPool** with the following parameters:
 - Identity**: specifies the "Lync gateway" Expressway **cluster** FQDN. This name must match the Common Name / Subject Alternate Name specified in the Expressway server certificate e.g. lyncexp.ciscotp.com.
 - ComputerFqdn**: specifies the "Lync gateway" Expressway **peer** FQDN (specify the master Expressway FQDN if running a cluster), e.g. exp01.ciscotp.com. This name must match the Common Name specified in the Expressway server certificate.
 - Registrar**: specifies the FQDN of the registrar for the Lync pool
 - Site**: specifies the siteID on which this application pool is homed

Note: you can use the command **Get-CsSite** to get the full list of sites (SiteID) and related pools.

 - RequiresReplication**: specifies that this trusted application must not be replicated between Pools (must be \$false)
 - ThrottleAsServer**: reduces the message throttling as it knows the trusted device is a server, not a client (must be \$true)
 - TreatAsAuthenticated**: specifies that this application is authenticated by default (must be \$true)

For example:

```
C:\Users\administrator.CISCOTP>New-CsTrustedApplicationPool -Identity  
lyncexp.ciscotp.com -ComputerFqdn exp01.ciscotp.com -Registrar feppool.ciscotp.com -  
site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
```

3. (For TCP only deployments) Use the Topology Builder to configure the IP address of the "Lync gateway" Expressway as a trusted server:

- a. Select **Start > All Programs > Microsoft Lync Server 2010 > Topology Builder**.
- b. Under **Lync Server 2010 > Trusted Application Servers**, right-click on the Expressway host and select **Edit Properties**.
- c. In the **General** tab, select **Limit service usage to selected IP addresses**, enter the **Primary IP address** of the Expressway and click **OK**.
- d. Publish the topology (you may need to restart the Lync Front-End Service to make sure that topology changes are applied).

4. If using a cluster of "Lync gateway" Expressways, use the shell to add the additional cluster peer members as computers to the trusted application pool using the command **New-CsTrustedApplicationComputer** with the following parameters:
 - Identity**: specifies the FQDN of the Expressway cluster peer being added, e.g. exp02.ciscotp.com. This name must match the Common Name specified in the Expressway server certificate.
 - Pool**: specifies the FQDN of the application pool this Expressway is being added to (identical to the FQDN used for -Identity in the previous step, e.g. lyncexp.ciscotp.com).For example:

```
C:\Users\Administrator.CISCOTP> New-CsTrustedApplicationComputer -Identity  
exp02.ciscotp.com -Pool lyncexp.ciscotp.com
```

5. Assign an application to a specific application pool:
Use the command **New-CsTrustedApplication** with the following parameters:
 - ApplicationID**: specifies a label for the "Lync gateway" Expressway application (it is internal to Lync only, not a DNS name)
 - TrustedApplicationPoolFQDN**: specifies the "Lync gateway" Expressway FQDN (or "Lync gateway" Expressway Cluster name if present)
 - Port**: specifies TLS/TCP port to use for neighboring. This should be set to the port configured as **Port on B2BUA for Lync call communications** in the B2BUA advanced settings on the Expressway (default 65072).
 - enableTCP**: this must be included only if TCP is the chosen transport protocolFor example, for TLS:

```
C:\Users\administrator.CISCOTP>New-CsTrustedApplication -ApplicationId  
ExpresswayApplication1 -TrustedApplicationPoolFqdn lyncexp.ciscotp.com -Port 65072
```

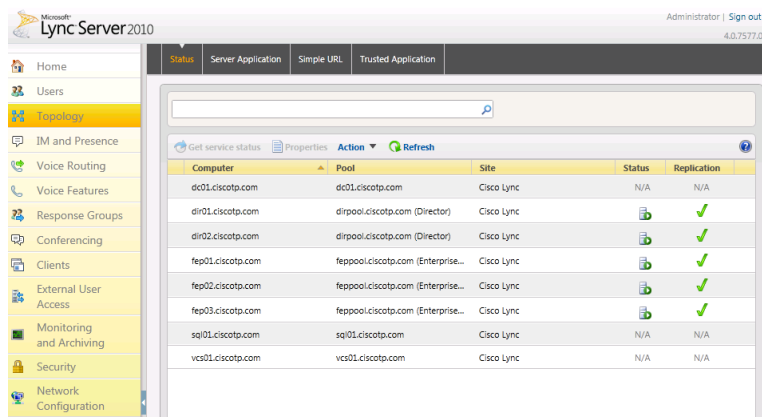
For example, for TCP:

```
C:\Users\administrator.CISCOTP>New-CsTrustedApplication -ApplicationId  
ExpresswayApplication1 -TrustedApplicationPoolFqdn lyncexp.ciscotp.com -Port 65072 -  
EnableTCP
```

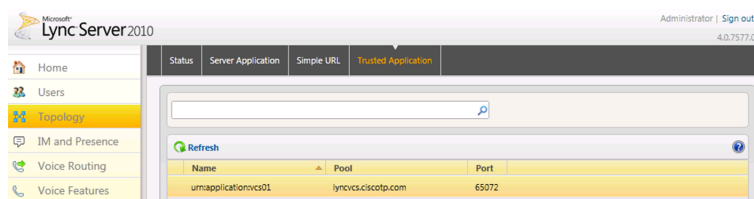
6. Apply the configuration
Use the command **Enable-CsTopology**.
For example:

```
C:\Users\administrator.CISCOTP>Enable-CsTopology
```

To verify that all Expressway systems integrated with Lync Servers are assigned to the correct trusted Application Pool on the LSCP (Lync Server Control Panel): **Topology > Status**:



To verify trusted application and its assignment to the correct Application Pool on the LSCP (Lync Server Control Panel): **Topology > Trusted Application** menu:



Configure Lync Server media encryption capabilities

By default Lync Server mandates the use of encrypted media. However, the headers used in Lync SRTP are different from those used by video network devices.

Expressway has the capability to carry out on-the-fly modification of these headers if the **Microsoft Interoperability** option key is enabled on the "Lync gateway" Expressway.

The choice of how to configure Lync's encryption capabilities depends on:

- Is the connection between Lync and the "Lync gateway" Expressway over TLS?
If it is not TLS, then crypto keys will not pass (they can be sent only over a secure – encrypted signaling link), encryption must **not** be set to **require** on Lync Server.
- Does the "Lync gateway" Expressway have the **Microsoft Interoperability** option key enabled?
If no, encryption must **not** be set to **require** on Lync Server.
- Do all video endpoints support encrypted media, and will they offer encrypted media when initiating calls?
If no, then configure the relevant Expressway so that the **Media encryption policy** for that endpoint's zone/subzone is set to *Force encrypted*.

To configure the way Lync will handle encryption, use the command:

```
set-CsMediaConfiguration -EncryptionLevel <value>
```

where <value> is one of **RequireEncryption**, **SupportEncryption**, **DoNotSupportEncryption**.

For example:

```
C:\Users\administrator.CISCOTP> set-CsMediaConfiguration -EncryptionLevel supportencryption
```

Note that:

- This parameter is a value communicated to Lync clients to affect its operation. To activate this change on a Lync client, sign out, then sign back into the Lync client.
It may take a while for the parameter to be shared throughout the pool (up to an hour) so you may have to wait a while before restarting the Lync clients for them take on the new value.
- If the **Microsoft Interoperability** option key is installed and the connection between the Expressway and Lync Server is TLS, then the default setting of the command set-CsMediaConfiguration **–EncryptionLevel RequireEncryption** may be used. However, be aware that if **RequireEncryption** is set on Lync, either all video endpoints must support encryption or the Expressway's **Media encryption policy** for the relevant zones and subzones must be set to *Force encrypted*. Otherwise, calls will fail – consider using **SupportEncryption** instead.

"Lync gateway" Expressway configuration (part 2)

This comprises the following steps:

1. Configure the B2BUA on the "Lync gateway" Expressway.
2. Set up a search rule to route calls to the Lync domain to Lync.
3. If required, set up search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync.

Configure the B2BUA on the "Lync gateway" Expressway

When configuring the B2BUA, two of the fields to configure are the destination address and destination port for the B2BUA to send signaling to in the Lync environment. The values that need to be entered depend on the structure of the Lync environment:

If the Lync environment...	Configure the signaling destination address and port to be that of the...
is fronted by a Hardware Load Balancer in front of Lync Directors	Hardware Load Balancer
is fronted by a Lync Director or Director pool	Lync Director (pool)
has no Lync Director but a Hardware Load Balancer in front of Front End Processors	Hardware Load Balancer
is a single FEP	FEP


1. Go to **Applications > B2BUA > Microsoft Lync > Configuration**.
2. Configure the fields as follows:

Microsoft Lync B2BUA	<i>Enabled</i>
Lync signaling destination address	IP address or FQDN of device specified above, for example dirpool.ciscotp.com
Lync signaling destination port	IP port used by device specified above – typically 5061
Lync signaling transport	<i>TLS</i>


Register FindMe users as clients on Lync	<i>No</i>
Enable transcoders for this B2BUA	<i>No</i>
Offer TURN Services	<i>No</i>
Advanced settings	Leave all advanced settings at their default values


3. Click **Save**.


Microsoft Lync B2BUA configuration You are here: [Applications](#) > [B2BUA](#) > [Microsoft Lync](#) > Configuration


 **Warning:** The B2BUA is enabled but no [search rules](#) have been configured for the To Microsoft Lync server via B2BUA zone.

Configuration


Microsoft Lync B2BUA Enabled 

Lync signaling destination address ★  [Configure trusted hosts](#)


Lync signaling destination port ★ 

Lync signaling transport TLS 


Capabilities

Register FindMe users as clients on Lync No 

Transcoders

Enable transcoders for this B2BUA No 

TURN

Offer TURN services No  [Configure B2BUA TURN servers](#)

Advanced

Advanced settings [Show advanced settings](#)

Save

"To Microsoft Lync Server via B2BUA" neighbor zone

When the B2BUA is enabled, a non-configurable neighbor zone called **To Microsoft Lync Server via B2BUA** is automatically set up:

Set up a search rule to route calls to the Lync domain to Lync

Search rules are used to specify the URIs to be forwarded to Lync (for example, by matching the domain of the destination or by matching some element in the URI).

Search rules can also be used to transform URIs before they are sent to a neighbor, for example to add or modify the domain or add, remove or translate user-id prefixes and even to add extra tags to SIP URIs, such

as user=phone (see [TEL URI handling for Expressway to Lync calls \[p.69\]](#) for further information about user=phone).

For this scenario, anything with a domain ciscotp.com will be matched (and passed to Lync via the B2BUA); no transformation is required.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the search rule so that all calls to URIs in the format `.+@ciscotp.com.*` are forwarded to Lync.

Rule name	To Lync
Priority	100
Source	Any
Mode	Alias pattern match
Pattern type	Regex
Pattern string	.+@ciscotp\.com.*
Pattern behavior	Leave
On successful match	Stop
Target zone	To Microsoft Lync Server via B2BUA

4. Click **Save**.

The screenshot shows the 'Configuration' window for a new search rule. The rule is named 'To Lync' with priority 100. The source is 'Any', mode is 'Alias pattern match', pattern type is 'Regex', pattern string is '.+@ciscotp\.com.*', pattern behavior is 'Leave', on successful match is 'Stop', target is 'To Microsoft Lync server via B2BUA', and the state is 'Enabled'.

Note: never use a **Mode** of *Any alias*. Always use a pattern string which matches the Lync domain as closely as possible so that only calls, notifies and other messages that are handled by Lync get sent to it. If *Any alias* were to be selected, then all calls and other messages would be routed to Lync — subject to no higher priority search rules matching — whether or not Lync supports that call or message and it may introduce delays, or worse cause calls to fail.

Set up search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync

If Lync supports only a single domain then no other search rule is required here. If Lync supports other domains and video endpoints should be able to call these devices, one or more additional search rules can be added.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the search rule so that all calls to the relevant URI are routed to Lync.

Rule name	xxxx To Lync
Priority	100
Source	<i>Any</i>
Mode	<i>Alias pattern match</i> (never use a Mode of <i>Any alias</i>)
Pattern type	<i>Regex</i>
Pattern string	.+@<relevant domain>.*
Pattern behavior	<i>Leave</i>
On successful match	<i>Stop</i>
Target zone	<i>To Microsoft Lync Server via B2BUA</i>

4. Click **Save**.
5. Repeat for all domains supported on Lync (that are not used in the video network).

Calls can now be made between SIP endpoints registered on the video network to Lync clients registered on Lync Server.

Testing the configuration

Test calls from endpoints registered on the video network to Lync clients registered on Lync Server.

For example, call david.jones@ciscotp.com or alice.parkes@ciscotp.com from endpoints registered on Unified CM.

Note that if Lync for Mac OS X is used and a Cisco AM GW is not installed, the call will result in an audio only call as Lync for Mac does not support any video codecs supported by standards-based endpoints.

Enabling Lync clients registered on Lync Server to call endpoints registered on the video network

This is configured in 2 stages:

1. “Lync gateway” Expressway configuration (B2BUA trusted hosts, neighbor zone and search rules to the video network).
2. Lync Server configuration (domain static routes to the “Lync gateway” Expressway).

“Lync gateway” Expressway configuration

This comprises the following steps:

1. Configure the B2BUA trusted hosts on the “Lync gateway” Expressway.
2. Configure the “Lync gateway” Expressway with a neighbor zone that contains the video network.
3. Set up one or more search rules to route calls with video network domains to the video network.
4. Creating a transform to strip port information from URIs.

Configuring the B2BUA trusted hosts on the “Lync gateway” Expressway

The Lync devices that must be trusted by the Expressway depend on the structure of the Lync environment:

If...	Trust the...
static routes are to be created from the Lync environment	Lync FEPs which will be sending traffic towards the “Lync gateway” Expressways
the Lync environment is fronted by a Hardware Load Balancer in front of Lync Directors	Hardware Load Balancer and the Lync Directors
the Lync environment is fronted by a Lync Director	Lync Director
the Lync environment has no Lync Director but a Hardware Load Balancer in front of Front End Processors	Hardware Load Balancer and the Lync FEPs
Lync is a single FEP	Lync FEP

1. Go to **Applications > B2BUA > Microsoft Lync > B2BUA trusted hosts**.
2. Click **New**.
3. Configure the fields as follows:

Name	Name to identify Lync device
IP address	IP address of the device
Type	<i>Lync device</i>

4. Click **Save**.
5. Repeat these steps until all Lync devices that need to be trusted have been added.

Microsoft Lync B2BUA trusted hosts You are here: [Applications](#) > [B2BUA](#) > [Microsoft Lync](#) > [B2BUA trusted hosts](#) > [New](#)

Configuration

Name

IP address

Type

Notes:

- Note that trusted host verification only applies to calls initiated by Lync that are inbound to the Expressway video network. It is not necessary to configure trusted hosts if calls are only ever to be initiated from the Expressway video network.
- The Expressway has a limit of 25 trusted hosts. If there are more than 25 trusted hosts, the Expressway raises an alarm. You can work around this limit by adding another "Lync gateway" Expressway, or by pointing some of the Lync servers to a Lync proxy and then trusting the proxy instead.

Configuring the “Lync gateway” Expressway with a neighbor zone that contains the video network

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

Name	CUCM Neighbor
Type	<i>Neighbor</i>
Hop count	15
H.323 mode	<i>Off</i> (H.323 is not supported between Expressway and Unified CM)
SIP mode	<i>On</i>
SIP port	5060 (if the SIP access port on Unified CM is not 5060, change the SIP Port value to be the same as used by Unified CM)
Transport	<i>TCP</i>
Media encryption mode	<i>Auto</i>
SIP authentication trust mode	<i>Off</i>
Peer 1 address	IP address of Unified CM, or the FQDN of Unified CM. If you are planning to ultimately use a TLS connection, then typically you will need to specify the FQDN of Unified CM here as this is the name that will be used to authenticate the certificate presented by Unified CM.

Zone profile (Advanced section)

This depends upon your version of Unified CM:

- Select *Cisco Unified Communications Manager* for versions prior to 8.6.1
- Select *Cisco Unified Communications Manager (8.6.1 or later)* for 8.6.1 or 8.6.2
- Select *Custom* for 9.x or later and:
 - Set **Call signaling routed mode** to *Always*
 - Leave all the other fields as their default values

Note that Unified CM 8.6.1 or later is required for BFCP (dual video / presentation sharing).

This configures the Expressway to use SIP over TCP to communicate with the Unified CM. To use TLS, complete the configuration as described here for TCP and then see [Connecting Expressway to Unified CM using TLS \[p.47\]](#).

4. Click **Create zone**.

Edit zone

TypeNeighbor

Hop count★15*i*

H.323

ModeOff*i*

SIP

ModeOn*i*

Port★5060*i*

TransportTCP*i*

Accept proxied registrationsDeny*i*

Media encryption modeAuto*i*

ICE supportOff*i*

Authentication

Authentication policyDo not check credentials*i*

SIP authentication trust modeOff*i*

Location

Peer 1 address10.50.157.22*i*

Peer 2 address*i*

Peer 3 address*i*

Peer 4 address*i*

Peer 5 address*i*

Peer 6 address*i*

Advanced

Zone profileCustom*i*

Monitor peer statusYes*i*

Call signaling routed modeAlways*i*

Creating a search rule to route calls to the Unified CM neighbor zone

Search rules specify the range of telephone numbers / URIs to be handled by this neighbor Unified CM. They can also be used to transform URIs before they are sent to the neighbor.

In this example deployment, this search rule routes calls with addresses in the format 3xxx@vc.ciscotp.com to Unified CM.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows to route the call to Unified CM:

Rule name	Route to CUCM
Description	For example: Send 3xxx@vc.ciscotp.com calls to CUCM
Priority	100
Protocol	<i>Any</i>
Source	<i>Any</i>
Request must be authenticated	Configure this setting according to your authentication policy
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	(3\d{3})@vc.ciscotp.com
Pattern behavior	<i>Leave</i> (@domain formatted addresses will work in Unified CM due to the Cluster Fully Qualified Domain Name enterprise parameter)
On successful match	<i>Stop</i>
Target zone	<i>CUCM Neighbor</i>
State	<i>Enabled</i>

4. Click **Create search rule**.

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	* Route to CUCM i
Description	Send 3xxx@vc.ciscoip.com calls to CUCM i
Priority	* 100 i
Protocol	Any i
Source	Any i
Request must be authenticated	No i
Mode	Alias pattern match i
Pattern type	Regex i
Pattern string	* (3\d{3})@vc.ciscoip.com i
Pattern behavior	Leave i
On successful match	Stop i
Target	* CUCM Neighbor i
State	Enabled i

See the “Zones and Neighbors” section of [Expressway Administrator Guide](#) for further details.

Creating a transform to strip port information from URIs

This transform matches URIs received from Unified CM in the form <uri>:<port> and strips off any port information to convert them into just <uri>.

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the fields as follows:

Priority	Enter a high priority such as 5 (the priority of this transform should be before any transforms that need to be applied for searching neighbor zones)
Description	Strip off any port information
Pattern type	Regex
Pattern string	For example: (.+):.*
Pattern behavior	Replace
Replace string	For example: \1
State	Enabled

4. Click **Create transform**.

Create transform You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority	<input type="text" value="5"/>	
Description	<input type="text" value="Strip off any port information"/>	
Pattern type	<input type="text" value="Regex"/>	
Pattern string	<input type="text" value="*(.+:)*"/>	
Pattern behavior	<input type="text" value="Replace"/>	
Replace string	<input type="text" value="\1"/>	
State	<input type="text" value="Enabled"/>	

Configuring Lync Server domain static routes

This involves configuring domain static routes that route calls to the video domain to the “Lync gateway” Expressway.

The routes should reside on the Director (pool) if present, otherwise on the FEP (pool).

Configuring static routes to route calls to the “Lync gateway” Expressway

1. Create a static route from Lync to the "Lync gateway" Expressway.
Use the command **New-CsStaticRoute** with the following parameters:
\$=: the label referring to this specific new route.
-TLSSRoute: specifies that the route is TLS (recommended).
-TCPRoute: specifies that the route is TCP.
-Destination: the "Lync gateway" Expressway Cluster FQDN for TLS routes. Use the IP Address in case of TCP routes.
-MatchUri: the SIP domain that "Lync gateway" Expressway is authoritative for.
-Port: the TLS/TCP port to use for neighboring. It should be the port configured as **Port on B2BUA for Lync call communications** in the B2BUA advanced settings on the Expressway (default 65072).
-UseDefaultCertificate: to use the default certificate assigned to the Front End (must be \$true) when using TLS. Do not specify this switch when using TCP.

For example, for TLS:

```
C:\Users\administrator.CISCOTP> $Route1=New-CsStaticRoute -TLSSRoute -Destination
"lyncexp.ciscotp.com" -MatchUri "vc.ciscotp.com" -Port 65072 -UseDefaultCertificate
$true
```

For example, for TCP:

```
C:\Users\administrator.CISCOTP> $Route1=New-CsStaticRoute -TCPRoute -Destination
"10.0.0.2" -MatchUri "vc.ciscotp.com" -Port 65072
```

2. Assign a static route.
Use the command **Set-CsStaticRoutingConfiguration** with the following parameters:

-Identity: specifies where to apply the route. It can be at the global level or on a specific pool.
-Route @{Add=}: the route (defined earlier) to assign to the Identity (note that brackets are “curly”).
For example:

```
C:\Users\administrator.CISCOTP> Set-CsStaticRoutingConfiguration -Identity global -  
Route @{Add=$Route1}
```

3. Verify the static route assignment. Use the command :

```
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
```

Note that:

- When Lync Server tries to route a call it will first check all its registrations:
 - If any registration is found that matches the called URI, the call will be sent to that device, or if multiple registrations exist, the call will be forked to all registered devices that match the URI.
 - If there is no registration, Lync Server will then check the static domain routes and if there is one for this domain then Lync Server will route the call to the destination specified.
- If static routes are set up, Expressway will receive any requests to that domain that Lync cannot handle, and thus may receive significant volumes of mis-dial traffic.

Testing the configuration

Test calls from Lync clients registered on Lync Server to endpoints registered on Unified CM. For example, call david.jones.office@vc.ciscotp.com from a Lync client registered on Lync Server.

Enabling Microsoft Edge Server and Expressway TURN capabilities

Ensure that the **Microsoft Interoperability** option key has been installed on the “Lync gateway” Expressway.

To enable call connectivity with Lync clients calling via an Edge server, the B2BUA needs to have TURN services properly configured to point to a Expressway-E with TURN enabled.

1. Go to **Applications > B2BUA > B2BUA TURN servers**.
2. Click **New**.
3. Configure the fields as follows:

TURN server address	IP address of a Expressway-E which has TURN enabled. (Just a single Expressway; it may be just one peer from a cluster.)
TURN server port	3478 The port on the Expressway-E that is listening for TURN requests. On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.
Description	An optional description of this TURN server.
TURN services username and TURN services password	The username and password to access the TURN server.

4. Click **Add address**.
5. Repeat the above steps if additional TURN servers are required.
6. Go to **Applications > B2BUA > Microsoft Lync > Configuration**.
7. Configure the fields as follows:

Offer TURN Services	Yes
----------------------------	-----

8. Click **Save**.

Connecting Expressway to Unified CM using TLS

These instructions explain how to take a system that is already configured and working using a TCP interconnection between Expressway and Unified CM, and to convert that connection to use TLS instead. This process involves:

- Ensuring certificate trust between Unified CM and Expressway
- Configuring a SIP trunk security profile on Unified CM
- Updating the Unified CM trunk to Expressway to use TLS
- Updating the Expressway neighbor zone to Unified CM to use TLS

Ensuring certificate trust between Unified CM and Expressway

For Unified CM and Expressway to establish a TLS connection with each other:

- Expressway and Unified CM must both have valid server certificates loaded (you must replace the Expressway's default server certificate with a valid server certificate)
- Expressway must trust Unified CM's server certificate (the root CA of the Unified CM server certificate must be loaded onto Expressway)
- Unified CM must trust Expressway's server certificate (the root CA of the Expressway server certificate must be loaded onto Unified CM)

See [Expressway Certificate Creation and Use Deployment Guide](#) for full details about loading certificates and how to generate CSRs on Expressway to acquire certificates from a Certificate Authority (CA).

Note: In a clustered environment, you must install CA and server certificates on each peer/node individually.

We strongly recommend that you do not use self-signed certificates in a production environment.

Loading server and trust certificates on Expressway

Expressway server certificate

Expressway has only one server certificate. By default, this is a certificate signed by a temporary certificate authority. We recommend that it is replaced by a certificate generated by a trusted certificate authority.

To upload a server certificate:

1. Go to **Maintenance > Security certificates > Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.
3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this server certificate.)
 - The **server private key** PEM file must not be password protected.
 - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data**.

Expressway trusted CA certificate

The **Trusted CA certificate** page (**Maintenance > Security certificates > Trusted CA certificate**) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

The root CA of the Unified CM server certificate must be loaded into the Expressway's trusted CA certificate list.

To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.

Repeat this process on every Expressway that will communicate with this Unified CM.

Loading server and trust certificates on Unified CM

Certificate management for Unified CM is performed in the **Cisco Unified OS Administration** application.

All existing certificates are listed under **Security > Certificate Management**. Server certificates are of type *certs* and trusted CA certificates are of type *trust-certs*.

Unified CM server certificate

By default, Unified CM has a self-signed server certificate **CallManager.pem** installed. We recommend that this is replaced with a certificate generated from a trusted certificate authority.

Unified CM trusted CA certificate

To load the root CA certificate of the authority that issued the Expressway certificate (if it is not already loaded):

1. Click **Upload Certificate/Certificate chain**.
2. Select a **Certificate Name** of *CallManager-trust*.
3. Click **Browse** and select the file containing the root CA certificate of the authority that issued the Expressway certificate.
4. Click **Upload File**.

Repeat this process on every Unified CM server that will communicate with Expressway. Typically this is every node that is running the CallManager service.

Configuring a SIP trunk security profile on Unified CM

On Unified CM:

1. Select **Cisco Unified CM Administration**, click **Go** and log in.
2. Go to **System > Security > SIP Trunk Security Profile**.
3. Click **Add New**.
4. Configure the fields as follows:

Name	A name indicating that this is an encrypted profile.
Description	Enter a textual description as required.
Device Security Mode	<i>Encrypted.</i>
Incoming Transport Type	<i>TLS.</i>
Outgoing Transport Type	<i>TLS.</i>
Enable Digest Authentication	Leave unselected.
X.509 Subject Name	The subject name or an subject alternate name provided by the Expressway in its certificate. For Expressway clusters, ensure that this list includes all of the names contained within all of the peers' certificates. To specify multiple X.509 names, separate each name by a space, comma, semicolon or colon.
Incoming Port	5061
Accept Unsolicited Notification	Select this check box
Accept Replaces Header	Select this check box
Other parameters	Leave all other parameters unselected.

- Click **Save**.

Updating the Unified CM trunk to Expressway to use TLS

On Unified CM:

- Go to **Device > Trunk**.
- Using Find, select the **Device Name** previously set up for the trunk to the Expressway.
- Configure the following fields:

SIP Information section	
Destination Port	5061 (unless using DNS SRV, in which case ensure the SRV records are set up correctly).
SIP Trunk Security Profile	Select the trunk profile set up above.

Leave other parameters as previously configured.

- Click **Save**.
- Click **Reset**.

Updating the Expressway neighbor zone to Unified CM to use TLS

Note that Expressway will report that the Unified CM zone is active even while it is communicating with Unified CM over TCP. The changes below are necessary to enable communications over TLS.

On Expressway:

1. Go to **Configuration > Zones > Zones**, then select the zone to Unified CM.
2. Configure the following fields:

SIP section	
Port	5061
Transport	TLS
TLS verify mode	On
Authentication trust mode	Off

Leave other parameters as previously configured.

3. Click **Save**.

Verifying that the TLS connection is operational

To verify correct TLS operation, check that the Expressway zone reports its status as active and then make some test calls.

1. Check the Expressway zone is active:
 - a. Go to **Configuration > Zones > Zones**.
 - b. Check the **SIP status** of the zone.
If the zone is not active, try resetting or restarting the trunk again on Unified CM.
2. Make a test call from a system routed through an Expressway to a Unified CM phone.
3. Make a test call from a Unified CM phone to a system routed through an Expressway.

Network of Expressways

If there is a network of Expressways behind this Expressway neighbored to Unified CM, then, either:

- Unified CM must trust the certificates of all the Expressways in the network ('optimal' routing mode), or
- The Expressway neighbor zone to Unified CM must 'always' route the signaling. In effect this sets up this Expressway as a gateway to Unified CM, and is the preferred option. The *Cisco Unified Communications Manager* and *Cisco Unified Communications Manager (8.6.1 or later)* zone profiles are pre-configured to 'always' route the signaling, thus no additional configuration is required providing one of these profiles is used.

Encrypted calls to endpoints registered to Unified CM

Endpoints registered to Unified CM need to be configured with a "SIP Secure profile" to provide encrypted media and call negotiation. If such a profile is not available by default, it will need to be created via **System > Security > Phone Security**.

See [Securing Cisco TelePresence Products](#) for further information on using the Cisco CTL Client and configuring Unified CM for secure communications.

Appendix 1: Federation

This section describes how to configure Expressway to provide IM, Presence, audio and video interoperability between Lync 2010/2013 and Cisco infrastructure and Cisco Jabber for the purpose of migrating to Cisco Jabber.

Note: The federation deployment discussed in this section has been tested at limited scale for the purpose of migration, and is therefore not supported as a permanent deployment in a production environment.

Partitioned Intra-Domain Federation

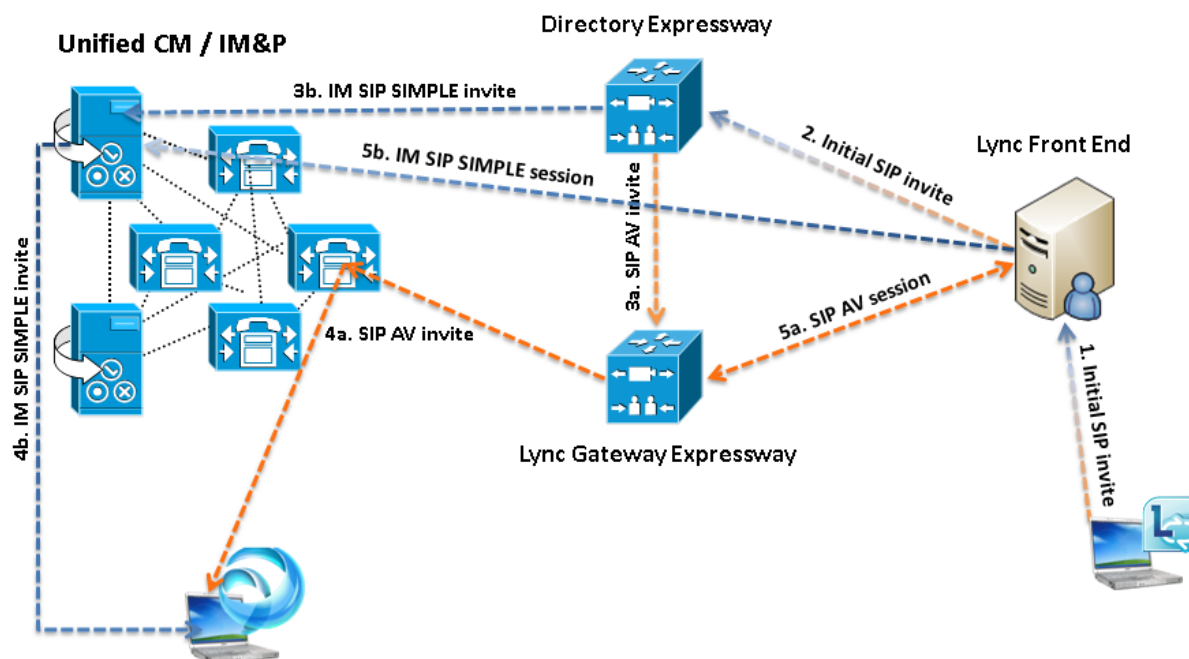
Partitioned Intra-Domain Federation is the sharing of enterprise Instant Messaging (IM), Presence, audio, and video between Unified Communications systems within a single presence / SIP domain. This model is used here as a migration tool from Microsoft Lync to Cisco infrastructure and Cisco Jabber.

Partitioned Inter-Domain Federation

Partitioned Inter-Domain Federation is the sharing of enterprise Instant Messaging (IM), Presence, audio, and video between Unified Communications systems deployed with different domains and subdomains. This model is also used here as an aid in migrating from Microsoft Lync to Cisco infrastructure and Cisco Jabber.

Solution overview

This solution requires a directory Expressway that uses CPL to split traffic coming from Lync. The directory Expressway routes audio / video traffic to the “Lync gateway” Expressway, and routes IM&P traffic to the Unified CM IM&P node, as shown in the following diagram:

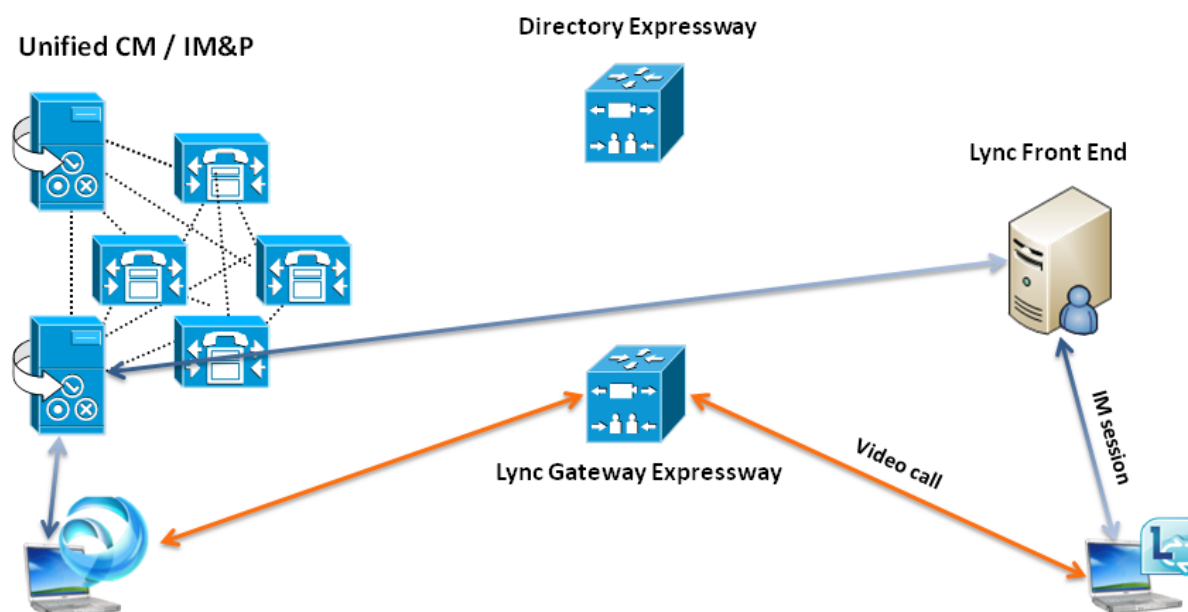


The IM&P and audio / video (AV) signaling flows are as follows:

1. A Lync user starts either a call or an IM session.
2. The Lync Front End routes it to the directory Expressway.

3. CPL on the directory Expressway splits the traffic according to the SDP event type and message headers:
 - a. **Audio / video signaling:** SIP AV invite is sent to the “Lync gateway” Expressway.
 - b. **IM&P signaling:** IM SIP SIMPLE invite is sent to the Unified CM IM&P node.
4. The invite is routed to the Jabber Client:
 - a. **Audio / video signaling:** SIP AV invite is routed to the Jabber Client through the “Lync gateway” Expressway and Unified CM.
 - b. **IM&P signaling:** IM SIP SIMPLE invite reaches the Jabber client through Unified CM IM&P.
5. The directory Expressway removes itself from signaling path:
 - a. **Audio / video signaling:** session is directly established between the Lync Front End and the B2BUA on the “Lync gateway” Expressway.
 - b. **IM&P signaling:** session is directly established between the Lync Front End and the Unified CM IM&P node.

The resulting IM and media paths are shown below:



Note that:

- The “Lync gateway” Expressway does the Microsoft SVC <> SVC or Microsoft SVC <> AVC conversion and encryption.
- The **Microsoft Interoperability Key** is required on the “Lync gateway” Expressway.

Configuring the directory Expressway

The directory Expressway serves the function of directing Lync traffic to the appropriate destination. It is required because Lync 2013 and Lync 2010 only support a single static route for all traffic to external domains. The CPL examines the SIP message and sends presence and IM messages to the IM&P server. All other messages are forwarded to the “Lync gateway” Expressway.

The directory Expressway configuration that is required is summarized below:

1. Ensure that the Expressway has rich media session licenses installed (**Maintenance > Option keys**). We recommend a minimum of 10 rich media session licenses.

The directory Expressway uses a license as it processes each call and it then holds on to the license until it times out, which takes 5 seconds. Thus, 10 rich media session licenses will allow up to 120 calls per minute (10 x 60 seconds / 5).

2. Configure a SIP neighbor zone that has a **Peer 1 address** set to the Lync Front End server.
3. Set **Call signaling optimization** to *On* (**Configuration > Call routing**) so that it removes itself from the signaling path.
4. Set **Call Policy mode** to *Local CPL* (**Configuration > Call Policy > Configuration**) and upload some CPL based on the example CPL below.

Example CPL

Here is an example of the CPL that you would load on to the directory Expressway:

```
<?xml version="1.0" encoding="UTF-8"?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl" xmlns:taa="http://www.tandberg.net/cpl-
extensions" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
<taa:rule-switch>
<!-- Route IM & presence messages SUBSCRIBE and PUBLISH direct to CUP -->
<taa:rule originating-zone="<To Lync Zone>" destination="(!CUP_.+)(.*)" message-
  regex="( (SUBSCRIBE|PUBLISH) (. *Event: (\s) *presence. *)) | ((. *m=message. *)) ">
<!-- Add CUP_ as a header to identify all messages destined for CUP. Strip CUP_ in search
rule -->
<taa:location clear="yes" regex="(.*)" replace="CUP_\1">
<proxy />
</taa:location>
</taa:rule>
</taa:rule-switch>
</taa:routed>
</cpl>
```

The **<To Lync Zone>** element should be replaced by the name of the neighbor zone that you have created on the directory Expressway that is pointed at Lync.

Modifying the Lync static route configuration

As the SDP messages coming from the Lync environment have to be analyzed by the directory Expressway, all the traffic coming from Lync must be directed to that Expressway. Therefore the static route configured on the Lync Server that routes calls to the address of the “Lync gateway” Expressway has to be modified to route calls to the address of the the directory Expressway instead.

Appendix 2: Troubleshooting

Troubleshooting checklist

If you are experiencing a problem with the Lync integration, we recommend that you go through the following list when performing the initial faultfinding. It will help to uncover any potential problems with the base configuration and status of the deployment:

- Ensure that video endpoints and infrastructure devices are running up-to-date software. Doing so lowers the chances for interoperability issues between the video environment and Lync.
- Ensure that all "Lync gateway" Expressways can successfully look up all Lync Server A-record FQDNs in DNS (this includes both Director and FEPs). You can use **Maintenance > Tools > Network utilities > DNS lookup** on the Expressway.
- Ensure that all Lync servers can successfully look up all "Lync gateway" Expressway peer A-record FQDNs and cluster FQDN in DNS. You can use the nslookup command-line utility locally on each Lync Server.
- Verify that the B2BUA has connectivity both with the Lync environment and the Expressway (on the **Status > Applications > Lync B2BUA** page, Status = Alive is the desired state for both).

Check for errors in the Event Log

Check the Event Log (**Status > Logs > Event Log**).

Tracing calls

Tracing calls at SIP / H.323 level

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.
4. (Optional) Enter some **Marker** text and click **Add marker**.
 - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
 - You can add as many markers as required, at any time while the diagnostic logging is in progress.
 - Marker text is added to the log with a "**DEBUG_MARKER**" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Download log** to save the diagnostic log archive to your local file system. You are prompted to save the archive (the exact wording depends on your browser).

Video endpoint reports that it does not support the Lync client SDP

If a video endpoint reports that it does not support the Lync client SDP, for example by responding "400 Unable to decode SDP" to a SIP INVITE message containing the Lync multi-part mime SDP sent to it:

1. Check whether the Lync Server is sending calls to the Expressway incoming IP port, rather than the B2BUA IP port that should be receiving the incoming SIP messages.
2. Reconfigure Lync Server to send calls to the B2BUA IP port.

TLS neighbor zone to Lync Server is active and messaging is sent from Expressway to Lync Server, but Lync debug says Lync fails to open a connection to Expressway

The local host name and domain name fields must be configured in the Expressway **System > DNS** page so that Expressway can use its hostname (rather than IP address) in communications. Lync requires the use of Expressway hostname so that it can open a TLS connection to the Expressway.

Lync client initiated call fails to connect

If a call fails to connect, check that the endpoint, IP Gateway, MCU or ISDN Gateway is NOT in Microsoft mode; ensure that it is in Standard or Auto mode. (From a H.323/SIP trace, an indication that the device is in Microsoft mode is the presence of a “proxy=replace” field in the contact header of the 200 OK from the device.)

Lync responds to INVITE with ‘488 Not acceptable here’

There can be two causes for this message:

From IP address

This is normally seen if the B2BUA forwards an INVITE from a standards-based video endpoint where the ‘From’ header in the SIP INVITE only contains the IP address of the endpoint, e.g. “From: <sip:10.10.2.1>;tag=d29350afae33”. This is usually caused by a misconfigured SIP URI in the endpoint. In future versions of B2BUA, the “From”-header will be manipulated if necessary to avoid this issue.

Encryption mismatch

Look for the reason for the 488. If it mentions encryption levels do not match, ensure that you have configured encryption appropriately, either:

- “Lync gateway” Expressway has the **Microsoft Interoperability** option key included, or
- Lync is configured such that encryption is supported (or set as “DoNotSupportEncryption”) – note that if the encryption support is changed on Lync then a short time must be left for the change to propagate through Lync Server and then the Lync client must be signed off and then signed back in again to pick up the new configuration.

Call connects but clears after about 30 seconds

If a call connects but shortly later clears, this is likely to be because the caller’s ACK response to the 200 OK is not being properly routed. To resolve this, make sure that the Expressway and Lync servers are able to resolve each other’s FQDNs in DNS.

Expressway to Lync Server calls fail – DNS server

Expressway needs to have details about DNS names of Lync pools and servers, and therefore needs to have one of its DNS entries set to point to a DNS server which can resolve the FQDNs of the Lync pools and

servers.

Expressway to Lync calls fail – Hardware Load Balancer

If the Lync environment has FEPs with an HLB in front, ensure that the Expressway is neighbored with the HLB. If it is neighbored with an FEP directly, trust for Expressway will be with the FEP. Expressway will send call requests to the FEP, but the FEP will record-route the message such that the ACK response should be sent to the HLB. The ACK sent to the HLB gets rejected by Lync Server, so Lync clears the call after the SIP timeout due to the FEP not seeing the ACK.

(Calls from Lync client – registered to the FEP – to Expressway may still work.)

Media problems in calls involving external Lync clients connecting via an Edge server

RTP over TCP/UDP

The Edge server supports RTP media over both TCP and UDP, whereas the B2BUA and standards based video endpoints only support RTP over UDP. The Edge server and any firewalls that the Edge server may pass media traffic through may need to be reconfigured to allow RTP over UDP as well as RTP over TCP to be passed.

ICE negotiation failure

This can usually be detected by the call clearing with a BYE with reason header “failed to get media connectivity”.

Video endpoints only support UDP media. ICE usually offers 3 candidates:

- Host (private IP)
- Server Reflexive (outside IP address of firewall local to the media supplying agent – B2BUA or Lync Client)
- TURN server (typically the Edge Server/Expressway-E)

For ICE to work where an endpoint is behind a firewall, the endpoint must offer at least one publicly accessible address (the Server Reflexive address or the TURN server address). This is used both for the B2BUA to try and send media to, but also to validate bind requests sent to the Expressway-E's TURN server – bind requests are only accepted by the TURN server if they come from an IP address that is ‘known’.

If a Lync INVITE offers only host candidates for UDP, for example:

```
a=candidate:1 1 UDP 2136431 192.168.1.7 30580 typ host
a=candidate:1 2 UDP 2135918 192.168.1.7 30581 typ host
a=candidate:2 1 TCP-ACT 1688975 192.168.1.7 30580 typ srflx raddr 192.168.1.7 rport 30580
a=candidate:2 2 TCP-ACT 1688462 192.168.1.7 30580 typ srflx raddr 192.168.1.7 rport 30580
```

...only one UDP candidate (two lines, one for RTP and one for RTCP) and they are for the host (private, presumably non-routable by Expressway address)

and the B2BUA responds, for example:

```
a=candidate:1 1 UDP 2136431 84.233.149.125 56056 typ host
a=candidate:1 2 UDP 2136430 84.233.149.125 56057 typ host
a=candidate:4 1 UDP 1677215 194.100.47.5 60000 typ relay raddr 84.233.149.125 rport 56056
a=candidate:4 2 UDP 1677214 194.100.47.5 60001 typ relay raddr 84.233.149.125 rport 56057
```

...Host and Relay candidates are both offered.

Neither device will be able to reach the other's private (host) address, and if the Lync client tries to bind to the Expressway-E TURN server it will get rejected because the request will come from the server reflexive address rather than private address and Lync client has not told the B2BUA what that IP address is.

Thus, Lync Server and the Microsoft Edge Server must be configured such that a Lync client offers at least one public address with UDP media for this scenario to work.

Note that in the above scenario the B2BUA may not offer the Server Reflexive address if the Server Reflexive address is seen to be the same as the host address.

Call between endpoint and Lync fails with reason 'ice processing failed'

If the search history on Expressway shows calls failing with 'ice processing failed', this means that all ICE connectivity checks between the B2BUA and the remote Lync device have failed.

Verify that the TURN server on Expressway-E has been enabled and that the TURN user credentials on Expressway-E and B2BUA configuration match properly. This failure could also indicate a network connectivity issue for STUN/TURN packets between B2BUA, Expressway-E/TURN server and the far end TURN server/Microsoft Edge.

One way media: Lync client to Expressway-registered endpoint

When using Microsoft Edge Server

When Lync clients register to Lync through a Microsoft Edge Server, the local IP address and port that the Lync client declares is usually private and un-routable (assuming that the Lync client is behind a firewall and not registered on a public IP address). To identify alternate addresses to route media to, the Lync client uses SDP candidate lines.

Calls traveling through the Microsoft Edge server are supported when using the B2BUA with the **Microsoft Interoperability** option key applied to the "Lync gateway" Expressway, and where the video architecture includes a Expressway-E with TURN enabled and the B2BUA is configured to use that TURN server.

When using a Hardware Load Balancer in front of Lync

Expressway modifies the application part of INVITEs / OKs received from Lync clients to make them compatible with traditional SIP SDP messaging. Expressway only does this when it knows that the call is coming from Lync. If there are problems with one-way media (media only going from Lync client to the Expressway registered endpoint), check the search history and ensure that the call is seen coming from a Lync trusted host. Otherwise, the call may be coming from a FEP rather than the load balancer. See ["Lync gateway" Expressway configuration \(part 2\) \[p.34\]](#) and configure Lync trusted hosts containing the FEP IP addresses.

Lync rejects Expressway zone OPTIONS checks with '401 Unauthorized' and INFO messages with '400 Missing Correct Via Header'

- A response '400 Missing Correct Via Header' is an indication that Lync does not trust the sender of the message.
- A response '401 Unauthorized' response to OPTIONS is another indication that Lync does not trust the sender of the OPTIONS message.

Ensure that Lync environment has been configured to trust the Expressway which is sending these messages, as described previously in this document.

Note, this can also be seen if a load balancer is used in front of the Lync, and Lync is configured to authorize the Expressway (Lync sees calls coming from the hardware load balancer rather than from the Expressway).

Lync client stays in 'Connecting ...' state

Lync client does not change into the connected state until it receives RTP (media) from the device with which it is in a call.

Call to PSTN or other devices requiring caller to be authorized fails with 404 not found

In some Lync configurations, especially where Lync PSTN gateways are used, calls are only allowed if the calling party is authorized. Thus, the calling party's domain must be the Lync Server domain. This means that the endpoints must register to the video network with a domain that is the same as the Lync domain.

Lync clients try to register with Expressway-E

SIP video endpoints usually use DNS SRV records in the following order to route calls to Expressway:

- `_sips._tcp.<domain>`
- `_sip._tcp.<domain>` and
- `_sip._udp.<domain>`

Lync clients use:

- `_sipinternaltls._tcp.<domain>` - for internal TLS connections
- `_sipinternal._tcp.<domain>` - for internal TCP connections (only if TCP is allowed)
- `_sip._tls.<domain>` - for external TLS connections

Lync clients only support TLS connection to the Edge Server. The `_sip._tcp.<domain>` DNS SRV record should be used for the Expressway-E.

B2BUA problems

B2BUA Lync Server status reports "Unknown" or "Unknown failure"

Check that the Expressway application has been added to the Lync trusted application pool and is configured to contact the Expressway B2BUA via port 65072 . See [Trust a "Lync gateway" Expressway \[p.31\]](#) for more information.

Lync problems

Run the Lync Server 'Best Practices Analyzer' to help identify configurations that may be incorrect on Lync Server.

Details and the download for Lync Server 2010 can be found at <http://www.microsoft.com/en-us/download/details.aspx?id=4750> and Lync Server 2013 content is at <http://www.microsoft.com/en-us/download/details.aspx?id=35455>.

Problems with certificates

If a non-Lync application is used to create certificates to load onto Expressway for use with Lync (for example when purchased from a certificate authority) it is vital that the Subject name and Subject Alternate Name contain the same details as they would if the certificates were created by Lync.

Specifically, if both Subject name and Subject Alternate Name are used, then the name entered in the Subject name must also appear in the Subject Alternative Name list.

See also [*Expressway Certificate Creation and Use Deployment Guide*](#).

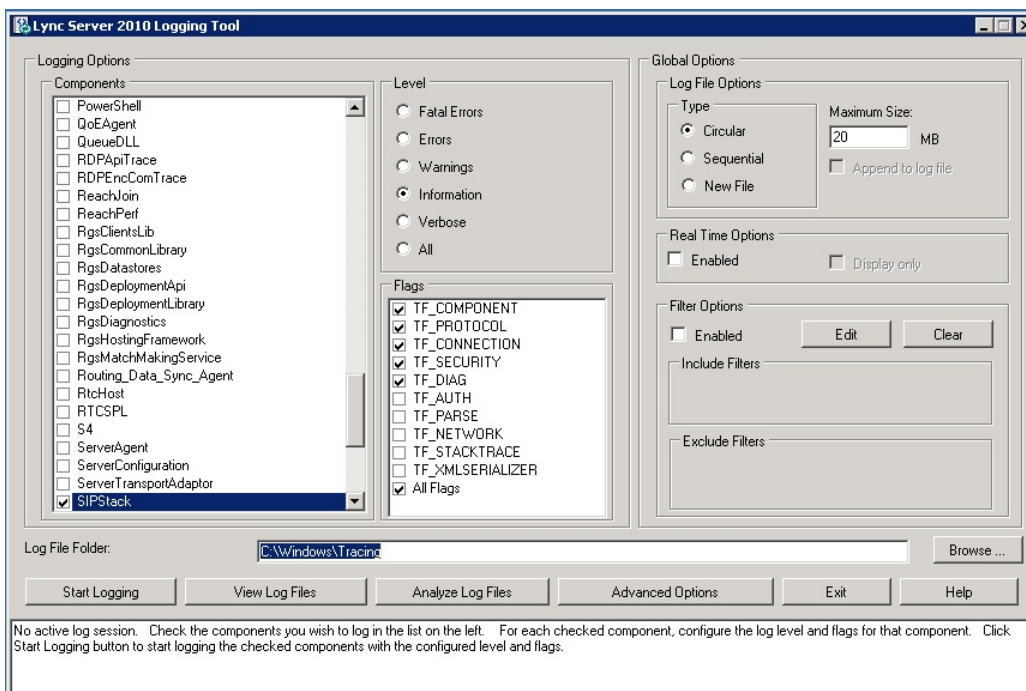
Appendix 3: Debugging on Lync

Use of Lync Server Logging Tool

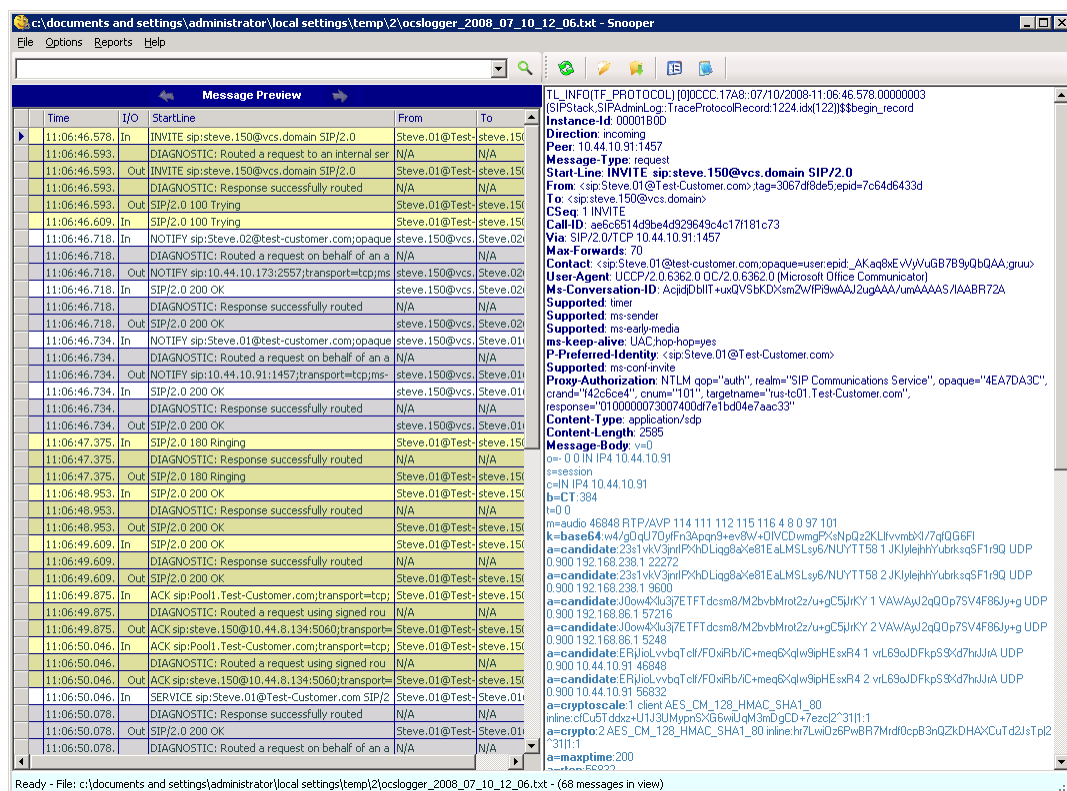
For debugging it is important to enable the logging on the appropriate Lync pool. If a Lync Director is in use, tracing here is a good starting point.

Looking at the record-route headers in SIP messages from Lync will identify the FEP and Director involved in the call.

1. On Lync Server select **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Logging Tool**.



2. Select the logging option, for example SIPStack to look at SIP logs. (Details about the logging tool may be found at: <http://technet.microsoft.com/en-us/library/gg558599.aspx>.)
3. Click **Start Logging**.
4. Make the call, or perform the function that needs to be debugged.
5. Click **Stop Logging**.
6. Click **Analyze Log Files** (install the Lync Server Resource Kit Tools if prompted to do so).
7. Review the trace:



Enabling debug on Lync client

If the Lync client is not working correctly, logging can be enabled and SIP messaging and other logging can be checked.

1. Select **Tools > Options**.
2. Select the **General** tab.
3. In the **Logging** section:
 - a. Select **Turn on logging in Lync**.
 - b. Select **Turn on Windows Event logging for Lync**.

Lync log files may be found in: c:\Documents and Settings\<user>\Tracing where <user> is the login name of the windows login.

The **.uccplog** file can be viewed with a text editor, or (more clearly) with the application provided in the Lync resource kit 'snooper.exe'.

Windows event logging can be observed using the Windows Event Viewer.

Appendix 4: Interoperating capabilities and limitations

Known interoperating capabilities

Upspeeding from a voice call to a video call

If a voice call is made from a Lync client to a video endpoint registered to Unified CM and then the video button is selected to enhance the call to a video call, the video endpoint will correctly upspeed to video.

When interworking a Lync client to an H.323 endpoint, the call will only upspeed from voice to video if the upspeed request occurs before the endpoint sends a BRQ lowering the connection bandwidth.

Maximum call resolution

The maximum resolution of an SVC to AVC converted call is 720p 30fps.

Known interoperating limitations

Video codecs

If Lync 2010 is used, the video endpoints registered to the Unified CM must support H.263; this is the common video codec supported by endpoints and the Lync client. (The Lync client does not support H.264.)

The Lync 2010 client for Apple Mac OS X only supports RTVideo, no standards-based video codecs (H.263 or H.264). To make video calls between this client and standards-based video endpoints, a Cisco AM GW is needed to transcode between RTVideo and H.263/H.264.

Video codec selection

When the B2BUA receives a call with no SDP – that is, without a list of codecs that can be used for the call (for example, a call that has been interworked from H.323), the B2BUA must populate the SDP with a “pre-configured” list of codecs from which Lync can select, as Lync does not support INVITES with no SDP.

The codecs offered and selected, therefore, may not reflect the best codecs that could have been selected by the endpoints.

MXP endpoints

Video from MXP endpoints to Lync 2013 H.264 SVC is limited to 15fps (video with other endpoints is 30fps).

Joining a Lync conference (AV MCU)

Using a Lync client to invite a third party to join the call does not work if the third endpoint is an endpoint registered to the Unified CM, or if the endpoint registered to the Unified CM is already in the call and another Lync client is introduced into the call.

This is because when the Lync client invites a third party to join a call, the Lync client tries to create a conference using Microsoft proprietary messaging (xml in SIP messages), and this is not supported by standards-based video endpoints.

Upspeeding from a voice call to a video call

Interworking a Lync client to an H.323 endpoint, the call will only upspeed from voice to video if the upspeed request occurs before the endpoint sends a BRQ lowering the connection bandwidth.

Microsoft Mediation Server

Calls to Microsoft Mediation Servers work from endpoints in the Expressway video network for SIP initiated calls, but do not work for interworked H.323 initiated calls (the mediation server does not respond to the Expressway INFO message, sent to check availability of the destination number).

A workaround is possible if the format of the numbers that will be routed to the mediation server can be configured in Expressway.

The workaround is to send some calls through a different zone from the "Lync gateway" Expressway to the Lync Server, as follows:

1. Create a new neighbor zone and select *Custom* in the **Zone profile** field.
2. Configure the zone with the values shown in [Table 1: Custom neighbor zone attributes to work around Mediation Server limitation \[p.63\]](#)
3. Configure one or more search rules, with the correct priority, such that the appropriate subset of calls destined for the Mediation Server are routed through the new zone rather than the standard "To Microsoft Lync Server via B2BUA" zone.
4. You may also need to change the **On successful match** action from *Stop* to *Continue* on the search rule in the "To Microsoft Lync Server via B2BUA" zone. See [Set up a search rule to route calls to the Lync domain to Lync \[p.35\]](#).

Table 1: Custom neighbor zone attributes to work around Mediation Server limitation

Setting	Lync Server zone configuration
Monitor peer status	Yes
Call signaling routed mode	Auto
Automatically respond to H.323 searches	Off
Automatically respond to SIP searches	On
Send empty INVITE for interworked calls	Off
SIP poison mode	On
SIP encryption mode	Microsoft
SIP SDP attribute line limit mode	On
SIP SDP attribute line limit length	130
SIP multipart MIME strip mode	On
SIP UPDATE strip mode	On
Interworking SIP search strategy	Info
SIP UDP/BFCP filter mode	Off
SIP Duo Video filter mode	On

Table 1: Custom neighbor zone attributes to work around Mediation Server limitation
(continued)

Setting	Lync Server zone configuration
SIP record route address type	Hostname
SIP Proxy-Require header strip list	<blank>

Lync client reports no audio device

Lync client sometimes complains that it has no audio device configured when selecting resume ... follow Lync client's instructions to update the audio device and resume will then work.

Appendix 5: Port reference

The port numbers listed below are the default port values. The values used in a real deployment may vary if they have been modified, for example, by changes of registry settings or through group policy, on Lync and Lync client, or configuration on Expressway ([Applications > B2BUA](#)).

Between B2BUA and Lync

Purpose	Protocol	B2BUA IP port	Lync IP port
Signaling to Lync Server	TLS	65072	5061 (Lync signaling destination port)
Signaling from Lync Server	TLS	65072	Lync ephemeral port
Media (the Lync B2BUA should be deployed on a separate "Lync Gateway" Expressway and thus there should be no conflict with the standard traversal media port range)	UDP	56000 to 57000	Lync client media ports

Note: The Expressway does not forward DSCP information that it receives in media streams.

Between B2BUA and Expressway (internal communications)

Purpose	Protocol	B2BUA IP port	Expressway IP port
Internal communications with Expressway application	TLS	65070	SIP TCP outbound port

Between B2BUA and Expressway-E hosting the TURN server

Purpose	Protocol	B2BUA IP port	Expressway-E IP port
All communications	UDP	56000 to 57000	3478 (media/signaling) *

Ensure that the firewall is opened to allow the data traffic through from B2BUA to Expressway-E.

* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

External Lync client and Edge server

Purpose	Protocol	Edge server	Lync client
SIP/MTLS used between Lync Client and Edge server for signaling (including any ICE messaging to the Edge Server)	TCP	5061	5061
SIP/TLS	TCP	443	443

Purpose	Protocol	Edge server	Lync client
STUN	UDP	3478	3478
UDP Media	UDP	50000-59999	1024-65535
TCP Media	TCP	50000-59999	1024-65535

External Lync client / Edge server and Expressway-E

Purpose	Protocol	Lync client / Edge server	Expressway-E
ICE messaging (STUN/TURN) if media is sent via the Expressway-E	UDP	3478	3478
UDP media if it is sent via the Expressway-E	UDP	1024-65535	24000-29999

Between B2BUA and transcoder

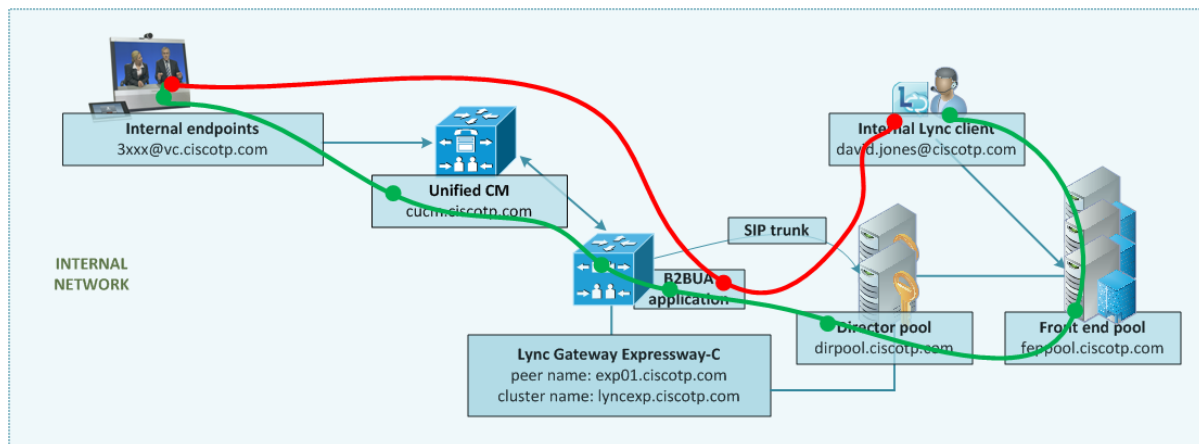
Purpose	Protocol	B2BUA IP port	Transcoder
B2BUA communications with transcoder (Cisco AM GW)	TLS	65080	5061

Appendix 6: Media paths and license usage for calls through B2BUA

Lync client call to SIP video endpoint

For a call of this type:

- Signaling flows through Lync, B2BUA, and Unified CM.
- Media is connected directly between the Lync client and the B2BUA.
- Media is connected directly between the internal video endpoint and the B2BUA (as the call is SIP to SIP).
- Calls made in the opposite direction, internal video endpoint to Lync client use the same signaling and media paths.
- Licenses:
 - 1 rich media session license on “Lync gateway” Expressway

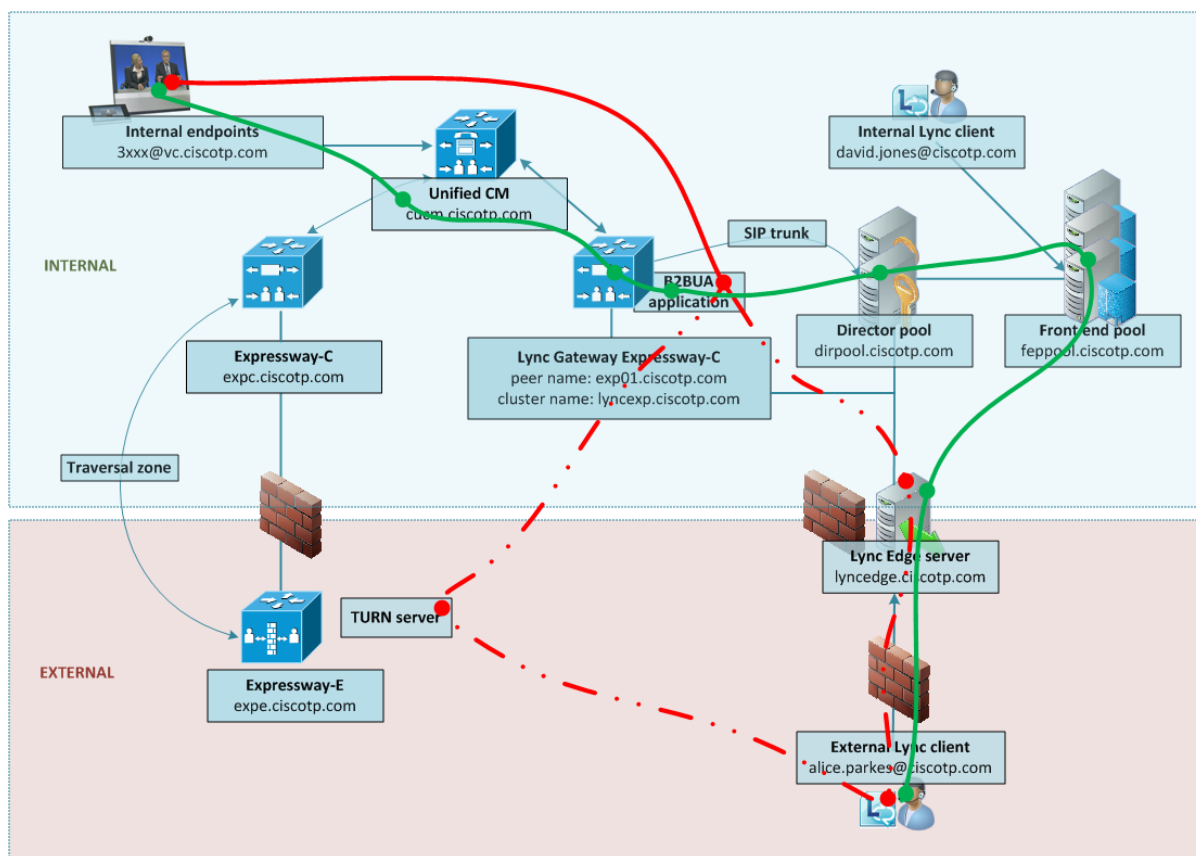


— Signaling
— Media

An external Lync client calls an internal SIP video endpoint

In this scenario an external Lync client (alice.parkes) calls an internal video system (david.jones.office).

- Signaling flows through the Microsoft Edge Server, Lync, B2BUA, and Unified CM.
- Media between the Lync client and the B2BUA flows either through the Microsoft Edge server or through the Expressway-E TURN server – ICE searching is used to determine the 'best' path.
- Media is connected directly between the internal video endpoint and the B2BUA (as the call is SIP to SIP).
- Calls made in the opposite direction, internal video endpoint to external Lync client will use the same signaling and media paths.
- Licenses:
 - 1 rich media session license on “Lync gateway” Expressway



Appendix 7: Additional information

TEL URI handling for Expressway to Lync calls

If an endpoint wants to dial a telephone number rather than selecting a user from a directory, the Unified CM must format the telephone number appropriately for Lync to be able to look it up. Lync expects to see telephone numbers (known as TEL: URIs) in the form: **+<country code><full dialed number>**

Unified CM can use transforms to appropriately format the telephone numbers. These transforms can either be implemented globally using **Configuration > Dial plan > Transforms** or just for the Lync neighbor zone or B2BUA neighbor zone by configuring the transform in the appropriate search rules.

For example, for 4 digit extension number dialing to be expanded to a full telephone number for a company in the UK whose telephone number is 781xxx, an extension number 1008 would need to be expanded to +441344781008. This can be implemented by configuring a transform as follows:

Priority	80 (match in preference to the no transform needed rule - 80 is higher priority than 100)
Source	<i>Any</i>
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	<code>(1...)@ciscotp\com(.*)</code>
Pattern behavior	<i>Replace</i>
Replace string	<code>+44134478\1;@ciscotp.com;user=phone\2</code>
On successful match	<i>Continue</i>
Target Zone	<i>To Microsoft Lync Server via B2BUA</i>

Document revision history

The following table summarizes the changes that have been applied to this document.

Date	Description
September 2015	Reissued X8.5 document to address CSCus01195.
December 2014	Updated for X8.5.
July 2014	Reissued X8.2 document to address CSCup55116.
June 2014	Reissued X8.2 document to include Federation information.
June 2014	Republished for X8.2.
December 2013	Initial release.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.