



Cisco Expressway with Microsoft Lync

Deployment Guide

First Published: December 2013

Last Updated: December 2015

Cisco Expressway X8.6

Microsoft Lync Server 2010 or 2013

Preface

Change History

Table 1 Cisco Expressway with Microsoft Lync Deployment Guide Change History

Date	Change	Reason
December 2015	Republished.	Scope of support for Lync screen sharing in point to point scenarios clarified.
December 2015	Republished.	Screen sharing from Lync now supported with MCU conferences.
November 2015	X8.6 version republished.	Scope of support for screen sharing from Lync clarified.
August 2015	X8.6 Expressway version republished.	Screen share topology diagrams corrected.
July 2015	Document revised and restructured. Screen sharing from Lync feature added.	X8.6 release.
December 2014	Updated.	X8.5 release.
July 2014	X8.2 version revised.	Content defect CSCup55116.
June 2014	X8.2 version revised to include Federation appendix.	New information.
June 2014	Updated.	X8.2 release.
December 2013	Initial release of Expressway version of this document.	Expressway product launched.

Introduction

This deployment guide describes how to configure a Cisco Collaboration video network to interwork with a Microsoft Lync environment, using the back to back user agent (B2BUA) on the Cisco Expressway (Expressway).

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

To enable video calling and desktop sharing between Cisco Unified Communications Manager-registered collaboration endpoints and Lync clients, you need to configure:

- A SIP trunk between the Gateway Expressway and Unified CM
- The Lync B2BUA on the Gateway Expressway to route calls to Lync
- Static routes from Lync to the Gateway Expressway

Deployment Scope

The following major Expressway-based deployments are mutually exclusive. They cannot be implemented together on the same Expressway (or traversal pair):

- Mobile and Remote Access
- Microsoft Lync Interoperability
- Jabber Guest

What is the Gateway Expressway and Why Should I Use It?

A Gateway Expressway is an Expressway-C (or cluster of Expressway-Cs) that provides interoperability between a Cisco Collaboration network and the Microsoft Lync environment.

We require that you dedicate an Expressway-C to this role so that you:

- Minimize the impact of adding Lync interoperability to your existing Cisco Collaboration network.
- Limit the number of Expressways that need the **Microsoft Interoperability** option key.
- Reduce the number of static routes that you need to define from the Lync environment.
Each static route matches a single SIP domain to a single FQDN, or IP address, but you can create appropriate DNS records to map this destination to a cluster of Expressways.
- Reduce the number of third-party applications that you configure Lync to trust.
Lync Server will only accept SIP messages from peers that it trusts. By dedicating a Gateway Expressway (or cluster), you reduce the number of trusted devices that you need to configure in Lync.

Recommendations

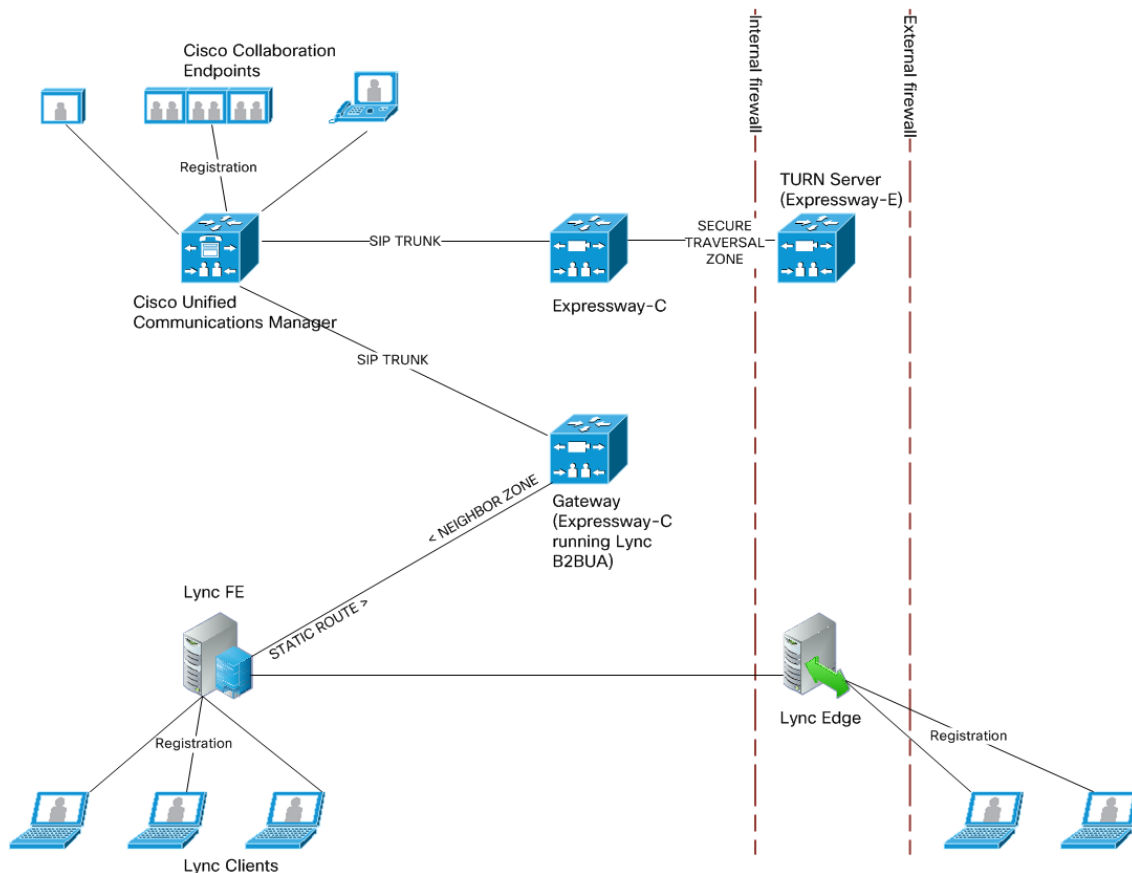
- We recommend that you use TLS connectivity throughout the deployment. We do not recommend TCP because:
 - Lync uses TLS by default
 - TCP prevents the use of encryption
 - TCP may not work for Lync Server environments that include hardware load balancers (HLBs) and / or Lync Director
 - A static route using TCP must go to the destination IP address. So, with TCP you cannot get redundancy from a clustered Gateway Expressway, which you can when you configure a TLS static route to the cluster's FQDN

- If the Gateway is a cluster, you must configure the master peer and allow the configuration to be replicated to the other peers automatically. When you see the **+** in the web interface, it indicates that a field must be completed on each peer.

Deployment Components

We are integrating your Microsoft® Lync environment with your video network to provide video calling and desktop sharing between Cisco Collaboration endpoints and Microsoft Lync clients.

Figure 1 Topology used in this deployment guide



What's in the diagram?

The Lync deployment has:

- A pool of Lync Servers with Front End Server role (one server shown for clarity)
- A Lync Server with Edge Server role
- Internal Lync clients registered to Lync FE
- External Lync clients registered to Lync Edge

The Cisco video deployment has:

- Unified CM
- Internal Cisco Collaboration endpoints registered to Unified CM
- A dedicated Gateway Expressway-C (referred to as Gateway Expressway)

- Cisco Expressway-C and Cisco Expressway-E for TURN server support

Example Values in this Deployment

The example presented uses the following values:

- The Lync environment uses `example.com` as the SIP domain. 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 `video.example.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@example.com`
 - Alice with a URI `alice.parkes@example.com`
- Lync Front End Server is configured with a static domain route which routes URIs with the Expressway's video network domain (`video.example.com`) to the Gateway Expressway. Take care when using domain static routes; any traffic for that domain that Lync cannot handle locally will be routed to Expressway.

Features and Limitations

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

This topic describes more detailed aspects of the integrated environments.

Voice and Video Calling

SIP Calls

- SIP endpoints registered to Unified CM can make calls to Lync clients registered to Lync Server.
- Lync clients registered to Lync Server can make calls to SIP endpoints registered to Unified CM.
- 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.
- Media encryption (SRTP) is supported when TLS is used between Expressway and Lync and the **Microsoft Interoperability** option key is added to the Gateway Expressway.
- 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).
- The maximum resolution of an SVC to AVC converted call is 720p 30fps.
- Lync client sometimes notifies 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.

Upspeeding a Voice Call to Video

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

MXP Endpoints

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

Screen Sharing

- Lync clients can share their screen with standards-based endpoints in the video network, because the Gateway Expressway can transcode RDP media into H.264.
- The reverse transcode (from H.264 to RDP) is not supported. If the endpoint is capable of putting the presentation in the main video channel, then the Lync user can see the presentation that way. Otherwise, if the parties are in a conference, the conference bridge will compose the presentation (from the standards-based endpoint) into the main video it sends to the Lync user.
- Lync 2013 for Windows is the required client version for screen sharing. Other client versions are not supported for this feature.
- Lync Server 2013 is the required server version for screen sharing. Other server versions are not supported for this feature.
- Screen share transcoding is not supported on a clustered Gateway Expressway.
- Screen sharing from Lync is supported when the Lync client is in a conference on a Cisco TelePresence Server.
- Screen sharing from Lync is supported when the Lync client is in a conference hosted on MCU 5300 Series or MCU MSE Series bridges, with the following caveats:
 - When another endpoint steals the floor from the Lync presenter, the MCU does not revoke the floor. Lync looks like it is still sharing, from the original presenter's point of view, when the other participants are not seeing the Lync screen. See issue number [CSCux48258](#).
- Screen sharing from Lync is not supported when the Lync client is in conferences hosted on MCU 4200 Series and MCU 4500 Series bridges.
- Point to point calls with screen sharing from Lync have been tested and validated with TC, CE, and DX endpoints, with the following caveats:
 - TC endpoints must be running TC version 7.2 or later to be able to compose main video and content when they are presenting.
 - CE endpoints must be running CE version 8.0 or later to be able to compose main video and content when they are presenting.
 - DX Series endpoints must be running firmware version 10.2(5) or later. The DX Series cannot compose content and main video, so Lync users will see the content instead of the main video when these endpoints are presenting.
- We do support screen sharing from Lync to SIP or H.323 standards-based endpoints, but we cannot explicitly test and validate all cases.
If you're using H.323 endpoints, you need infrastructure for registering H.323 endpoints, e.g. a VCS Control. That infrastructure is not documented in this deployment guide.
- Cisco Jabber Video for TelePresence is not supported for screen sharing from/to Lync.
- Cisco Jabber is not supported for screen sharing from/to Lync.

Screen Sharing Performance Considerations

On all platforms, the default maximum number of concurrent transcoding sessions is 10. We recommend the following numbers, depending on your platform:

Table 2 Recommended Number of Desktop Transcode Sessions by Platform

On this platform:	Set Maximum RDP transcode sessions to:
CE500, CE1100 [†] , or Medium OVA	10
CE1000, CE1100 [†] , or Large OVA	20
Note: This recommendation requires an active 10 Gbps network connection.	

‡ The CE1100 appliance operates with Medium capacity if you install 1 Gbps NICs, or with Large capacity if you install 10 Gbps NICs.

These numbers were chosen conservatively. They are based on the additional CPU load caused by transcoding 1920 by 1080 screens while the Gateway Expressway was processing 100 concurrent 720p video calls from Lync.

If you want to increase the maximum number of sessions, consider the following:

- A screen share transcoding session requires more media ports than a video call, so you may need to increase the media port range; the default range accommodates 100 video calls, 20 of which are sharing their desktop.
- Screen share transcoding loads the CPU more heavily than video (AV) calls. Testing shows that CPU load increases in a roughly linear way when increasing the number of transcode sessions. There is a similar characteristic when increasing the number of AV calls without screen sharing, so you should be able to get more shares if the Expressway is processing fewer concurrent AV calls overall.
- Higher resolutions and/or multiple monitors also affect performance. The transcoder will output the same resolution that it receives from Lync, up to a maximum resolution of 1920x1200. Beyond that, the transcoder will scale the shared screen down to fit within 1920x1200. If the received resolution exceeds 3840x2160, the transcoder crops the screen to fit within that resolution before scaling it down. The transcoder will also scale down if it needs to respond to constraints on resources, for example, bandwidth limitations.

Screen Sharing Deployments

The following deployments support screen sharing from Lync:

Figure 2 Lync environment to conference managed by TelePresence Conductor trunked to Unified CM

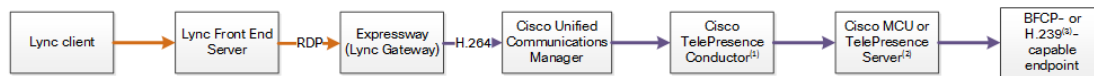


Figure 3 Lync environment to SIP endpoint registered to Unified CM



Notes:

1. If you are using the Optimize Resources feature with Lync screen sharing, you need TelePresence Conductor version XC4.0 or later.
2. If you are using the Optimize Resources feature with Lync screen sharing, you need TelePresence Server version 4.2 or later.
3. Requires Cisco VCS Control for H.323 registrations, not shown in the diagram.

Lync Environment

The scale of your Lync deployment could mean that your deployment model is more complex than what is described in this guide. [Appendix 2: Extended Lync Deployments, page 56](#) describes some of the different options and how the deployment model will vary in each case.

Lync Client Versions

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](#).

Lync 2013 for Windows and Lync 2010 for Windows can call Unified CM-registered endpoints. Lync 2011 for Mac cannot do this, it uses an unsupported video codec.

Lync Server Versions

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.

Screen sharing from Lync clients towards video network endpoints is not supported on Lync Server 2010.

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.

Skype for Business Server

Not supported.

Video Codecs

If you use Lync 2010 for Windows, the other video endpoints must support H.263; this is the common video codec supported by endpoints and the Lync client. (Lync 2010 for Windows does not support H.264)

The Lync 2010 client for Apple Mac OS X only supports RTVideo. It does not support H.263 or H.264. To make video calls between this client and Cisco Collaboration video endpoints, you need the Cisco AM GW 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.

Conferencing

Cisco TelePresence Server

Supported Lync clients can join conferences hosted on a TelePresence Server.

The TelePresence Server must be trunked to Unified CM or controlled by a TelePresence Conductor that is trunked to Unified CM.

Lync users can share their screen in a TelePresence Server conference. They will receive presentation from other participants in the composited video stream from the TelePresence Server.

Cisco TelePresence MCU Series

Supported Lync clients can join conferences hosted on a MCU.

The MCU must be trunked to Unified CM or controlled by a TelePresence Conductor that is trunked to Unified CM.

Lync users can share their screen in an MCU conference. They will receive presentation from other participants in the composited video stream from the MCU.

There is a known issue with the MCU which does not revoke the floor after it stops sharing the content from Lync. To the Lync user it looks like Lync is still sharing the screen, but other participants have stopped seeing the screen.

Lync Conference (AV MCU) not supported

When a point to point call involves a standards-based endpoint and a Lync client, a third party cannot be invited into the conference because the Lync client tries to start a Lync conference. The Expressway and the standards-based endpoints do not support endpoints joining Lync conferences.

Configuration

Prerequisites

Lync Environment

- Lync Servers are running Lync Server 2010 or Lync Server 2013.
- Lync is configured and operational and you have access to Active Directory for managing users.
- The Lync Server topology has successfully been validated using the Topology Validation Tool.
- Lync clients should be able to call each other (there is more detail on setting this up in [Verify Calls Between Lync Clients, page 62](#))

Cisco Collaboration Environment

- The dedicated Gateway Expressway(s) are running X8.1 or later. X8.6 or later is required for Lync screen sharing. X8.7 or later is required for Lync screen sharing through a clustered Gateway Expressway.
- The Expressway pair at the network edge is configured as described in *Cisco Expressway Basic Configuration Deployment Guide* on the [Cisco Expressway Configuration Guides page](#).
- Unified CM is trunked to the Cisco Expressway-C as described in *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* on the [Cisco Expressway Configuration Guides page](#).
- The Gateway Expressway(s) have a Rich Media Sessions option key.
- The Gateway Expressway(s) have a Microsoft Interoperability key.
- The Expressway-E must have a TURN Relays option key (for calls from off-site Lync users).
- Unified CM-registered endpoints should be able to call each other.

DNS Records

- The FQDNs of all Lync servers are resolvable by the DNS server used by the Gateway Expressway (Gateway and Lync Servers should use the same DNS server).
- The FQDNs of each Gateway Expressway is resolvable by DNS. If the Gateway Expressway is a cluster, the FQDN of the cluster must be resolvable by DNS (with a round-robin A-record for each peer).
- The DNS server must support reverse DNS lookup (typically by PTR records) if you enable TLS (recommended).



Configuration Overview

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

1. Unified CM-registered endpoints to call internal or external Lync clients registered to Lync ([Enable Calls to Lync, page 14](#))
2. Internal or external Lync clients to call Unified CM-registered endpoints ([Enable Calls from Lync, page 34](#) and [Enable Calls from External Lync Clients, page 41](#))
3. Application/desktop sharing from Lync clients to Unified CM-registered endpoints ([Enable Screen Sharing from Lync, page 42](#))

The configuration process describes each of these stages separately, so that individual stages can be implemented and tested before moving on to the next.



Enable Calls to Lync

Table 3 Overview of Tasks Required to Enable Calls from Collaboration Endpoints to Lync Clients (All Internal)

Command or Action	Purpose
Configure the Gateway Expressway, page 14	Prepare the Gateway Expressway to work in your environment: configure DNS and NTP, and enter a cluster name
Trunk the Gateway Expressway to Unified CM, page 16	To route calls destined for Lync domains towards the Gateway Expressway
Connecting Expressway to Unified CM Using TLS, page 22	Secure the trunk to the Unified CM to enable encrypted media between Unified CM registered endpoints and Lync clients
Configure Lync Server Environment , page 27	Enable SIP TLS, trust the Gateway Expressway, and configure media encryption
Configure the B2BUA and Search Rules on the Gateway Expressway, page 30	To route calls destined for Lync domains towards the internal Lync environment
Test Calls from Internal Endpoint to Internal Lync Client, page 33	To verify this part of the configuration.

Configure the Gateway Expressway

Table 4 Prepare the Gateway Expressway for the Network

Command or Action	Purpose
Task 1: Configure DNS and Local Hostname, page 14	So that the Gateway Expressway can resolve trusted Lync Servers (B2BUA hosts)
Task 2: Enter a Cluster Name, page 15	So that Lync Server static routes can resolve the Gateway Expresswaycluster
Task 3: Configure an NTP Server, page 16	To synchronize the Gateway Expressway with ththe Lync Server environment

Task 1: Configure DNS and Local Hostname

Configure the DNS Server Details

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

On a 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 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 Server, and specify the Lync domain e.g. example.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**.

Enter System Host Name and DNS Domain

Give each Gateway Expressway peer a unique **System host name** and check it has the correct **DNS Domain**:

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

Note:

- Concatenate **System host name** with **Domain name** to get the routable FQDN of this Expressway
- These items must be configured to properly enable TLS between Expressway and Lync Server environment. If they are not, the neighbor zone may go active and Expressway may send messaging to Lync Server, but Lync Server will never open a TLS connection back to Expressway.

Task 2: Enter a Cluster Name

Lync will be configured with a static route that always uses the Gateway Expressway's cluster name / FQDN.

For each Gateway Expressway peer (even if there is only one), ensure that **Cluster name (System > Clustering > Cluster name)** is the FQDN of the cluster. You would have created the FQDN when setting up the cluster. See *Expressway Cluster Creation and Maintenance Deployment Guide* for details of changing the cluster name.

Task 3: Configure an NTP Server

On each Gateway Expressway peer:

1. Go to **System > Time**.
2. Set **NTP server 1** to the IP address of an NTP server.
3. (Optional) Enter the details of additional NTP servers.
4. Set **Time zone** as appropriate to the location of the Expressway.

To find out which time server the Lync Server is using, enter `net time /queryntp` at the Windows command line.

Trunk the Gateway Expressway to Unified CM

Table 5 Task summary for trunking the Gateway Expressway to Unified CM

Command or Action	Purpose
Task 1: Check Unified CM Configuration, page 16	Check that Unified CM has the required configuration for trunking to Gateway Expressway.
Task 2: (Pre 9.x) Configure the SIP Profile for Expressway, page 17	Not required for Unified CM 9.x or later. Configure a SIP profile for Expressway.
Task 3: Configure the Region Session Bit Rate for Video Calls, page 19	Prepare the Unified CM region for higher bitrates required by video calls.
Task 4: Configure the SIP Trunk Security Profile, page 19	Prepare the non-secure SIP trunk profile for trunking to Gateway Expressway. Note: Not required if you are going to use SIP TLS on the trunk. This task is replaced by the corresponding task Configure a SIP Trunk Security Profile on Unified CM, page 25 , in the next section Connecting Expressway to Unified CM Using TLS, page 22 .
Task 5: Configure the SIP Trunk to the Gateway Expressway, page 19	Create the trunk to the Gateway Expressway.
Task 6: Configure the SIP Trunk to the Cisco Expressway-C, page 21	Create the trunk to the Cisco Expressway-C.
Task 7: Configure the Clusterwide Domain Enterprise Parameters, page 21	Check that the Unified CM has fully qualified domain in the same video network as the Gateway Expressway
Task 8: Check the Message Size Limit on Unified CM, page 22	Make sure the incoming SDP message size in Unified CM is set to an appropriate value. In older versions, the SDP message size was too small for video applications, but the default has changed to 11000 bytes.

Task 1: Check Unified CM Configuration


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

Task 2: (Pre 9.x) Configure the SIP Profile for Expressway

Note: This procedure does not apply to Unified CM versions 9.x and later, because the newer versions have a "Standard SIP Profile For Cisco VCS" (you can also use that profile for 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 ▼ Find Clear Filter ⬆ ⬇			
<input type="checkbox"/>	Name ▲	Description	Copy
	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

4. Click **Save**.

Task 3: Configure the Region 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**.

Task 4: Configure the SIP Trunk Security Profile

1. Go to **System > Security > SIP Trunk Security Profile**.
2. (Before version 9.x) Click **Add New** and name the new profile.
3. (9.x onwards) Select **Non Secure SIP Trunk Profile**.
4. 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

5. Click **Save**.

Task 5: Configure the SIP Trunk to the Gateway Expressway

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. For background, read Secure RTP between CUCM and VCS or Expressway Configuration Example
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**.

Task 6: Configure the SIP Trunk to the Cisco Expressway-C

If there is not already a trunk between the Unified CM and the Cisco Expressway-C, then you need to create one as described in *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* on the [Cisco Expressway Configuration Guides page](#).

Task 7: Configure 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 video.example.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 video.example.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.ciscoip.com
Cluster Fully Qualified Domain Name	vc.ciscoip.com

Task 8: Check the Message Size Limit on Unified CM

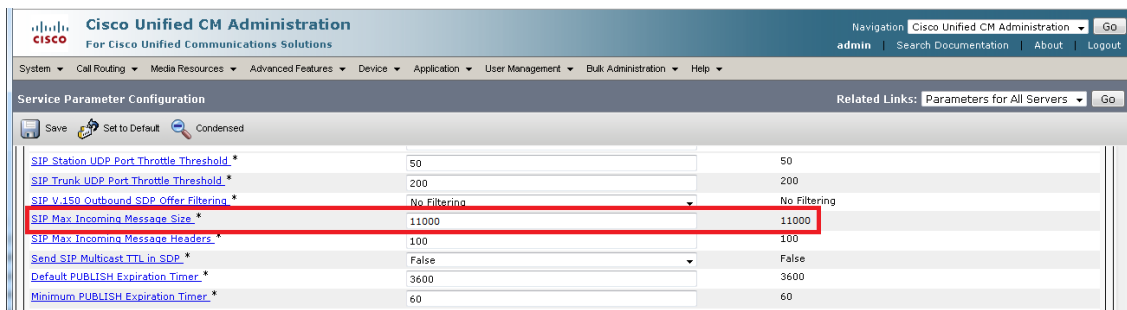
SIP messages for video are considerably larger than SIP messages for audio calls, in particular, when a Cisco TelePresence Server is used in the video network.

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**.



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 trunk to use TLS instead. This table summarizes the process:

Table 6 Overview of Tasks to Create SIP TLS Trunk Between Expressway and Unified CM

Command or Action
Ensure Certificate Trust Between Unified CM and Expressway, page 22
Set the Cluster Security Mode to Mixed Mode, page 24
Configure a SIP Trunk Security Profile on Unified CM, page 25
Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints, page 26
Update the Unified CM Trunk to Expressway to Use TLS, page 26
Update the Expressway Neighbor Zone to Unified CM to Use TLS, page 27
Verify That the TLS Connection is Operational, page 27

Ensure 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.

Load 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**.

Note: If you are using Unified CM version 8.5(1) or earlier and are having problems establishing a TLS connection between Expressway and Unified CM, we recommend adding the following x509 extended key attributes into the CSR:

- serverAuth (1.3.6.1.5.5.7.3.1) -- TLS Web server authentication
- clientAuth (1.3.6.1.5.5.7.3.2) -- TLS Web client authentication
- ipsecEndSystem (1.3.6.1.5.5.7.3.5) -- IP security end system

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.

Load 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.

Set the Cluster Security Mode to Mixed Mode

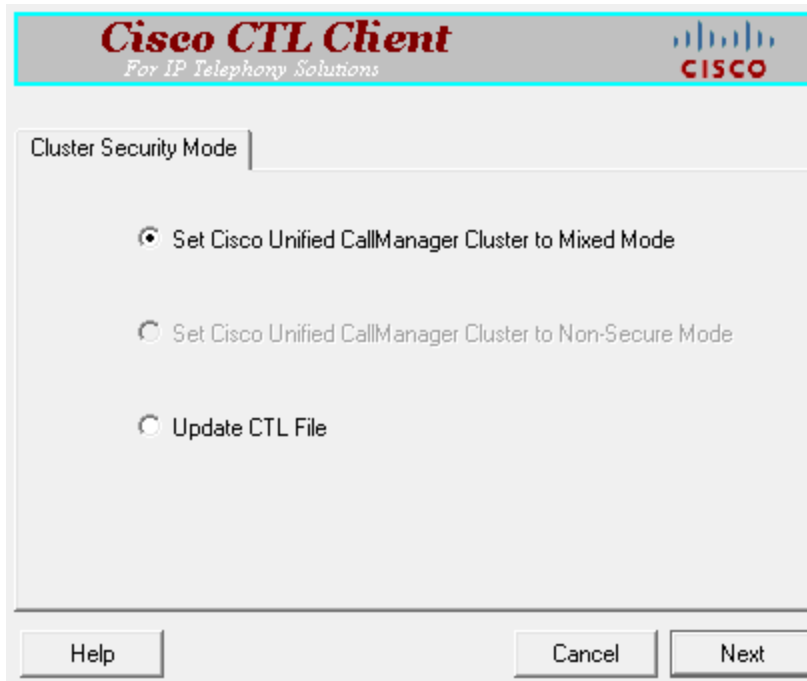
The Cisco Unified Communications Manager cluster must be in Mixed Mode to allow the registration of both secure devices and non-secure devices. This allows for best effort encryption between the Expressway and the Cisco Unified Communications Manager. Read [Secure RTP between CUCM and VCS or Expressway Configuration Example](#) for background on best effort encryption between Expressway and Unified CM.

As of version 10.0, you can use the CLI to change the cluster security mode. On earlier versions, you must use the Cisco CTL Client plugin to change the cluster security mode. The security mode change updates the CTL file, so you must restart the Cisco CallManager and Cisco Tftp services after the change.

The process is summarized below, but you should refer to the *Cisco Unified Communications Manager Security Guide* for your version, which you can find on the [Cisco Unified Communications Manager \(CallManager\) Maintain and Operate Guides](#) page.

1. Obtain access to the Unified CM publisher node, including hardware security tokens (if using the CTL Client plugin).
2. (Pre 10.0) Download and install the Cisco CTL Client plugin from Unified CM.

3. Run the CTL Client plugin to enable Mixed Mode. On 10.0 or later, you can use `utils ctl set-cluster mixed-mode` at the CLI.



4. Update the CTL file (via the plugin or `utils ctl update CTLFile`).
5. Restart the Cisco CallManager and Cisco Tftp services (via Cisco Unified Serviceability).

Configure 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 a 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.

5. Click **Save**.

Update the Unified CM Trunk to Expressway to Use TLS

On Unified CM:

1. Go to **Device > Trunk**.
2. Using Find, select the **Device Name** previously set up for the trunk to the Expressway.
3. 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.

4. Click **Save**.
5. Click **Reset**.

Update Device Profiles to Encrypt Calls to Unified CM-registered Endpoints

Endpoints registered to Unified CM need to be configured with a "SIP Secure profile" to provide encrypted media and call negotiation. If such profiles are not available by default, create them at **System > Security > Phone Security**. On the secure profiles, you must set **Device Security Mode** to *Encrypted*.

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

Update 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**.

Verify 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.

Configure Lync Server Environment

- [Task 1: Trust the Gateway Expressway, page 27](#)
- [Task 2: Configure Lync Server Media Encryption Capabilities, page 29](#)

Task 1: Trust the Gateway Expressway

This procedure creates a trusted application pool for each Expressway Gateway (or cluster) in the Lync environment, because Lync Server treats Expressway as an application. Then you add any subordinate peers to the application pool, create a trusted application to run in that pool, and then enable the topology.

The context for the following procedure depends on your Lync environment, as follows:

- If a Lync Director is in use, then configure the Lync Director (pool) to trust the Gateway Expressway and to route traffic to it.

Other Lync FE Servers 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 a hardware load balancer in front of a set of FE server pools, configure each server pool.
- If there is just a single Lync FE Server, configure that server.

Note: When you run the following shell commands, you could see warnings that the machine names were not found in the Active Directory domain. Ignore these warnings, because you do not need to add the Gateway Expressway to the AD domain.

1. Open the Lync Server Management Shell.
2. Use the command `New-CsTrustedApplicationPool` to create a trusted application pool for the Gateway Expressway.

(Repeat the command for each Gateway Expressway, or for the master peer of each Gateway Expressway cluster).

Example Command

```
C:\Users\Administrator.example>New-CsTrustedApplicationPool -Identity lyncexp.video.example.com -
ComputerFqdn exp01.video.example.com -Registrar fepool.example.com -site 1 -RequiresReplication
$false -ThrottleAsServer $true -TreatAsAuthenticated $true
```

Table 7 Parameter Reference

<code>-Identity</code>	The Gateway Expressway cluster FQDN, which must match the Common Name or a Subject Alternate Name on the Expressway server certificate
<code>-ComputerFqdn</code>	The Gateway Expressway peer FQDN (or the master's FQDN if running a cluster), which must match the Common Name on the Expressway server certificate.
<code>-Registrar</code>	The FQDN of the registrar for the Lync pool.
<code>-Site</code>	Specifies the siteID on which this application pool is homed. You can use <code>Get-CsSite</code> for a list of sites (SiteID) and related pools.
<code>-RequiresReplication \$false</code>	Specifies that the trusted application must not be replicated between Pools.
<code>-ThrottleAsServer \$true</code>	Reduces the message throttling because the trusted device is a server, not a client.
<code>-TreatAsAuthenticated \$true</code>	Specifies that this application is authenticated by default.

3. If the Gateway Expressway is a cluster, use the command `New-CsTrustedApplicationComputer` to add each peer to the trusted application pool.

(Repeat the command for each subordinate peer in each Gateway Expressway cluster)

Example Command

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

Table 8 Parameter Reference

<code>-Identity</code>	The FQDN of the Expressway peer you're adding, eg. exp02.video.example.com, which must match the Common Name on the peer's server certificate.
<code>-Pool</code>	The FQDN of the application pool (the value of <code>-identity</code> when you created the application pool).

4. Use the command `New-CsTrustedApplication` to assign a new application to the trusted application pool.

Example Command

```
C:\Users\Administrator.example>New-CsTrustedApplication -ApplicationId ExpresswayApplication1 -
TrustedApplicationPoolFqdn lyncexp.video.example.com -Port 65072
```

Table 9 Parameter Reference

<code>-ApplicationID</code>	Names the Gateway Expressway application (this is for Lync only, it is not a DNS name).
<code>-TrustedApplicationPoolFQDN</code>	Specifies the FQDN of the Gateway Expressway.
<code>-Port</code>	Specifies TLS/TCP port to use for neighboring, which must match the Port on B2BUA for Lync call communications on the Gateway B2BUA (default 65072).

5. Run the command `Enable-CsTopology` to enable the configuration.
6. To read and check the application pool and application configurations, use `Get-CsTrustedApplicationPool` and `Get-CsTrustedApplication`.

Task 2: Configure Lync Server Media Encryption Capabilities

The Lync Server defaults to mandatory media encryption, which you may need to change to suit your video network. To read the current media encryption policy on Lync Server use `get-CsMediaConfiguration`. The default `EncryptionLevel` is `RequireEncryption`.

Also, the headers used in Lync SRTP are different from those used by Cisco Collaboration devices. The Expressway B2BUA can modify these headers if the Gateway Expressway has the **Microsoft Interoperability** option key.

When Should I Consider Changing the Default Encryption on Lync Server?

You can modify the media encryption setting on Lync Server, and the value you choose will depend on the following factors:

- **Is the connection between Lync and the Gateway Expressway made over TLS?**

If the connection is TLS, then mandatory encryption is possible.

If the connection is not TLS, then the crypto keys will not be sent across the unsecure connection. Mandatory encryption will be impossible and calls will fail. In this case, you must change the default media encryption on Lync Server.

- **Does the Gateway Expressway have the Microsoft Interoperability option key?**

This key is required for interoperating with Lync Server 2013 and also for RDP transcoding. If it is installed on the Gateway Expressway, then mandatory encryption is possible.

The Gateway Expressway might not have this key when interworking with Lync Server 2010. In this case, mandatory encryption will be impossible because the B2BUA will not be able to modify the SRTP headers from Lync. You must change the default media encryption on Lync Server in this case.

- **Do all video endpoints in the network support encrypted media and offer encrypted media?**

If all Unified CM-registered endpoints can do media encryption, then mandatory encryption on Lync Server is possible.

If some endpoints cannot do media encryption, then mandatory encryption from Lync Server will not work.

How do I Change the Media Encryption Policy on Lync Server?

To configure the media encryption policy on Lync Server use `Set-CsMediaConfiguration` as follows:

`set-CsMediaConfiguration -EncryptionLevel <value>` where <value> is one of `RequireEncryption`, `SupportEncryption`, `DoNotSupportEncryption`.

For example:

```
C:\Users\Administrator.example> set-CsMediaConfiguration -EncryptionLevel SupportEncryption
```

See [TechNet article on Set-CsMediaConfiguration](#).

Note:

- `EncryptionLevel` is communicated to Lync clients and changes their operation. Users must sign out of the Lync client and sign back in.

You may have to wait (up to an hour, depending on complexity) for `EncryptionLevel` to propagate throughout the pool. Restarting Lync clients too soon may not change their media encryption policy.

- If the Gateway Expressway has the **Microsoft Interoperability** option key AND it makes a TLS connection to Lync Server, then you can use the default setting `-EncryptionLevel RequireEncryption`.

In this case, all video endpoints must support encryption or calls will fail. If some endpoints cannot do media encryption, you should use `-EncryptionLevel SupportEncryption`.

Configure the B2BUA and Search Rules on the Gateway Expressway

- [Task 3: Configure the B2BUA on the Gateway Expressway, page 30](#)
- [Task 4: Create a Search Rule to Route Calls for the Lync Domain to Lync Environment, page 31](#)
- [Task 5: \(If Required\) Create Search Rules to Route Calls to Other Domains Supported on Lync, page 32](#)

Task 3: Configure the B2BUA on the Gateway Expressway

The values you enter for **Lync signaling destination address** and **Lync signaling destination port** 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 has a Hardware Load Balancer in front of Front End Servers	Hardware Load Balancer
is a single Lync FE Server or FE Server Pool	The Lync Server or server pool

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.example.com
Lync signaling destination port	IP port used by device specified above – typically 5061
Lync signaling transport	<i>TLS</i>
Enable RDP transcoding for this B2BUA	Yes enables desktop/application sharing from Lync clients towards Cisco Collaboration endpoints. The Maximum RDP transcode sessions is 10 by default. Click Show advanced settings to change that if necessary.
Enable external transcoders for this B2BUA	<i>No</i>
Offer TURN Services	<i>No</i>
Advanced settings	Leave all advanced settings at their default values, unless otherwise indicated

3. Click **Save**.

The B2BUA is active now, and a non-configurable neighbor zone called **To Microsoft Lync Server via B2BUA** has been created for you.

Task 4: Create a Search Rule to Route Calls for the Lync Domain to Lync Environment

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.

For this scenario, any calls to the domain example.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 `identifier@example.com.*` are forwarded to Lync.

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

4. Click **Save**.

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.

This misconfiguration could introduce delays or cause calls to fail.

Task 5: (If Required) Create Search Rules to Route Calls to Other Domains Supported on Lync

If Lync supports only a single domain then no other search rules are 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	<code>.+@<relevant domain>.*</code>
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.

Test Calls from Internal Endpoint to Internal Lync Client

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

For example, call david.jones@example.com or alice.parkes@example.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.



Enable Calls from Lync

Table 10 Overview of Tasks Required to Enable Calls from Lync Clients to Collaboration Endpoints (All Internal)

Command or Action	Purpose
Configure the B2BUA Trusted Hosts, page 34	Provide the B2BUA application on the Gateway Expressway with a list of sources of Lync calls. The addresses you need depends on how the Lync Server environment is structured
Neighbor the Gateway to the Unified CM, page 35	Route Lync-originated calls from the Gateway Expressway to the Unified CM
Configure Static Routes from Lync Server to Gateway Expressway, page 39	Enable Lync Server to route unrecognized addresses in the internal SIP domain to the Gateway Expressway
Test Calls from Internal Lync Client to Internal Endpoint, page 40	To verify that calls from Lync clients are routed properly

Configure the B2BUA Trusted Hosts

When you're creating static routes from the Lync environment, you must configure the B2BUA to trust the hosts at the source of those routes. The hosts that the Expressway needs to trust depend on the structure of the Lync environment:

If...	Trust the...
the Lync environment has a single FE Server	Lync FE Server
the Lync environment has multiple front end servers (the deployment covered by this document)	Lync FE Servers which will be sending traffic towards the Gateway Expressways
the Lync environment is fronted by a Hardware Load Balancer in front of Lync Directors (see Appendix 2: Extended Lync Deployments, page 56)	Hardware Load Balancer and the Lync Directors
the Lync environment is fronted by a Lync Director (see Appendix 2: Extended Lync Deployments, page 56)	Lync Director
the Lync environment has no Lync Director but a Hardware Load Balancer in front of Front End Servers (see Appendix 2: Extended Lync Deployments, page 56)	Hardware Load Balancer and the Lync FE Servers

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 Gateway Expressway, or by pointing some of the Lync servers to a Lync proxy and then trusting the proxy instead.

Neighbor the Gateway to the Unified CM

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 for TCP or 5061 for TLS (must match the port set on the SIP trunk)
Transport	<i>TCP</i> or <i>TLS</i> . Choose <i>TLS</i> if you want secure transport and encrypted media
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: <ul style="list-style-type: none"> – Select <i>Cisco Unified Communications Manager</i> for versions prior to 8.6.1 – Select <i>Cisco Unified Communications Manager (8.6.1 or later)</i> for 8.6.1 or 8.6.2 – Select <i>Custom</i> for 9.x or later and: <ul style="list-style-type: none"> · Set Call signaling routed mode to <i>Always</i> · Leave all the other fields as their default values <p>Note that Unified CM 8.6.1 or later is required for BFCP (dual video / presentation sharing).</p>

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, page 22](#).

4. Click **Create zone**.

Edit zone

Type

Neighbor

Hop count

★

15

i

H.323

Mode

Off

▼

i

SIP

Mode

On

▼

i

Port

★

5060

i

Transport

TCP

▼

i

Accept proxied registrations

Deny

▼

i

Media encryption mode

Auto

▼

i

ICE support

Off

▼

i

Authentication

Authentication policy

Do not check credentials

▼

i

SIP authentication trust mode

Off

▼

i

Location

Peer 1 address

10.50.157.22

i

Peer 2 address

i

Peer 3 address

i

Peer 4 address

i

Peer 5 address

i

Peer 6 address

i

Advanced

Zone profile

Custom

▼

i

Monitor peer status

Yes

▼

i

Call signaling routed mode

Always

▼

i

Create 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@video.example.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@video.example.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})@video.example.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**.

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

Create 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	<i>Regex</i>
Pattern string	For example: <code>(.+)..*</code>
Pattern behavior	Replace
Replace string	For example: <code>\1</code>
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	Regex	
Pattern string	<input type="text" value="(.)..*"/>	
Pattern behavior	Replace	
Replace string	<input type="text" value="\1"/>	
State	Enabled	

Configure Static Routes from Lync Server to Gateway Expressway

This involves configuring domain static routes that route calls for Cisco Collaboration endpoints to Gateway Expressway.

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

Note: Adding and deleting static routes on a Lync Server does not automatically apply the route to all the other Lync Servers that may need the route. You need to add the route to the global static routing configuration. You then need to enable the changed topology to put the changes into effect.

1. Use `New-CsStaticRoute` to create a static route from Lync to the Gateway Expressway. Use the following switches:

`$routename=New-CsStaticRoute:` name and assign a variable to hold the new route.

`-TLSSRoute:` the route uses TLS (recommended)

`-TCPRoute:` the route uses TCP (not recommended)

`-Destination:` the Gateway Expressway Cluster FQDN. Use the IP Address in case of TCP routes.

`-MatchUri:` the SIP domain in which the Gateway Expressway is authoritative.

-Port: the TLS or TCP port to use for neighboring. It should be the same port as **Port on B2BUA for Lync call communications**. The default is 65072, but you can check the **Advanced B2BUA** settings on the Gateway Expressway, at **Applications > B2BUA > Microsoft Lync > Configuration**.

-UseDefaultCertificate: to use the default certificate assigned to the Front End (must be `$true`) when using TLS. Do not use this switch when creating a TCP route.

TLS route example:

```
C:\Users\administrator.example> $Route1=New-CsStaticRoute -TLSType -Destination  
"lyncexp.video.example.com" -MatchUri "video.example.com" -Port 65072 -UseDefaultCertificate $true
```

TCP route example:

```
C:\Users\administrator.example> $Route1=New-CsStaticRoute -TCPType -Destination "10.0.0.2" -MatchUri  
"video.example.com" -Port 65072
```

2. Use `Set-CsStaticRoutingConfiguration` to assign the route to the Lync Server environment routing configuration:

-Identity: specifies the scope of the routing configuration for the new route. It can be at `global` or supply the identity of a specific pool. If a pool does not have a more specific static route, it will choose the global route.

-Route @{Add=\$routename}: the name of the route you're assigning to the Identity (note the curly braces).

For example:

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

3. Verify the static route assignment using

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

4. Use `Enable-CsTopology` to put the changed routing configuration into effect for the specified scope.

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.

Test Calls from Internal Lync Client to Internal Endpoint

Test calls from Lync clients registered on Lync Server to endpoints registered on Expressway-C. For example, call `david.jones.office@video.example.com` from a Lync client registered on Lync Server.

Enable Calls from External Lync Clients

Table 11 Configure TURN in the Cisco Collaboration network

Command or Action	Purpose
Activate the TURN Server on the Expressway-E, page 41	Enable the Expressway-E to relay the media between external Lync clients and internal endpoints
Configure the Lync B2BUA to Offer TURN Services to External Lync Clients, page 42	To tell Lync clients the addresses of the TURN servers when they are establishing connectivity (ICE)

Activate the TURN Server on the Expressway-E

Prerequisites

- Expressway-E is configured as required in *Cisco Expressway Basic Configuration Deployment Guide* on [Cisco Expressway Series Configuration Guides page](#)
- Expressway-E has a TURN Relays option key

Create a Local Account for the Gateway Expressway and Enable TURN Services

1. Log in to the Expressway-E and go to **Configuration > Traversal > TURN**
2. Set **TURN services** to *On*
3. Click **Configure TURN client credentials on local database**
A window pops up showing the local authentication accounts
4. Click **New**
5. Enter a **Name** that you can recognize as the Gateway Expressway account, eg. `GatewayB2BUA`
6. Enter a **Password** to authenticate the Gateway Expressway
7. Click **Create Credential**
8. Close the pop up window
9. Leave the default values in place for all other configuration fields
10. Click **Save**

The **TURN server status** section now shows the listening address, the number of active clients, and the number of active relays.

Note: If you need to change any of the defaults on this page in future, restart the TURN server with your changes as follows:

- a. Make your changes and set **TURN services** to *Off*
- b. Click **Save** and then set **TURN services** to *On*
- c. Click **Save**

Configure the Lync B2BUA to Offer TURN Services to External Lync Clients

Prerequisites

- The Gateway Expressway has the **Microsoft Interoperability** option key
- There is a TURN server in the DMZ. This topic presumes that you will use the Expressway-E as a TURN server.

Configure TURN Services on the 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 default TURN listening port on the Expressway-E. 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 that the Gateway Expressway uses to authenticate against the TURN server. For example, <code>GatewayB2BUA</code>

4. Click **Add address**
5. Repeat the above steps if additional TURN servers are required
6. Go to **Applications > B2BUA > Microsoft Lync > Configuration**
7. Set **Offer Turn services** to *Yes*
8. Click **Save**

Enable Screen Sharing from Lync

Prerequisites

- Lync clients can make video calls to the Unified CM-registered endpoints
- The **Microsoft Interoperability** key is installed on the Gateway Expressway
- Read [Port Reference, page 47](#) and [Screen Sharing, page 8](#)

Enable RDP Transcoding on the Gateway Expressway

1. Go to **Applications > B2BUA > Microsoft Lync > Configuration**
2. Find **Enable RDP transcoding for this B2BUA** and select *Yes*

3. Adjust the following Advanced settings, if necessary for your environment:

Table 12 Advanced RDP Transcoding Settings

Setting name	Default and description
RDP TCP port range start - end	6000-6099 for incoming TCP presentation streams from Lync clients
RDP UDP port range start - end	6100-6199 for outgoing UDP presentation streams towards BFCP-capable endpoints
Maximum RDP transcode sessions	10 Simultaneous transcoding sessions

4. Save the configuration

Test Screen Sharing from Lync

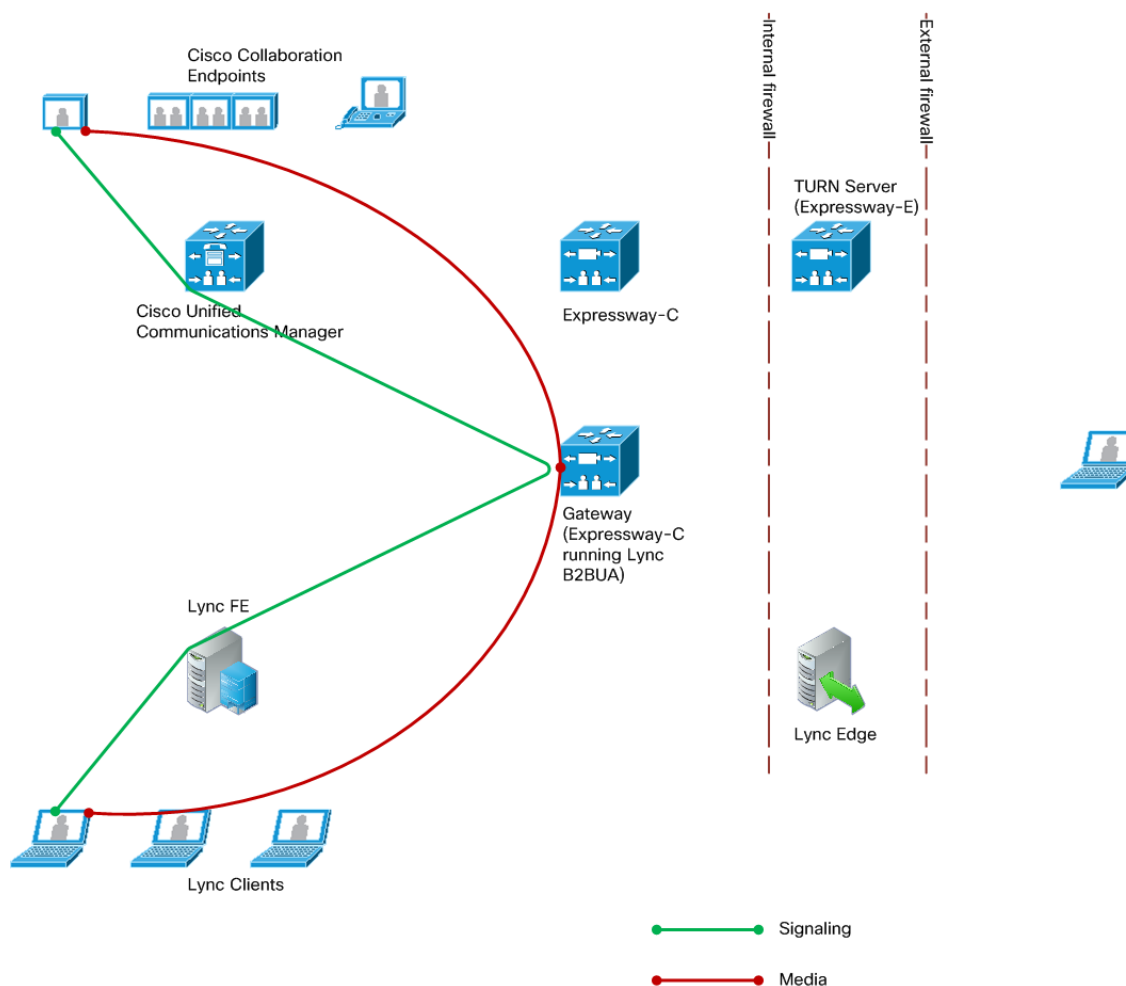
1. Open a Lync client and make a video call to a Unified CM-registered endpoint.
2. Start sharing the Lync user's screen with the endpoint.
3. Verify that the endpoint is showing the shared screen.
4. Repeat the test for application sharing.

Media Paths and License Usage

Lync Client Call to SIP Video Endpoint	44
Off-site Lync Client Calls Internal SIP Video Endpoint	45

Lync Client Call to SIP Video Endpoint

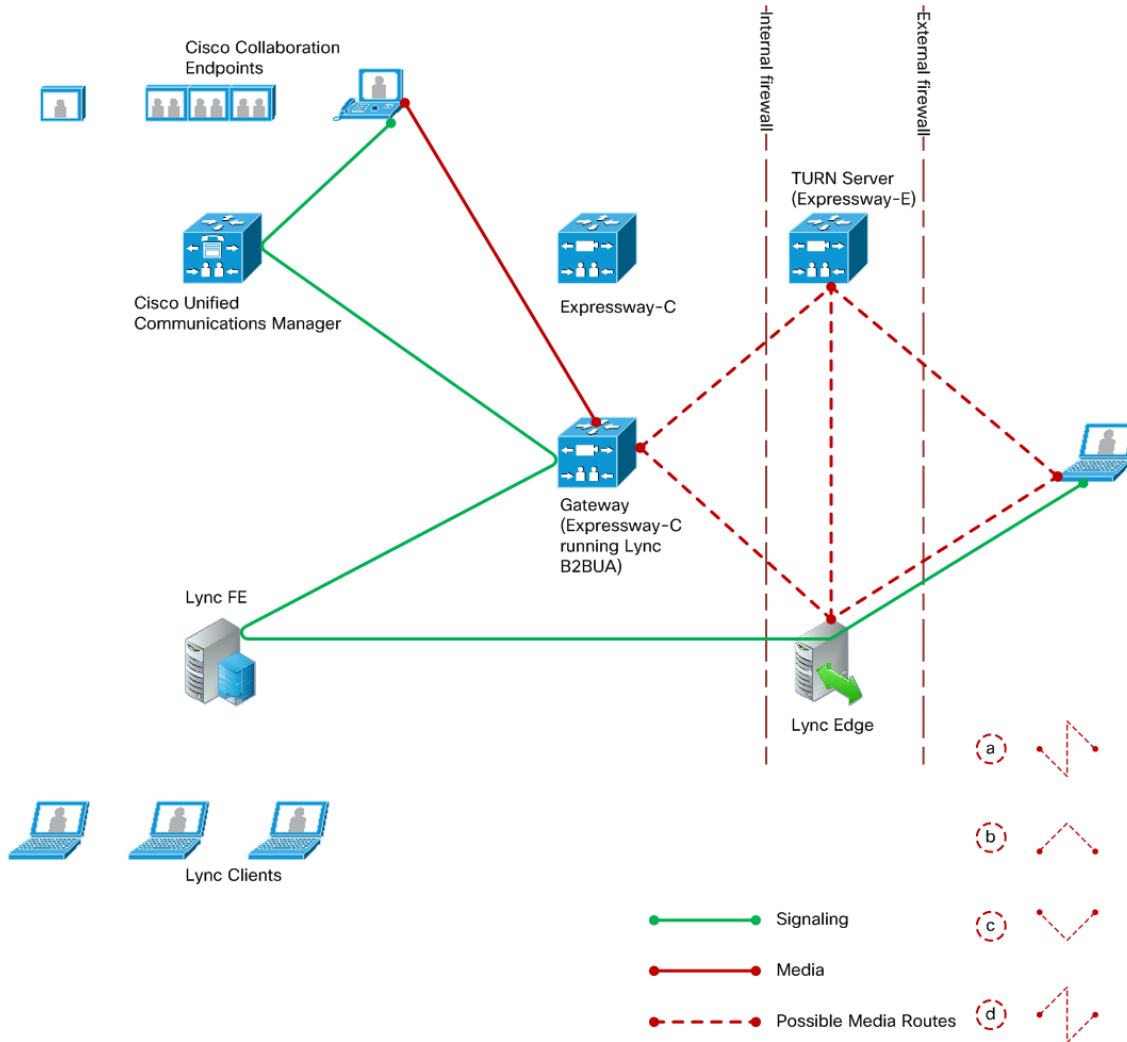
Figure 4 Call between internal Lync client and internal SIP endpoint



- Licenses consumed by this call:
 - 1 rich media session license on Gateway Expressway
- 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 SIP video endpoint and the B2BUA.
- Calls in both directions use the same signaling and media paths.

Off-site Lync Client Calls Internal SIP Video Endpoint

Figure 5 Call between off-site Lync client and internal SIP endpoint.



- Licenses consumed by this call:
 - 1 rich media session license on Gateway Expressway
 - A number of TURN licenses on the Expressway-E, which depends on what media streams are relayed
- Signaling flows through the Microsoft Edge Server, Lync Server, B2BUA, and Unified CM.

- Media between the Lync client and the B2BUA can be routed in a number of ways, depending on the ICE (Interactive Connectivity Establishment) negotiation between the Lync client and the B2BUA. The options (dotted red lines on the diagram) are:

- a. Lync Client - Expressway-E - Lync Edge - Gateway Expressway - SIP endpoint
- b. Lync Client - Expressway-E - Gateway Expressway - SIP endpoint
- c. Lync Client - Lync Edge - Gateway Expressway - SIP endpoint
- d. Lync Client - Lync Edge - Expressway-E - Gateway Expressway - SIP endpoint

Note: The exact media path for any particular call is impossible to determine until the call is made. This is because the clients perform the connectivity checks and candidate sorting each time the media path is established, and route selection is based on loosely regulated factors. See [RFC 5245](#) for details.

- Media is connected directly between the internal SIP endpoint and the B2BUA (because 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.

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**).

Table 13 Between B2BUA and Lync

Purpose	Protocol	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 application should run on a separate "Gateway" Expressway and so this range should not conflict with the standard traversal media port range) Note: The Expressway does not forward DSCP information that it receives in media streams.	UDP	56000 to 57000 Each call can use up to 18 ports if you Enable RDP Transcoding for this B2BUA . Increase this range if you see "Media port pool exhausted" warnings.	Lync client media ports
Desktop shares from Lync clients to B2BUA	TCP	56000 to 57000	Lync client RDP ports

Table 14 Between B2BUA and Internal Video Network

Purpose	Protocol	B2BUA port	Expressway IP port
Internal communications with Expressway application	TLS	65070	SIP TCP outbound port on Expressway
Transcoded desktop shares from B2BUA to internal recipients	UDP	56000 to 57000	Recipient of media is dependent on deployment and called alias; eg. endpoint, TelePresence Server, Expressway-C

Table 15 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.

Table 16 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
STUN	UDP	3478	3478
UDP Media	UDP	50000-59999	1024-65535
TCP Media	TCP	50000-59999	1024-65535

Table 17 External Lync Client / Edge Server and Expressway-E

Purpose	Protocol	Lync client / Edge server	Expressway-E
ICE messaging (STUN/TURN) (Expressway-E must listen on TCP 3478 for desktop sharing relay requests from Lync clients, and on UDP 3478 for A/V media relay requests)	UDP & TCP	3478	3478
UDP media	UDP	1024-65535	24000-29999

Table 18 Between B2BUA and External Transcoder

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

How Many Media Ports are Required on the Gateway Expressway?

The UDP port range of the B2BUA on the Gateway Expressway is set to 1000 ports by default, starting at 56000 and ending at 57000. That is the default destination range for media from Lync clients, and may be different in your Lync environment.

The B2BUA uses the UDP ports as follows:

Purpose	Call type	Number of ports used
Traversal of audio and video streams	Internal/external Lync client to SIP endpoint	8
RDP transcoding	Desktop share from Lync client	10
Maximum per call	Lync client sharing desktop	18
Connections from B2BUA to TURN server	Per TURN server connection	2

The number of ports used is one of the reasons why the default maximum number of RDP transcode sessions is set to 20, and why the hard limit for maximum Lync B2BUA calls is 100.

For example, if the B2BUA is handling 100 internal Lync AV calls, and 20 of those calls are doing RDP:

$(80 \times 8) + (20 \times 18) + (0 \times 2) = 1000$ ports are required, and no further sharing sessions can be accommodated by the default port range.

(In this example, there are no connections to TURN servers)

If you increase the maximum number of RDP transcode sessions, you should also increase the B2BUA media port range.

Appendix 1: 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:

- Check the Event Log (**Status > Logs > Event Log**) on Expressway
- Enable logging on Lync Server
- Enable debug on Lync Client
- 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 Gateway Expressways can successfully look up all Lync Server A-record FQDNs in DNS (this includes both Director and FE Servers). You can use **Maintenance > Tools > Network utilities > DNS lookup** on the Expressway.
- Ensure that all Lync servers can successfully look up all 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).

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).

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](#).

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.

Lync Cannot Open a TLS Connection to Expressway

Lync Debug says Lync Fails to Open a Connection to Expressway, even though the TLS neighbor zone to Lync Server is active and messaging is sent from Expressway to Lync Server.

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 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:

- Gateway Expressway has the **Microsoft Interoperability** option key included, or
- (Lync Server 2010 only) 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 Drops 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 (HLB)

If the Lync environment has FE Servers with a hardware load balancer in front, ensure that the Expressway is neighbored with the HLB. If it is neighbored directly with a FE Server, trust for Expressway will be with the FE Server. Expressway will send call requests to the FE Server, but the FE Server 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 FE Server not seeing the ACK.

(Calls from Lync client - registered to the FE Server- 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 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 FE Server rather than the load balancer. See [Enable Calls to Lync, page 14](#) and configure Lync trusted hosts containing the FE Servers' IP addresses.

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:

1. `_sips._tcp.<domain>`
2. `_sip._tcp.<domain>`
3. `_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

If Lync clients are trying to register with Expressway-E, it could be because the wrong SRV record points to it.

You must make sure that the six DNS records above do not resolve to overlapping addresses.

Lync clients only support TLS connection to the Microsoft Edge Server, so use the `_sip._tcp.<domain>` DNS SRV for the Expressway-E.

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 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).

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 [Enable Calls to Lync, page 14](#) for more information.

Lync Client

Lync Client Stuck in 'Connecting ...' State

This could be because the Lync client is not receiving media. The client cannot change into the "Connected" state until it receives RTP (media) from the other party.

Presentation Handover Fails in TelePresence Server Conference

Symptom: A participant cannot share their screen when another participant has been sharing.

Note: This issue was seen in a test of an unsupported Expressway and Lync scenario, but the solution applies more generally. You could see this symptom whenever endpoints are sharing in a TelePresence Server conference, or if endpoints that are sharing are registered to Cisco Unified Communications Manager. If you are seeing presentation issues, check the solution shown here (even if your conditions are different).

Conditions:

- Gateway Expressway deployed with Lync 2013 Front End Server and Lync 2013 for Windows clients.
- Gateway Expressway configured for Lync screen sharing.
- The Gateway Expressway is trunked to Cisco Unified Communications Manager.
- TC endpoints are registered to Unified CM.
- TC endpoints and Lync clients are in a conference on TelePresence Server.
- The conference is registered to the Gateway Expressway (The TelePresence Server is in locally managed mode - no TelePresence Conductor in this scenario).

Possible Root Causes:

- The TelePresence Server is not configured to allow participants to steal the floor.
- The neighbor zone from Expressway to Unified CM does not support BFCP.
- The SIP profile used by the trunk or endpoints does not support BFCP.

Solution:

1. Sign in to the TelePresence Server and check that **Automatic content handover** is enabled (the check box is on **Configuration > System settings** page).
2. Check the box and save the configuration.
3. Log in to the Expressway, go to **Configuration > Zones > Zones**, and open the neighbor zone toward Unified CM.
4. Check the **Zone profile** (in the **Advanced** section of the zone configuration).
 - BFCP is enabled on the neighbor zone if **Zone profile** is *Cisco Unified Communications Manager (8.6.1 or later)*.
 - BFCP is not enabled on the neighbor zone if **Zone profile** is *Cisco Unified Communications Manager*.
5. Change the zone profile if necessary, then save the configuration.
6. Log in to Unified CM Administration, go to **Device > Trunk**, and open the SIP trunk to Expressway.
7. Find the **SIP Profile** field and click **View Details** to see the configuration of the selected profile.
8. Find the **SDP Information** field, which has a check box to **Allow Presentation Sharing using BFCP**.
9. Go to **Device > Phone**, open the affected phone configuration, and check the details of the SIP profile it's using.
10. If a SIP profile does not allow BFCP, go to **Device > Device Settings > SIP Profile** to modify the SIP profile.

Appendix 2: Extended Lync Deployments

Clustered Gateway	56
Lync Environments	56
Multiple Lync Domains and Multiple Gateway Expressways	60

Clustered Gateway

When this document refers to a 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 FE will typically arrive at a single Expressway in the cluster because Lync FE will use the static domain route; the route resolves to a single FQDN for TLS connectivity, or to a single IP address for TCP connectivity.

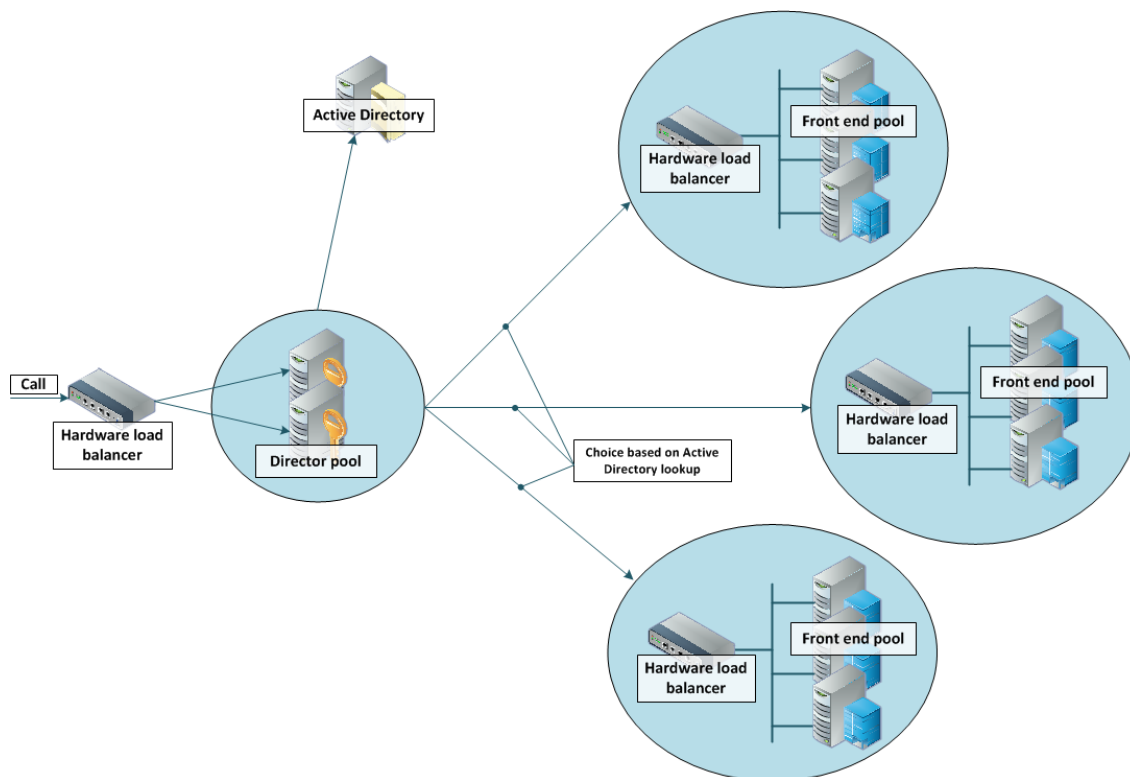
If you use a DNS A record to map the peers' IP addresses to the FQDN of the cluster, the DNS server typically returns the IP addresses in a different order each time the Lync Server queries DNS (round-robin). Lync FE chooses one of the returned addresses, based on its own logic (outside of this document's scope).

Lync Environments

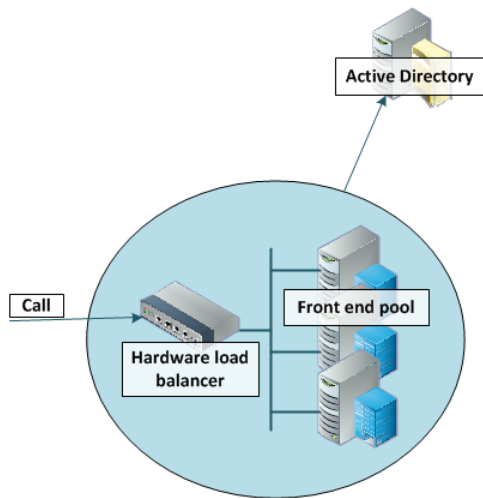
Lync environments have a number of building blocks, and so they may be constructed in many ways. A full scale Lync deployment is likely to use Lync Director, Hardware Load Balancers (HLBs), Front End Servers in enterprise pools, and a redundant AD server.

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>.

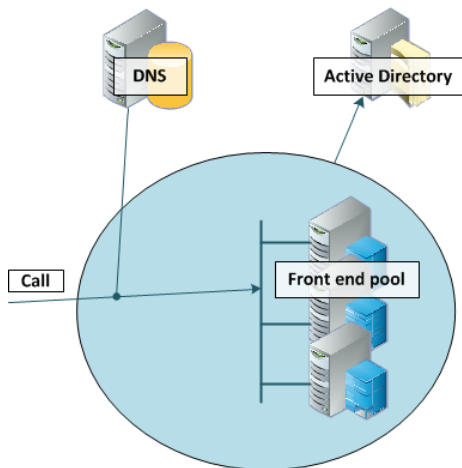
An example architecture is shown below:



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 Servers.

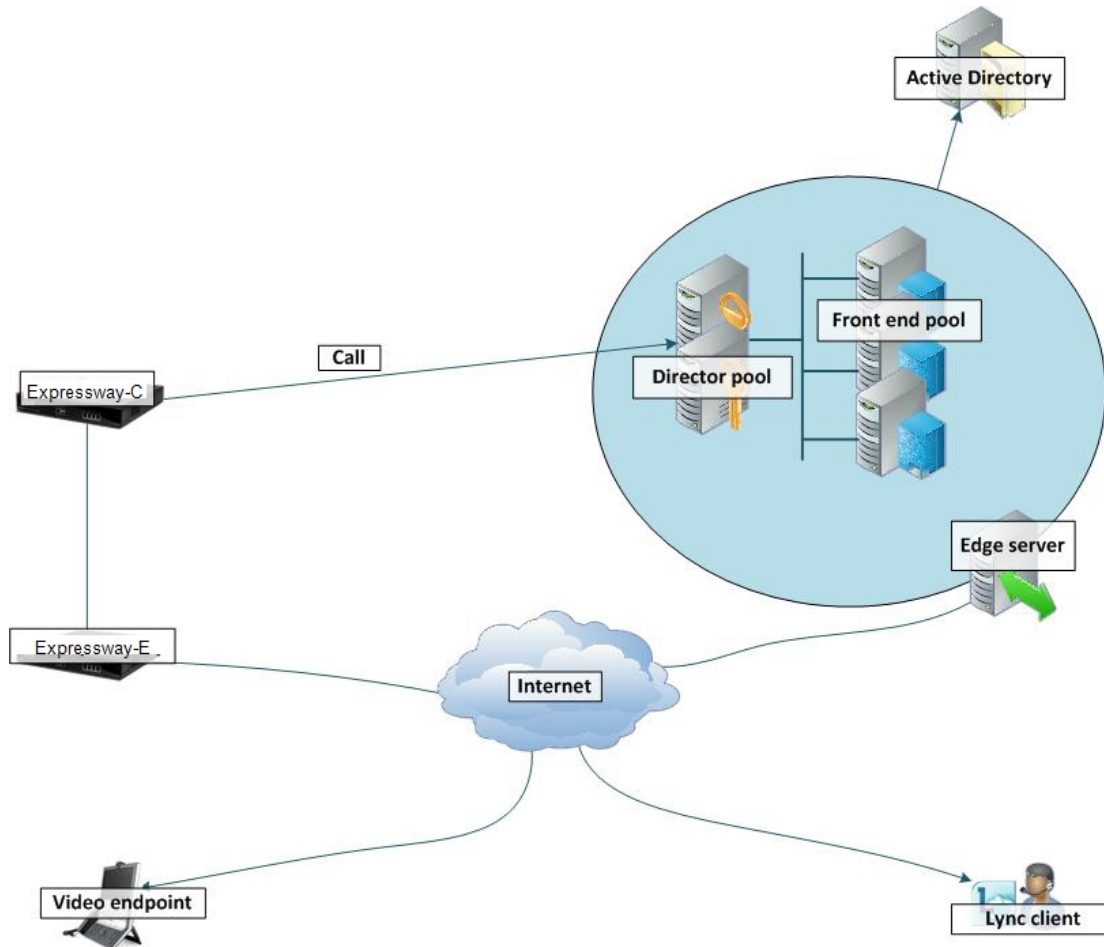


A Lync environment may use DNS instead of the Hardware Load Balancer, for example:



Note that Lync requires that the AD server and the FE Server 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 Front End Server to the Expressway, or from the FE Server via a Director 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 FE Servers:
 - Lync Directors should trust the Gateway Expressway(s).
 - Lync Directors should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.
 - Depending on Lync configuration, FE Servers 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 FE Servers:
 - Lync Directors should trust the Gateway Expressway(s).
 - Lync Directors should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.
 - Depending on Lync configuration, FE Servers 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 Server pool(s) then configure the pool(s) (not each FE Server):
 - The FE Server pools should trust the Gateway Expressway(s).
 - All FE Server pools should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.

Configuring the pool ensures that the same configuration is applied to every FE Server in the pool.

- If Lync is a single Front End Server, then configure that server:
 - The FE Server should trust the Gateway Expressway(s).
 - It should route the video network domain (video.example.com) to the Gateway Expressway cluster FQDN.

We recommend that you use a Expressway cluster FQDN (e.g. lyncexp.example.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.

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 Gateway B2BUA needs to specify the Hardware Load Balancer as the Lync signaling destination address.
 - The Gateway B2BUA needs to include the addresses of both Lync Directors as trusted hosts (and any FE Servers 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 Gateway B2BUA needs to specify the Lync Director (pool) as the Lync signaling destination address.
 - The Gateway B2BUA needs to include the address of each individual Lync Director as a trusted host (and any FE Servers 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 Servers then the B2BUA should be configured to route calls for Lync to the Hardware Load Balancer, and receive calls from any of the FE Servers:
 - The Gateway B2BUA needs to specify the Hardware Load Balancer as the Lync signaling destination address.
 - The Gateway B2BUA needs to include the addresses all of the Lync FE Servers as trusted hosts.
 - Search rules that route calls to Lync will target the B2BUA neighbor zone.
- If Lync is a single FE Server, then the B2BUA should be configured to route calls for Lync directly to that FE Server, and to receive calls from that FE Server:
 - The Gateway B2BUA needs to specify the FE Server as the Lync signaling destination address.
 - The Gateway B2BUA needs to include the address of the FE Server as a trusted host.
 - Search rules that route calls to Lync will target the B2BUA neighbor zone.

Multiple Lync Domains and Multiple Gateway Expressways

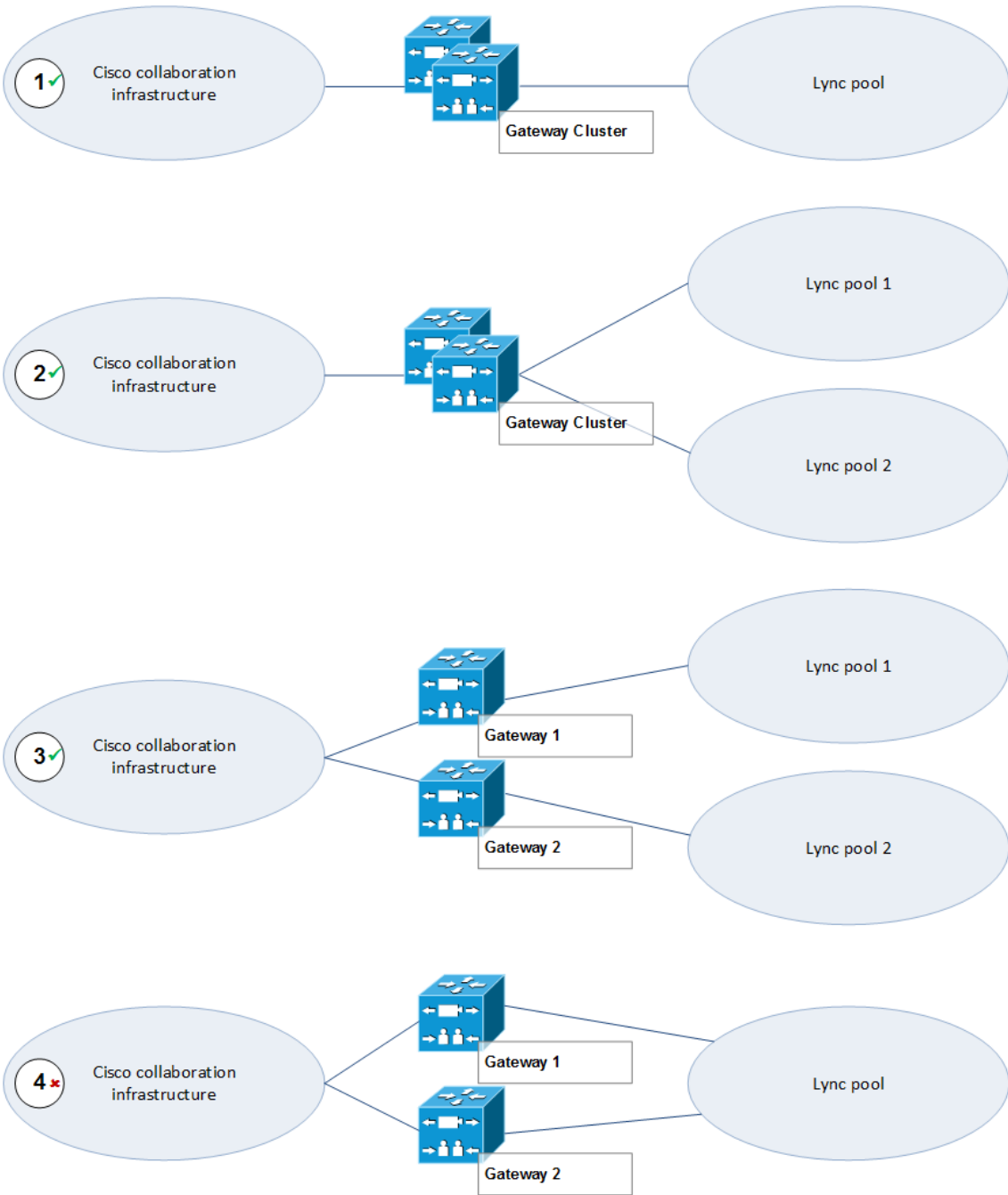
You can integrate Cisco collaboration infrastructure with more than one Lync domain if required. Wherever you put a single Expressway as a gateway, you could use a cluster instead.

The diagram below 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. One gateway or gateway cluster serving multiple Lync domains. Requires multiple search rules to route the calls to and from Lync correctly.
3. It is possible to configure multiple Lync domains with an independent gateway serving each. This option is not exhaustively tested, nor is it described in this document.
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 6 Gateway Expressway Deployment Options, Showing Potential Misconfiguration



Appendix 3: Assistance with Prerequisite Tasks

Verify Calls Between Lync Clients

This is a prerequisite to integrating Expressway with your Microsoft Lync environment. The simplified procedures are listed here but you should refer to the Microsoft documentation for your products.

Enable 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.

To enable AD users for Lync using the Lync Server Control Panel:

1. Open the Lync Server Control Panel and find the Users section.
2. Find the control to enable users, which allows you to search for and add existing AD users.
3. Assign the selected users to the appropriate Lync Server pool.
4. Select which AD user properties are used to generate the users' SIP URIs.

To enable AD users for Lync, using PowerShell:

Use the command `enable-csuser`. For example:

```
enable-csuser -identity "example\alice.parkes" -registrarpool "fepool.example.com" -sipaddress  
sip:alice.parkes@example.com
```

Register Lync Clients to Lync Server

1. Install and run the Lync client.
2. Enter the SIP URI as the sign-in address.
3. Point the client to the FQDN of the correct Lync FE pool.
4. Save the configuration and verify log in.

Test Calls

1. Select a contact in the Lync client
2. Start a video call
3. Answer the call with the contact's Lync client



Cisco Legal Information

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.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2015 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)