



Cisco TelePresence Microsoft Lync and Cisco VCS

Deployment Guide

Cisco VCS X8.5
Microsoft Lync 2010, Lync 2013

December 2014

Contents

| | |
|--|-----------|
| Introduction | 6 |
| Objectives and intended audience | 6 |
| Deployment scenario | 6 |
| Clustered "Lync gateway" VCS | 8 |
| Why add a "Lync gateway" VCS? | 8 |
| Features and capabilities | 11 |
| Client support | 11 |
| Interoperability with different versions of Lync Server | 11 |
| Microsoft Lync B2BUA interoperating capabilities | 12 |
| Summary of configuration objectives | 12 |
| Lync environments | 13 |
| Prerequisites prior to configuring VCS and Lync to interoperate | 17 |
| Benefits of using the B2BUA over legacy OCS Relay | 17 |
| Video network: check that calls between endpoints registered to VCS Controls operate as expected | 18 |
| VCS Control configuration summary | 18 |
| Ensure SIP domain of video network endpoints is configured in the VCS Control | 18 |
| Optional. Configuring interworking for H.323 endpoints registered to other systems | 18 |
| Lync configuration | 18 |
| Registering video endpoints to the video network | 19 |
| Video endpoint configuration | 19 |
| Confirming registrations | 19 |
| Testing the configuration | 19 |
| Check that calls between Lync clients registered on Lync Server operate as expected | 20 |
| VCS Control configuration | 20 |
| Enabling users for Lync | 20 |
| Registering Lync clients to the Lync Server | 22 |
| Lync client configuration | 22 |
| Testing the configuration | 23 |
| Enabling endpoints registered on the video network to call clients registered on Lync | 24 |
| Video network: VCS Control configuration | 24 |
| Video network: Set up a neighbor zone from VCS Control to the "Lync gateway" VCS | 24 |
| Video network: Set up a search rule on VCS Control to route calls for the Lync domain to the "Lync gateway" VCS | 26 |
| Video network: Set up search rules to route calls to the "Lync gateway" VCS for domains supported on Lync (but not in the video network) | 26 |
| "Lync gateway" VCS configuration (part 1) | 27 |
| "Lync gateway" VCS: Load CA certificate and server certificate (if using TLS to Lync) | 27 |
| "Lync gateway" VCS: Configure DNS and local hostname | 28 |
| "Lync gateway" VCS: Ensure that cluster name is configured | 29 |
| "Lync gateway" VCS: Configure an NTP server | 29 |
| "Lync gateway" VCS: Ensure that TLS is enabled in SIP configuration | 29 |
| Lync Server configuration | 29 |
| Trust a "Lync gateway" VCS | 30 |
| Configure Lync Server media encryption capabilities | 32 |
| "Lync gateway" VCS configuration (part 2) | 32 |
| Configure the B2BUA on the "Lync gateway" VCS | 33 |

| | |
|--|-----------|
| Set up a search rule to route calls to the Lync domain to Lync | 34 |
| Set up search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync | 35 |
| Testing the configuration | 36 |
| Enabling Lync clients registered on Lync Server to call endpoints registered on the video network | 37 |
| "Lync gateway" VCS configuration | 37 |
| Configuring the B2BUA trusted hosts on the "Lync gateway" VCS | 37 |
| Configuring the "Lync gateway" VCS with a neighbor zone that contains the video network | 38 |
| Setting up search rules to route calls with video network domains to the video network | 40 |
| Configuring Lync Server domain static routes | 41 |
| Configuring static routes to route calls to the "Lync gateway" VCS | 41 |
| Testing the configuration | 42 |
| Enabling Lync clients to see the presence of endpoints registered on VCS Control | 43 |
| VCS Control configuration | 43 |
| "Lync gateway" VCS configuration | 44 |
| Testing the configuration | 44 |
| Enabling Microsoft Edge Server and VCS TURN capabilities | 45 |
| Using FindMe for enhanced deployments | 46 |
| Deployment information | 46 |
| Prerequisites | 48 |
| Configuring the "Lync gateway" VCS for FindMe | 48 |
| Configure all the required SIP domains | 48 |
| Configure the B2BUA to register FindMe users to Lync | 48 |
| Enable FindMe and create FindMe user accounts for each user that is to share Lync client and VCS endpoints | 49 |
| Configuring Lync Active Directory for FindMe users | 50 |
| Testing the configuration | 53 |
| Enabling Lync clients to see the presence of endpoints registered on VCS Control | 53 |
| VCS Control configuration | 53 |
| "Lync gateway" VCS configuration | 55 |
| Lync client configuration | 56 |
| Log in to the Lync client | 56 |
| Appendix 1: Federation | 57 |
| Solution overview | 57 |
| Configuring the directory VCS | 58 |
| Modifying the Lync static route configuration | 59 |
| Appendix 2: Troubleshooting | 60 |
| Troubleshooting checklist | 60 |
| Problems connecting VCS Control local calls | 60 |
| Check for errors in the Event Log | 61 |
| Tracing calls | 61 |
| Presence not observed as expected | 61 |
| Video endpoint reports that it does not support the Lync client SDP | 62 |
| TLS neighbor zone to Lync Server is active and messaging is sent from VCS to Lync Server, but Lync debug says Lync fails to open a connection to VCS | 62 |
| Lync client initiated call fails to connect | 62 |

| | |
|---|-----------|
| Lync responds to INVITE with '488 Not acceptable here' | 62 |
| Call connects but clears after about 30 seconds | 63 |
| Media problems in calls involving external Lync clients connecting via an Edge server | 63 |
| One way media: Lync client to VCS-registered endpoint | 64 |
| Lync rejects VCS zone OPTIONS checks with '401 Unauthorized' and INFO messages with '400 Missing Correct Via Header' | 65 |
| Lync client stays in 'Connecting ...' state | 65 |
| Call to PSTN or other devices requiring caller to be authorized fails with 404 not found | 65 |
| Lync clients try to register with VCS Expressway | 65 |
| B2BUA problems | 66 |
| B2BUA users fail to register | 66 |
| B2BUA Lync Server status reports "Unknown" or "Unknown failure" | 66 |
| Lync problems | 66 |
| Problems with certificates | 66 |
| Appendix 3: Debugging on Lync | 67 |
| Use of Lync Server Logging Tool | 67 |
| Enabling debug on Lync client | 68 |
| Appendix 4: Interoperating capabilities and limitations | 69 |
| Known interoperating capabilities | 69 |
| SIP and H.323 endpoints making basic calls | 69 |
| Upspeeding from a voice call to a video call | 69 |
| Maximum call resolution | 69 |
| Multiway generation of ad hoc conferences | 69 |
| Known interoperating limitations | 69 |
| Video codecs | 69 |
| MXP endpoints | 70 |
| Joining a Lync conference (AV MCU) | 70 |
| Upspeeding from a voice call to a video call | 70 |
| Microsoft Mediation Server | 70 |
| Cluster calls to endpoints not registered using FindMe | 71 |
| Lync client reports no audio device | 71 |
| Call forward from Lync to a VCS FindMe or endpoint results in a 'loop detected' call | 71 |
| FindMe Caller ID set to FindMe ID causes calls from Lync client to fail | 71 |
| Appendix 5: Port reference | 73 |
| Appendix 6: Media paths and license usage for calls through B2BUA | 75 |
| Lync client call to SIP video endpoint | 75 |
| Lync client call to H.323 video endpoint | 75 |
| Lync client call to a SIP video endpoint via Cisco AM GW | 76 |
| Lync client call to H.323 video endpoint via Cisco AM GW | 77 |
| An external Lync client calls an external video endpoint | 78 |
| An external Lync client calls an internal SIP video endpoint | 79 |
| Appendix 7: Additional information | 80 |
| B2BUA registration on "Lync gateway" VCSs | 80 |
| What does "Register FindMe users as clients on Lync" do? | 80 |
| Configuring domains | 81 |
| B2BUA and Cisco AM GW integration | 81 |
| TEL URI handling for VCS to Lync calls | 81 |

| | |
|--|-----------|
| Document revision history | 82 |
|--|-----------|

Introduction

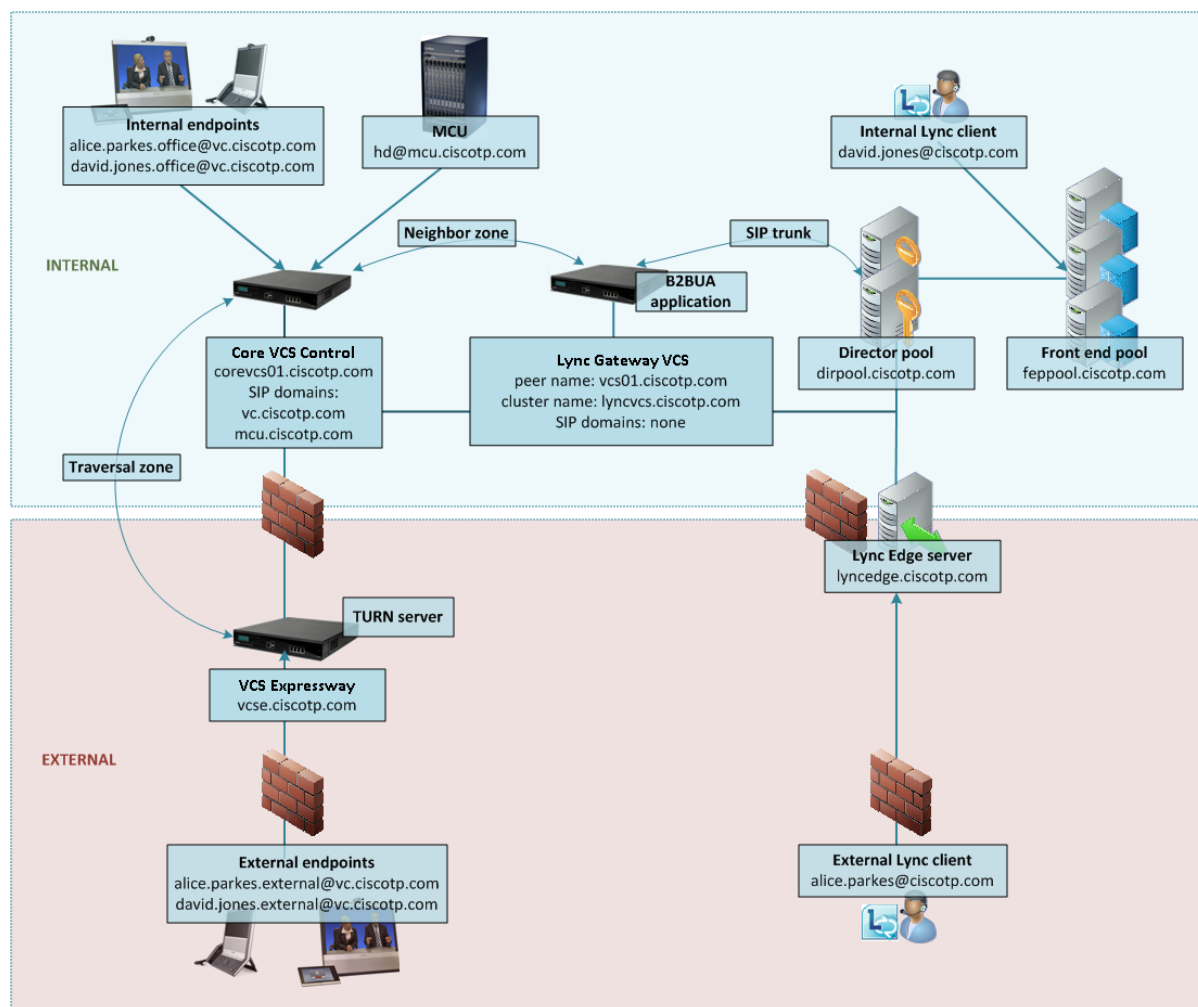
Objectives and intended audience

This deployment guide describes how to configure a Cisco TelePresence Video Communication Server (VCS) using the Back-2-Back-User-Agent (B2BUA) and Microsoft Lync 2010 / 2013 (Lync) to interwork. It also highlights the capabilities and limitations of interoperation of VCS and Lync.

Deployment scenario

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

This deployment guide uses the example environment depicted below:



This guide describes two deployment solutions:

1. **Basic configuration using static routes:** this uses static routes to route calls from Lync to VCS and provides basic interoperability for voice, video and Presence. This configuration is described below.
2. **FindMe-based configuration:** uses FindMe to provide an enhanced experience and richer Presence. This configuration builds on the basic configuration and is described in [Using FindMe for enhanced deployments \[p.46\]](#).

The basic configuration environment consists of the following elements:

Lync deployment with:

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

Cisco video deployment with:

- Lync gateway VCS Control (referred to as the "Lync gateway" VCS) with peer FQDN vcs01.ciscotp.com and cluster FQDN lyncvcs.ciscotp.com. The cluster FQDN must resolve to a list of DNS A-records including the IP addresses of all cluster peers (for round-robin operation).
- Core VCS Control (referred to as the VCS Control) with FQDN corevcs01.ciscotp.com
- VCS Expressway with FQDN vcse.ciscotp.com
- Internal and external video endpoints for video users david.jones and alice.parkes
- MCU registered to a video network VCS Control

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

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

- A VCS Control (or cluster of VCS Control peers) – the "Lync gateway" VCS – to act as the link between the existing video network and Lync.
- The Lync's SIP domain is ciscotp.com. The SIP domain for Lync need not be the same as the AD domain of Lync clients (the Lync login domain used in the login user name may be different from the SIP domain used in the sign-in address).
- The Cisco video network's domain is vc.ciscotp.com (used for video device registrations).
- Endpoints registered to the video network may be SIP or H.323 endpoints; they must register with an ID in the format alias@domain, where domain is a domain hosted on the video network (for example firstname.lastname.device_type@vc.ciscotp.com). We recommend that any H.323 to SIP and IPv4 to IPv6 protocol interworking is performed on the VCS Control.
- Lync clients registered to Lync are identified by URIs, for example:
 - David with a URI david.jones@ciscotp.com
 - Alice with a URI alice.parkes@ciscotp.com
- Endpoints registered to the video network are identified by URIs, frequently including the location or type of the endpoint, for example:
 - Alice's internal video endpoint with an alias of alice.parkes.office@vc.ciscotp.com
 - Alice's home office video endpoint with an alias of alice.parkes.external@vc.ciscotp.com

- David's internal video endpoint with an alias of david.jones.office@vc.ciscotp.com
- David's home office video endpoint with an alias of david.jones.external@vc.ciscotp.com
- Lync Front End Server is configured with a static domain route which routes URIs with the VCS's video network domain (vc.ciscotp.com) to the VCS. Care must be taken when using domain static routes; any traffic for that domain that Lync cannot handle locally will be routed to VCS.
- MCUs that will receive calls from Lync can register conferences to the video network with a dedicated MCU domain (mcu.ciscotp.com) and make these available to Lync users via a static SIP domain route from the Lync environment (suitable for ad-hoc conference aliases). A separate domain for MCU registrations is recommended as it more easily allows you to prevent SIP traffic coming from Lync via a static route from propagating further into the video network than needed (by using search rules).
- The Presence Server residing on the VCS Control publishes presence information into the Lync environment via the B2BUA application on the Lync gateway VCS. This Presence Server must be authoritative for the video domain (vc.ciscotp.com) and any dedicated MCU domains (mcu.ciscotp.com) in use.

Clustered “Lync gateway” VCS

When this document refers to a “Lync gateway” VCS, a cluster of VCSs can also be used. The operation is functionally the same, but there is more capacity available.

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

If you use a DNS A record to map the peers' IP addresses to the FQDN of the cluster, the DNS server typically returns the IP addresses in a different order each time the Lync Server queries DNS (round-robin). The Lync Server selects one IP address to use, based on its own logic (outside of this document's scope). If the TTL of the record has not expired when the Lync Server makes a new DNS query, the Lync Server will use the same IP address it used the previous time. If the Lync Server cannot connect to the IP address it selected, it will try another of the IP addresses returned by the DNS server.

Why add a “Lync gateway” VCS?

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

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

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

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

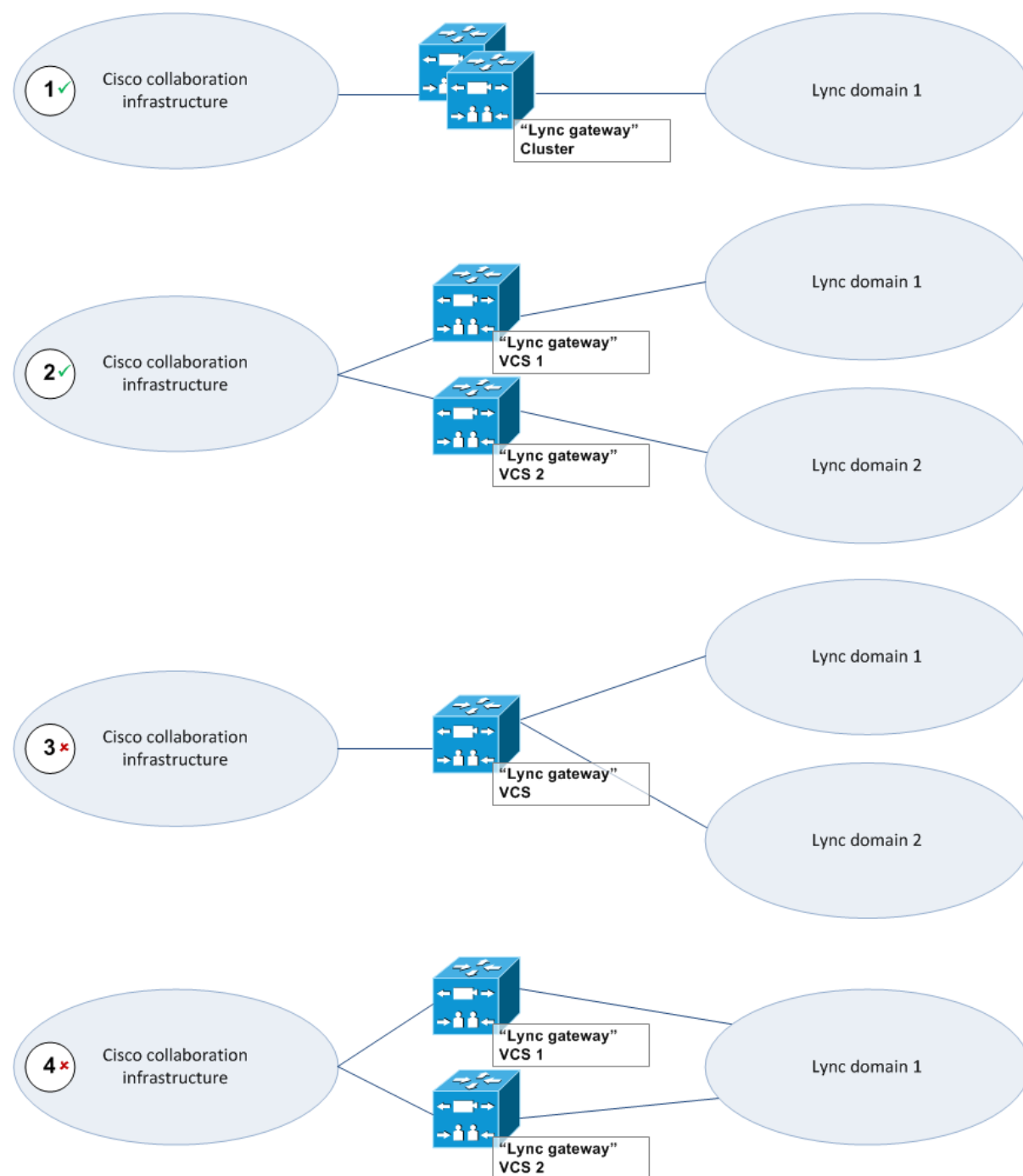
Multiple Lync domains and relationships to multiple Lync gateway VCS

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

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

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

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



MCUs for ad hoc conferences from Lync

The configuration of VCS and Cisco MCU described in *Cisco TelePresence Multiway Deployment Guide* is the correct configuration for VCS and Cisco MCU when working with Lync Server. The MCU should be configured to support SIP access to conferences to avoid the need to interwork the Lync client calls.

MCUs must register to a VCS to allow Lync users to join conferences (MCUs cannot register to Lync Server; the "Lync gateway" VCS handles the protocol differences on behalf of the MCU). We recommend that MCUs

that are used for conferences that Lync clients can dial, are registered using their own domain (different from any other video or Lync domain) to the video network VCSs.

When configured in their own domain, the MCU conferences can be accessible via a static route configured on Lync for this MCU domain. If regional MCUs exist, the MCUs should have regional domains. For ad hoc conferences routed via the Lync static domain route:

- If the conference is not underway presence status will be “Offline”.
- If the conference has any participants, presence status will be “Available”.

Calling an MCU conference from a Lync device requires the MCU’s domain to be entered.

Note that:

- If the PUA is configured so that registered devices do not report ‘Available’, presence will always show “Off-line”.
- VCS supports a maximum of 100 presence subscriptions per presentity.

Small test/demo networks

For small test and demo networks, video endpoints may be registered to the “Lync gateway” VCS, the small video network being controlled by the same VCS that is the interface to Lync Server. (In this case, you need to configure the SIP domains and enable the Presence Server on the “Lync gateway” VCS.)

Scaling up from a small test/demo network

As extra capacity, regional management and reduced license usage is required, you can scale away from the ‘small test and demo network’ system to the “Lync gateway” VCS connected to video network approach. This is achieved by adding video network VCSs and neighboring them (directly, or indirectly through other VCSs) to the “Lync gateway” VCS.

Endpoints can be added to the video network VCSs and endpoints and other devices then gradually migrated off the “Lync gateway” VCS onto the video network VCSs.

Features and capabilities

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

Client support

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

Interoperability with different versions of Lync Server

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

Microsoft Lync Server 2010

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

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

Microsoft Lync Server 2013

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

Lync 2013 no longer supports H.263, so X8.1 or later software is required to interoperate successfully with Lync 2013. X7.2 or earlier software will work with Lync 2013 only if calls are routed through a Cisco AM GW transcoder.

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

Microsoft Lync B2BUA interoperating capabilities

When using the Microsoft Lync B2BUA:

- Domain static routes are set up on Lync Server to route calls to domains in the video network.
- Search rules are set up on VCS to route calls to Lync domains.
- Lync Server accepts and handles call hold (and resume) requests.
- Lync clients can be the object of a transfer (even if there is an AM gateway involved in the call).
- Lync clients can be joined into a Multiway conference (even if there is an AM gateway involved in the call).
- Presence updates are only supported from VCS to Lync Server:
 - Use of 'Available' for registered endpoints is optional via PUA configuration
 - "Off-line" and "Available" (not "In-call", which requires FindMe-based configuration) are reported for users (for up to 100 subscribers)
- Passing Lync presence to devices registered to VCS is not supported.
- Calls to Microsoft Mediation Servers work from endpoints in the VCS video network for SIP initiated calls, but do not work for calls interworked from H.323 (unless the workaround specified in [Appendix 4: Interoperating capabilities and limitations \[p.69\]](#) is implemented).
- Lync systems may use hardware load balancers for resilience and capacity.
- A "Lync gateway" VCS (or VCS cluster) can communicate to Lync via Lync Director.
- Media encryption (SRTP) is supported when TLS is used between VCS and Lync and the **Microsoft Interoperability** option key is added to the "Lync gateway" VCS.
- SIP signaling and RTP media is always routed via the B2BUA application for calls involving Lync clients. Each B2BUA application (one application per VCS) can handle 100 simultaneous calls between Lync and the VCS video environment. However, a call involving Cisco AM GW will consume two B2BUA call resources.

Summary of configuration objectives

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

- SIP and H.323 video endpoints registered in the video network to other SIP and H.323 video endpoints registered in that same video network.
- Microsoft Lync clients registered on Lync Server to other Lync clients registered on that Lync Server.

- SIP and H.323 video endpoints registered in the video network to Lync clients registered on Lync.
- Lync clients registered on Lync Server to SIP and H.323 video endpoints registered in the video network.

It also describes how to enable presence so that Lync clients can see the presence status of endpoints registered in the video network.

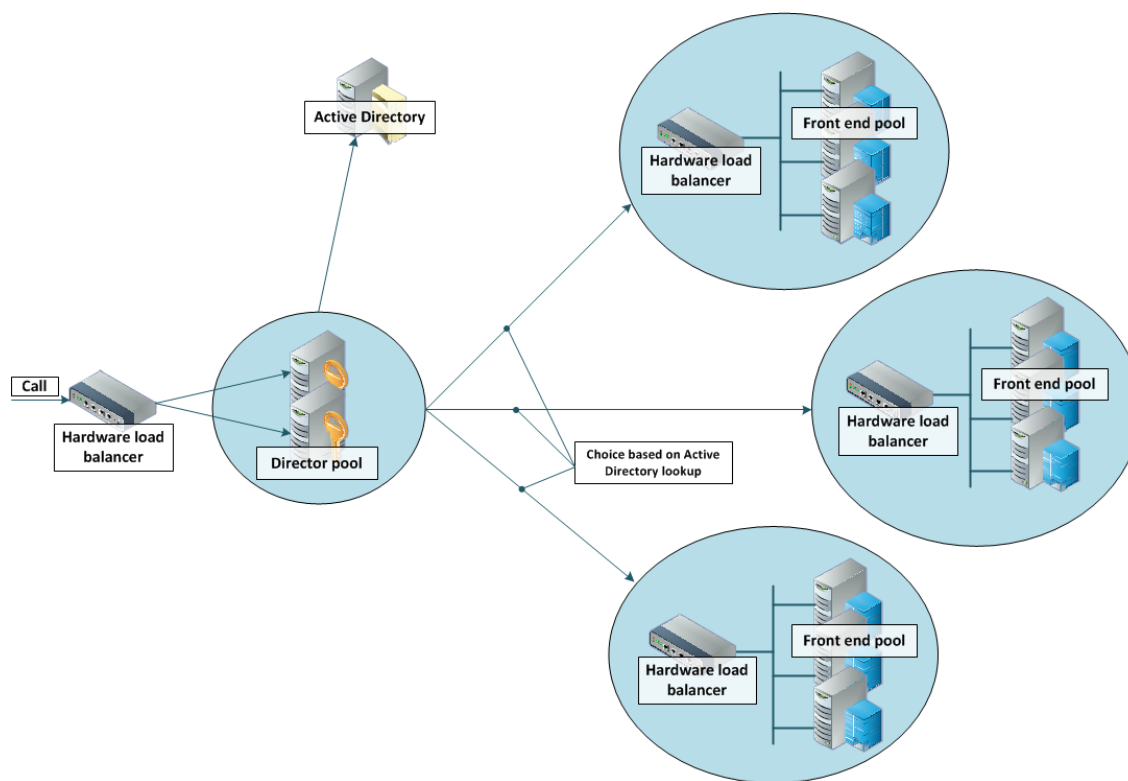
The configuration process describes each of these stages separately, so that individual stages can be implemented and tested before moving on to the next.

Lync environments

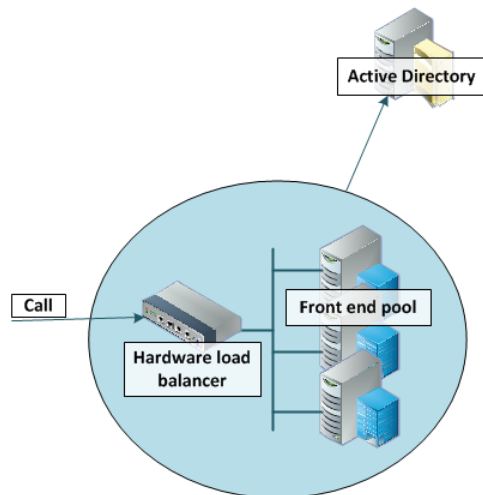
Lync environments have a number of building blocks, and so they may be constructed in many ways. A full scale Lync deployment is likely to use Lync Director, Hardware Load Balancers (HLBs), Front End Processors (FEPs) in enterprise pools, and a redundant AD server.

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

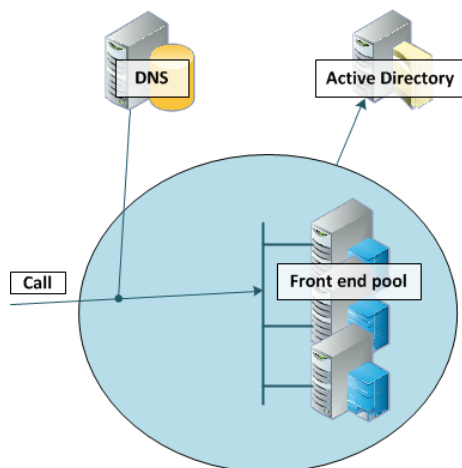
An example architecture is shown below:



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

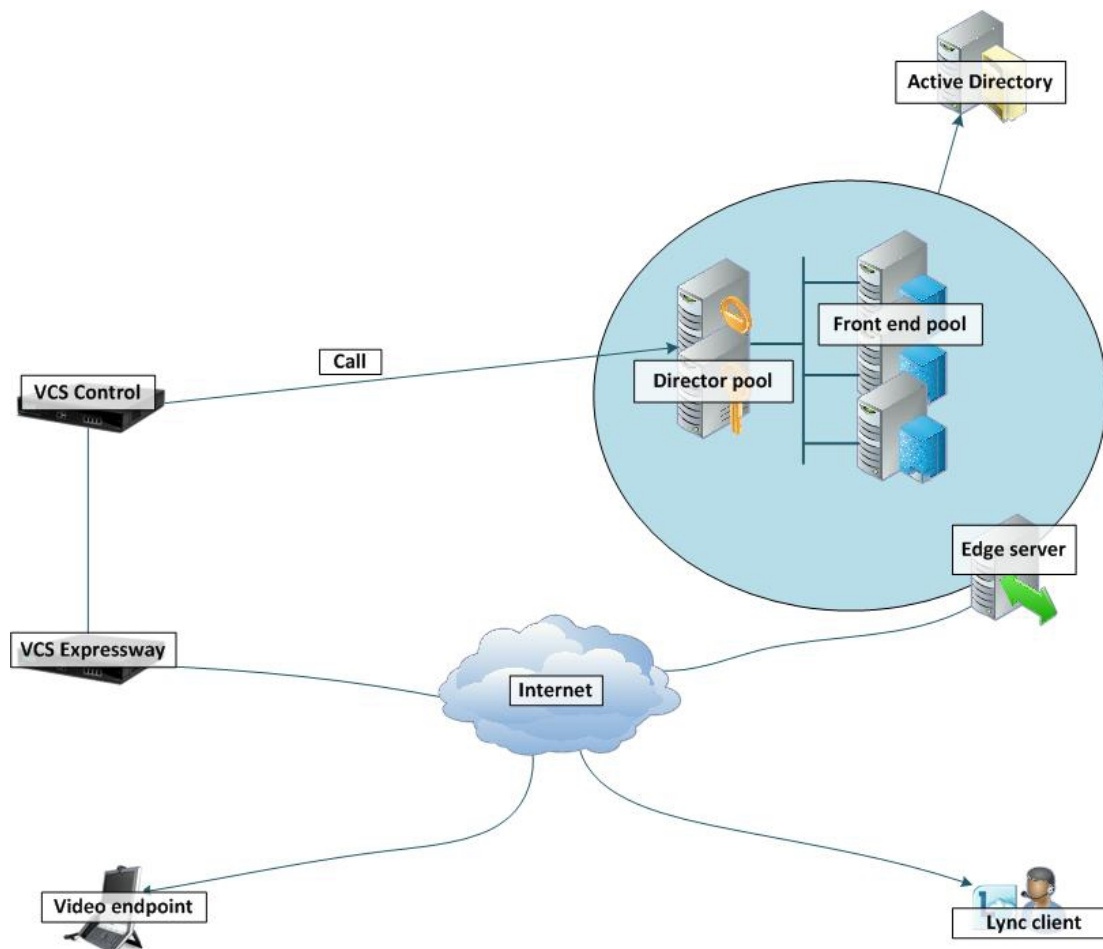


A Lync environment may use DNS instead of the Hardware Load Balancer, for example:



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

Lync deployments may also contain Edge servers to allow Lync clients to register from outside the local network through the Edge server to Lync. Communicating with Lync devices outside the edge server requires both the Edge Server and the VCS Expressway connecting to the public Internet. (Calls involving a Microsoft Edge server require the VCS 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 VCS and Lync:

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

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

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

“Lync gateway” VCS should be configured such that:

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

Prerequisites prior to configuring VCS and Lync to interoperate

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

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

Benefits of using the B2BUA over legacy OCS Relay

The Lync B2BUA is the preferred method of integrating Lync with VCS. It was introduced in VCS X7. It provides an interface between Lync and the video network and replaces the legacy OCS Relay application (removed from VCS in X8.1).

The B2BUA is a new application that expands upon the feature set of OCS Relay by providing:

- improved stability, speed and performance
- greatly enhanced logging/diagnostics capabilities (using the “Diagnostics logging” functionality of the VCS)
- improved ease of use (B2BUA does not require complex CPL to be installed on the VCS, which was required with OCS Relay)
- improved configuration and control (B2BUA has a variety of available configuration settings whereas OCS Relay was limited in terms of configuration options)
- support for Lync clients registered via an Edge server (requires a VCS Expressway and the **Microsoft Interoperability** option key)
- TURN/ICE support embedded into the B2BUA (requires VCS Expressway and the **Microsoft Interoperability** option key)

Video network: check that calls between endpoints registered to VCS Controls operate as expected

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

VCS Control configuration summary

The configuration of the VCS Control in the video network to allow calls to be made between endpoints that register to them should already have been carried out. Ensure that the SIP domain of the video network, which is needed for SIP registration and presence handling, is configured.

If appropriate, you may also want to configure interworking to handle calls with any H.323 endpoints that are registered to other systems in the video network.

Note that in small test and demo networks this configuration is carried out on the same VCS that is the “Lync gateway” VCS.

Ensure SIP domain of video network endpoints is configured in the VCS Control

SIP endpoints register with the VCS Control with a URI in the format `user-id@sip-domain`. The VCS Controls accepting these registrations must be configured with the SIP domain information so that it will accept these registrations.

1. Go to **Configuration > Domains**.
2. Check that the domain is listed; if it is not listed:
 - a. Click **New**.
 - b. Set **Name** to, for example, `vc.ciscotp.com`.
 - c. Click **Create domain**.
3. Repeat for any other domains being used, such as `mcu.ciscotp.com`.

Optional. Configuring interworking for H.323 endpoints registered to other systems

By default the VCS Control will perform H.323 to SIP protocol interworking between H.323 endpoints registered to the VCS Control and any SIP devices also registered to the VCS Control or to Lync devices.

If you have any H.323 endpoints that are registered to other systems in the video network, you will need change the interworking configuration from the default of *Registered only* to *On*:

1. Go to **Configuration > Protocols > Interworking**.
2. Set **H.323 <-> SIP interworking mode** to *On*.
3. Click **Save**.

Lync configuration

No configuration is required on Lync to allow endpoints registered on the VCS Control to call other endpoints registered on the VCS Control.

Registering video endpoints to the video network

Video endpoint configuration

For H.323, configure the endpoints as follows:

- H.323 ID (for example, david.jones.office@vc.ciscotp.com)
- H.323 Call Setup Mode = Gatekeeper
- Gatekeeper IP address = IP address or FQDN of VCS Control (cluster)

For SIP, configure the endpoints as follows:

- SIP Address (URI) (for example, alice.parkes.office@vc.ciscotp.com)
- Server Address (Proxy address) = IP address or FQDN of VCS Control (cluster)

Confirming registrations

Registration status can be confirmed on the [Registrations](#) page ([Status > Registrations](#)).

By default the VCS Control accepts all registrations to SIP domains configured in the VCS Control. You can limit registrations by explicitly allowing or denying individual registrations (see *VCS Administrator Guide* for further details).

Calls can now be made between endpoints registered on VCS Control.

Testing the configuration

To test the configuration:

1. Make some test calls between the endpoints.
2. Clear the calls.
3. Check the [Call history](#) page on the VCS Control ([Status > Calls > History](#)).

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

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

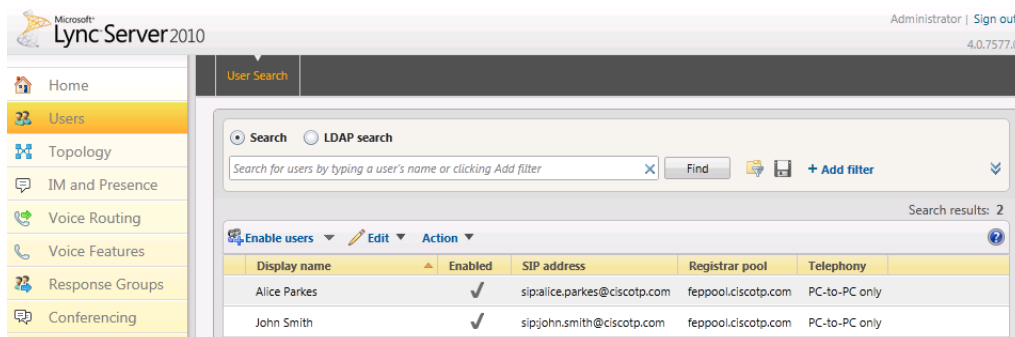
VCS Control configuration

No configuration is required on VCS Control for endpoints registered on Lync to call other endpoints registered on Lync Server.

Enabling users for Lync

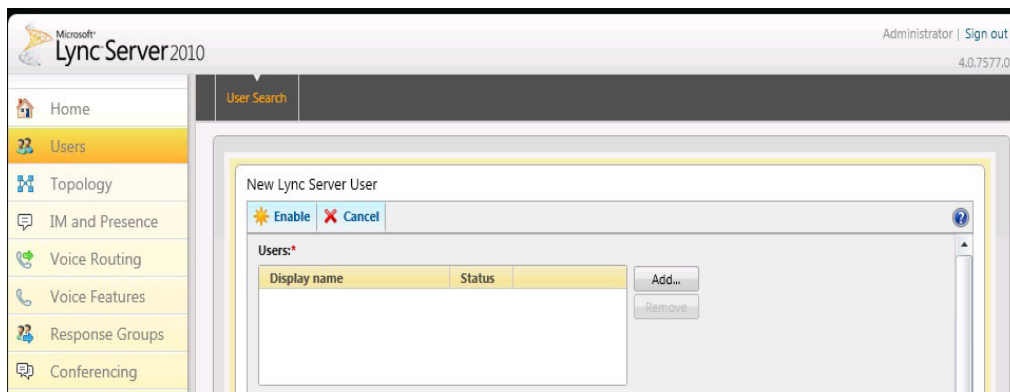
By default, Active Directory users are not Lync enabled. Check that users required to support Lync are enabled to do so, and if not enable them. This can be done both by Lync Server Control Panel or through Windows PowerShell commands (using Lync 2010 as an example):

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

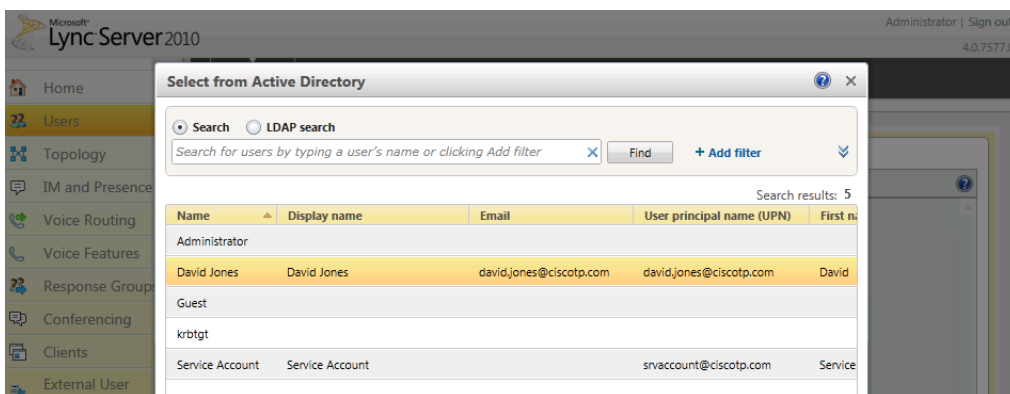


To add a new user:

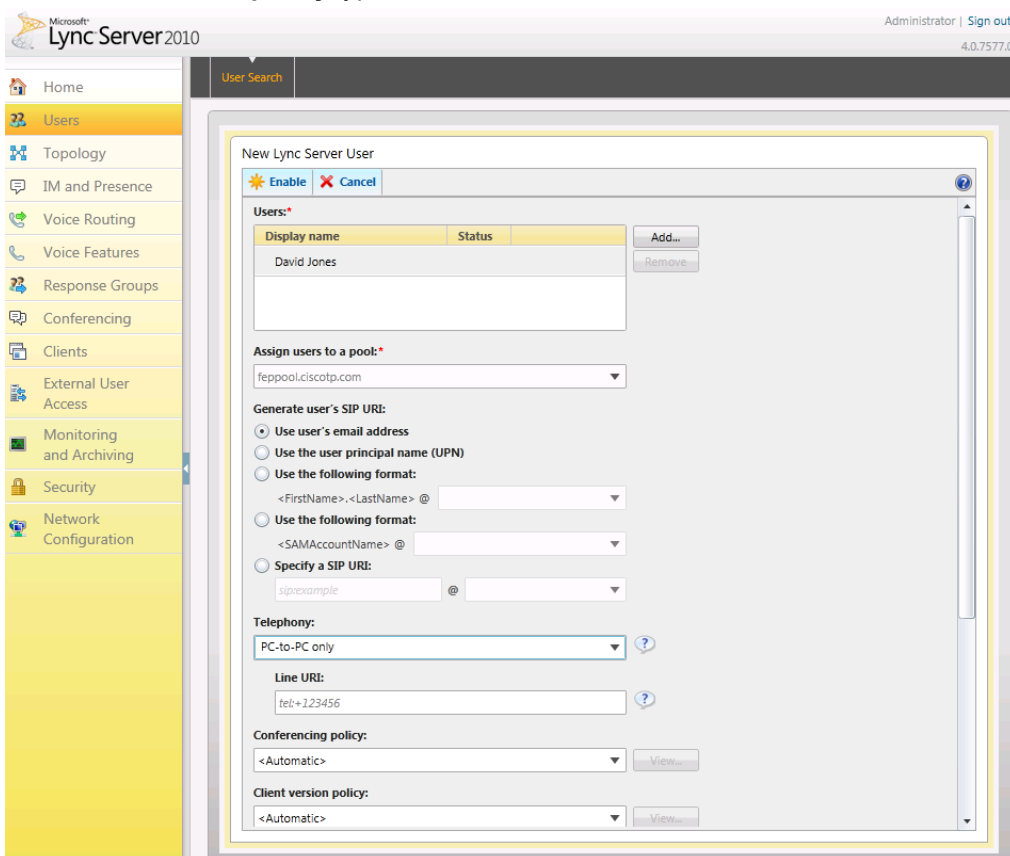
1. Select **Enable users** and click **Add**.



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



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




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

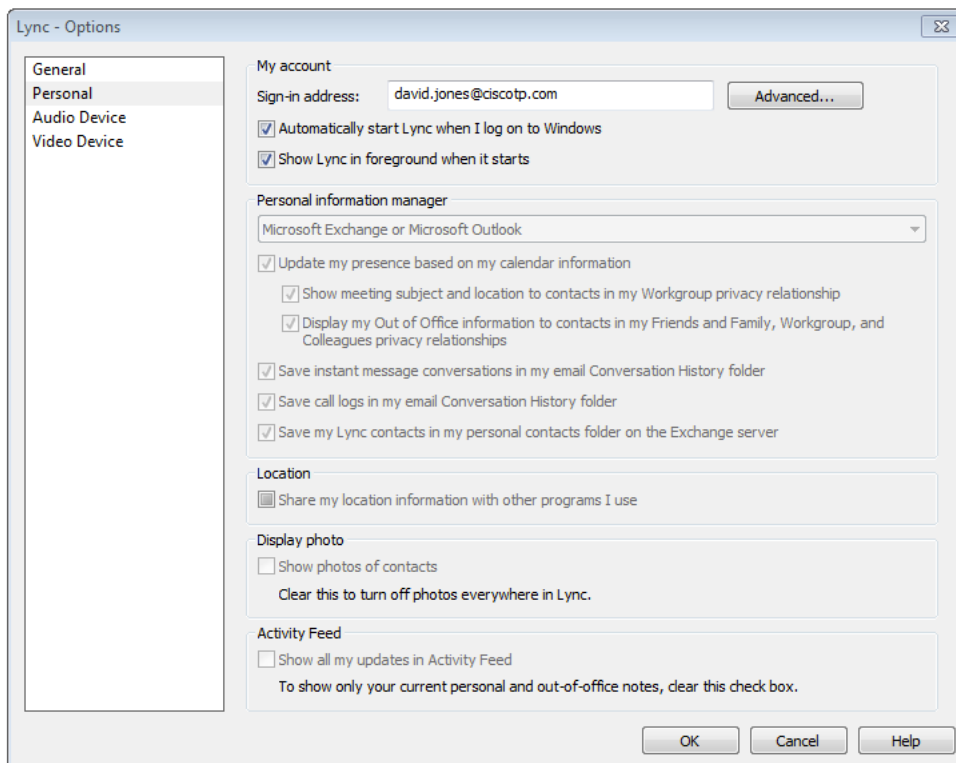
For example:

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

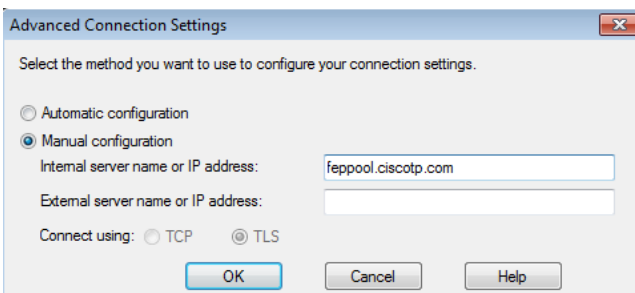
Registering Lync clients to the Lync Server

Lync client configuration

1. Install and start the Lync client.
2. On the Sign in screen, click on the  icon or select the menu arrow beside it and select **Tools > Options**.
3. Select **Personal**.
4. Set up **Sign-in address** as required.
This is the SIP URI of the Lync user, for example david.jones@ciscotp.com:



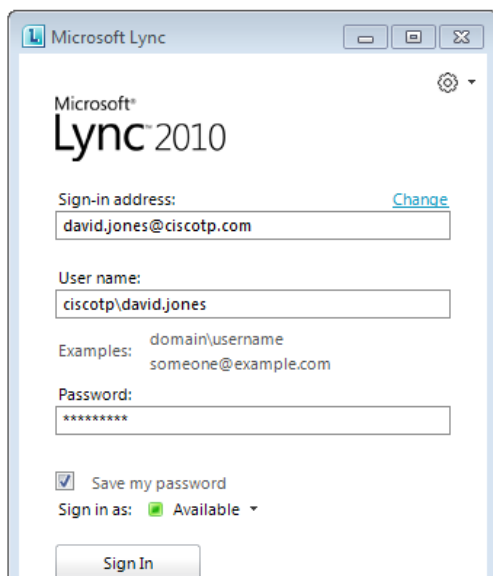
5. Click **Advanced**.



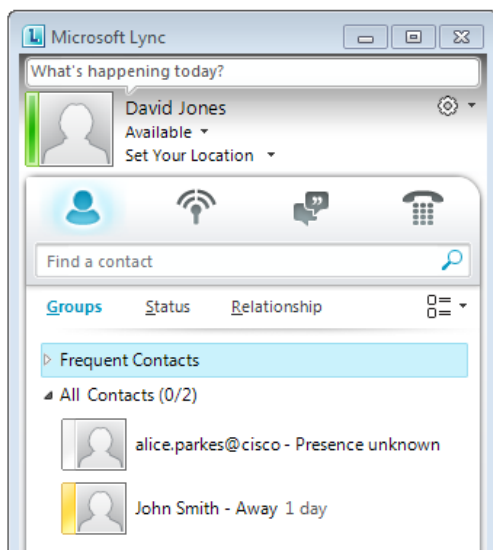
6. In a production environment ensure *Automatic configuration* is selected.
If this does not work, select *Manual configuration* and set **Internal server name or IP address** to the FQDN of the Lync Server.
7. Click **OK** to return to the **Lync - Options** panel.
8. Click **OK** to return to the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

10. Enter the **User name** and **Password**.

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



11. Click **Sign In**.



Testing the configuration

To make a video call between Lync endpoints:

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

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

This is configured in 4 stages:

1. Video network: VCS Control configuration
2. "Lync gateway" VCS configuration (part 1)
3. Lync Server configuration
4. "Lync gateway" VCS configuration (part 2)

Video network: VCS Control configuration

The video network must have a link to the "Lync gateway"; to configure this:

1. Set up a neighbor zone from the VCS Control to the "Lync gateway" VCS (cluster).
2. Set up a search rule, on the VCS Control, to route calls to the Lync domain to the "Lync gateway" VCS (cluster).
3. If required, set up search rules on the VCS Control to route calls to any other domains supported on Lync (but not in the video network) to the "Lync gateway" VCS (cluster). There may not be any such domains, so this step may not be required.

Note that in small test and demo networks this configuration is not necessary - the video network VCS is the "Lync gateway" VCS. In this case, skip the following sections and go to ["Lync gateway" VCS configuration \(part 1\) \[p.27\]](#).

Video network: Set up a neighbor zone from VCS Control to the "Lync gateway" VCS


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


| | |
|---|--|
| Name | An appropriate name, for example "To Lync gateway" |
| Type | <i>Neighbor</i> |
| SIP mode | <i>On</i> |
| SIP port | 5061 (or the value that is the same as that configured on the "Lync gateway" VCS for TLS mode SIP) |
| SIP transport | <i>TLS</i> |
| H.323 mode | <i>Off</i> |
| In the Location section: Peer 1 address | IP address or FQDN of the "Lync gateway" VCS (or the 1st VCS in the "Lync gateway" VCS cluster) |
| In the Location section: Peer 2 to Peer 6 address | IP address or FQDN of the 2nd to 6th "Lync gateway" cluster peers (if any) |
| In the Advanced section: Zone profile | <i>Default</i> |


4. Click **Create zone**.

Create zone You are here: [Configuration](#) > [Zones](#) > [Zones](#) > Create zone


Configuration

Name * 


Type * 


Hop count * 


H.323


Mode 


SIP


Mode 


Port * 

Transport 


TLS verify mode 


Accept proxied registrations 

Media encryption mode 


ICE support 


Authentication


Authentication policy 


SIP authentication trust mode 


Location


Peer 1 address 

Peer 2 address 


Peer 3 address 

Peer 4 address 

Peer 5 address 

Peer 6 address 

Advanced

Zone profile 

Video network: Set up a search rule on VCS Control to route calls for the Lync domain to the "Lync gateway" VCS

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the following fields (leave all other fields with default values):

| | |
|----------------------------|---|
| Rule name | An appropriate name, for example "Route to Lync gateway" |
| Priority | Leave as default, for example 100 |
| Source | <i>Any</i> |
| Mode | <i>Alias pattern match</i> |
| Pattern type | <i>Regex</i> |
| Pattern string | <code>.+@ciscotpl.com.*</code> |
| Pattern behavior | <i>Leave</i> |
| On successful match | <i>Continue</i> |
| Target | Select the Lync gateway zone, for example "To Lync gateway" |

4. Click **Create search rule**.

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

Configuration

| | |
|-------------------------------|---------------------------|
| Rule name | * Route to Lync gateway ⓘ |
| Description | ⓘ |
| Priority | * 100 ⓘ |
| Protocol | Any ⓘ |
| Source | Any ⓘ |
| Request must be authenticated | No ⓘ |
| Mode | Alias pattern match ⓘ |
| Pattern type | Regex ⓘ |
| Pattern string | * .+@ciscotpl.com.* ⓘ |
| Pattern behavior | Leave ⓘ |
| On successful match | Continue ⓘ |
| Target | * To Lync gateway ⓘ |
| State | Enabled ⓘ |

Video network: Set up search rules to route calls to the "Lync gateway" VCS for domains supported on Lync (but not in the video network)

There may be no additional domains supported by Lync, but if there are:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

- Configure the following fields (leave all other fields with default values):

| | |
|----------------------------|---|
| Rule name | An appropriate name, for example "Route domain xxx to Lync gateway" |
| Priority | Leave as default, for example 100 |
| Source | <i>Any</i> |
| Mode | <i>Alias pattern match</i> |
| Pattern type | <i>Regex</i> |
| Pattern string | <code>.+@<relevant domain>.*</code> |
| Pattern behavior | <i>Leave</i> |
| On successful match | <i>Stop</i> |
| Target | Select the Lync gateway zone, for example "To Lync gateway" |

- Click **Create search rule**.
- Repeat the process if additional search rules are needed, for example a search rule for the dedicated MCU domain mcu.ciscotp.com.

"Lync gateway" VCS configuration (part 1)

This comprises the following steps:

- Load CA certificate and server certificate onto VCS for TLS connectivity with Lync.
- Configure DNS.
- Ensure that a cluster name is configured.
- Configure an NTP server.
- Ensure that TLS is enabled in SIP configuration.

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

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

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

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

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

- **Subject Name:** the VCS peer's FQDN e.g. vcs01.ciscotp.com
and if it is part of a cluster:
- **Subject Alternate Name:** a comma separated list of the VCS cluster's FQDN and the VCS peer's routable FQDN, e.g. lyncvcs.ciscotp.com, vcs01.ciscotp.com

The VCS's trusted CA certificate is loaded via **Maintenance > Security certificates > Trusted CA certificate**.

The VCS's server certificate is loaded via **Maintenance > Security certificates > Server certificate**.

See [VCS Certificate Creation and Use Deployment Guide](#) for more details about creating certificates for VCS.

"Lync gateway" VCS: Configure DNS and local hostname

Configure the DNS server details

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

On a machine running Lync Server:

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

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

On each "Lync gateway" VCS peer:

1. Go to **System > DNS**.
2. If the DNS server that Lync Server uses can provide all DNS lookups needed by VCS:
 - 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 VCS must use other DNS servers for normal calls and only the Lync DNS server for Lync access: Configure the **Default DNS servers** with the servers which will be used for normal, non-Lync related DNS operation and configure the **Per-domain DNS servers** section as follows:

| | |
|-----------------------------|--|
| Address 1 | IP address of the DNS server used by Lync Server |
| Domain names | Domain shared with Lync |
| Address 2 ... 5 | Use these fields only if Lync Server uses more than one DNS server |
| Domain names 2 ... 5 | Use these fields only if Lync Server uses more than one DNS server; configure with the domain shared with Lync |

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

Ensure that Local hostname and DNS domain are configured

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

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

Note that:

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

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

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

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

"Lync gateway" VCS: Configure an NTP server

On each "Lync gateway" VCS peer:

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

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

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

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

Lync Server configuration

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

- If a Lync Director is in use, then configure the Lync Director (pool) to trust the "Lync gateway" VCS and to route traffic to VCS. Other FEPs receiving calls for the video domain may not know how to route them (depending on Lync SIP routing configuration), and may pass the calls to the Director pool for routing.

- If there is just a hardware load balancer in front of a set of FEP pools, configure each FEP pool.
- If there is just a single FEP, configure it.

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

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

Trust a "Lync gateway" VCS

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

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

1. Select **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Management Shell**.

2. Set one or more "Lync gateway" VCSs as a trusted application for Lync Server (VCS is treated as an application by Lync Server).

Use the command **New-CsTrustedApplicationPool** with the following parameters:

-**Identity**: specifies the "Lync gateway" VCS **cluster** FQDN. This name must match the Common Name / Subject Alternate Name specified in the VCS server certificate e.g. lyncvcs.ciscotp.com.

-**ComputerFqdn**: specifies the "Lync gateway" VCS **peer** FQDN (specify the master VCS FQDN if running a cluster), e.g. vcs01.ciscotp.com. This name must match the Common Name specified in the VCS server certificate.

-**Registrar**: specifies the FQDN of the registrar for the Lync pool

-**Site**: specifies the siteID on which this application pool is homed

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

-**RequiresReplication**: specifies that this trusted application must not be replicated between Pools (must be \$false)

-**ThrottleAsServer**: reduces the message throttling as it knows the trusted device is a server, not a client (must be \$true)

-**TreatAsAuthenticated**: specifies that this application is authenticated by default (must be \$true)

For example:

```
C:\Users\administrator.CISCOTP>New-CsTrustedApplicationPool -Identity lyncvcs.ciscotp.com -ComputerFqdn vcs01.ciscotp.com -Registrar feppool.ciscotp.com -site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
```

3. (For TCP only deployments) Use the Topology Builder to configure the IP address of the "Lync gateway" VCS as a trusted server:
 - a. Select **Start > All Programs > Microsoft Lync Server 2010 > Topology Builder**.
 - b. Under **Lync Server 2010 > Trusted Application Servers**, right-click on the VCS host and select **Edit Properties**.
 - c. In the **General** tab, select **Limit service usage to selected IP addresses**, enter the **Primary IP address** of the VCS and click **OK**.
 - d. Publish the topology (you may need to restart the Lync Front-End Service to make sure that topology changes are applied).
4. If using a cluster of "Lync gateway" VCSs, use the shell to add the additional cluster peer members as computers to the trusted application pool using the command **New-**

CsTrustedApplicationComputer with the following parameters:

-**Identity**: specifies the FQDN of the VCS cluster peer being added, e.g. vcs02.ciscottp.com. This name must match the Common Name specified in the VCS server certificate.

-**Pool**: specifies the FQDN of the application pool this VCS is being added to (identical to the FQDN used for -Identity in the previous step, e.g. lyncvcs.ciscottp.com).

For example:

```
C:\Users\Administrator.CISCOTP> New-CsTrustedApplicationComputer -Identity vcs02.ciscottp.com -Pool lyncvcs.ciscottp.com
```

5. Assign an application to a specific application pool:

Use the command **New-CsTrustedApplication** with the following parameters:

-**ApplicationId**: specifies a label for the "Lync gateway" VCS application (it is internal to Lync only, not a DNS name)

-**TrustedApplicationPoolFQdn**: specifies the "Lync gateway" VCS FQDN (or "Lync gateway" VCS Cluster name if present)

-**Port**: specifies TLS/TCP port to use for neighboring. This should be set to the port configured as **Port on B2BUA for Lync call communications** in the B2BUA advanced settings on the VCS (default 65072).

-**enableTCP**: this must be included only if TCP is the chosen transport protocol

For example, for TLS:

```
C:\Users\administrator.CISCOTP>New-CsTrustedApplication -ApplicationId VCSApplication1 -TrustedApplicationPoolFqdn lyncvcs.ciscottp.com -Port 65072
```

For example, for TCP:

```
C:\Users\administrator.CISCOTP>New-CsTrustedApplication -ApplicationId VCSApplication1 -TrustedApplicationPoolFqdn lyncvcs.ciscottp.com -Port 65072 -EnableTCP
```

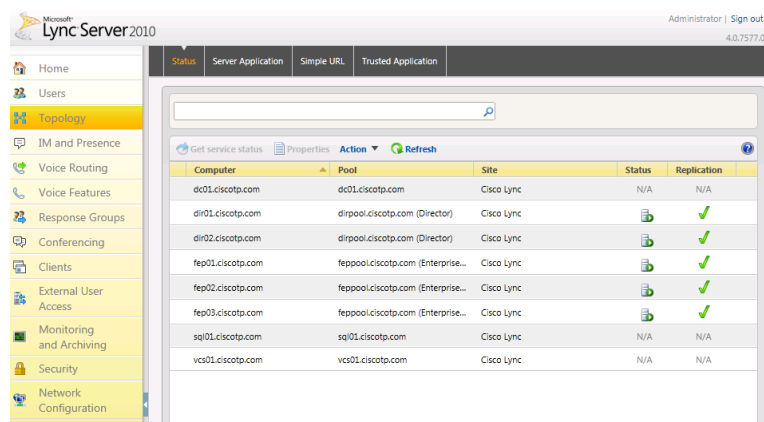
6. Apply the configuration

Use the command **Enable-CsTopology**.

For example:

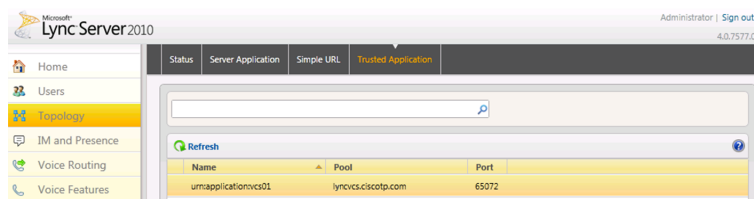
```
C:\Users\administrator.CISCOTP>Enable-CsTopology
```

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



| Computer | Pool | Site | Status | Replication |
|---------------------|--------------------------------------|------------|--------|-------------|
| dc01.ciscottp.com | dc01.ciscottp.com | Cisco Lync | N/A | N/A |
| dir01.ciscottp.com | dirpool.ciscottp.com (Director) | Cisco Lync | | ✓ |
| dir02.ciscottp.com | dirpool.ciscottp.com (Director) | Cisco Lync | | ✓ |
| feep01.ciscottp.com | feepool.ciscottp.com (Enterprise...) | Cisco Lync | | ✓ |
| feep02.ciscottp.com | feepool.ciscottp.com (Enterprise...) | Cisco Lync | | ✓ |
| feep03.ciscottp.com | feepool.ciscottp.com (Enterprise...) | Cisco Lync | | ✓ |
| sq01.ciscottp.com | sq01.ciscottp.com | Cisco Lync | N/A | N/A |
| vcs01.ciscottp.com | vcs01.ciscottp.com | Cisco Lync | N/A | N/A |

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



Configure Lync Server media encryption capabilities

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

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

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

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

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

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

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

For example:

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

Note that:

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

"Lync gateway" VCS configuration (part 2)

This comprises the following steps:

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

Configure the B2BUA on the "Lync gateway" VCS

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


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

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


| | |
|---|--|
| Microsoft Lync B2BUA | <i>Enabled</i> |
| Lync signaling destination address | IP address or FQDN of device specified above, for example dirpool.ciscotp.com |
| Lync signaling destination port | IP port used by device specified above – typically 5061 |
| Lync signaling transport | <i>TLS</i> |
| Register FindMe users as clients on Lync | <i>No</i> |
| Enable transcoders for this B2BUA | If no Cisco AM GW is to be used, set to <i>No</i> . If an Cisco AM GW is to be used, see <i>Microsoft Lync 2010, VCS and Cisco AM GW Deployment Guide</i> |
| Offer TURN Services | <i>No</i> |
| Advanced settings | Leave all advanced settings at their default values |


3. Click **Save**.


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


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

Configuration


Microsoft Lync B2BUA Enabled 

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


Lync signaling destination port ★ 

Lync signaling transport TLS 


Capabilities

Register FindMe users as clients on Lync No 

Transcoders

Enable transcoders for this B2BUA No 

TURN

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

Advanced

Advanced settings [Show advanced settings](#)

"To Microsoft Lync Server via B2BUA" neighbor zone

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

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

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

Search rules can also be used to transform URIs before they are sent to a neighbor, for example to add or modify the domain or add, remove or translate user-id prefixes and even to add extra tags to SIP URIs, such as user=phone (see [TEL URI handling for VCS to Lync calls \[p.81\]](#) for further information about user=phone).

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

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the search rule so that all calls to URIs in the format `.+@ciscotp.com.*` are forwarded to Lync. (To handle presence messaging a `.*` is included at the end of the domain to allow any parameters

following the domain to be retained in the SIP messaging.)

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

4. Click **Save**.

The screenshot shows a 'Configuration' window for a search rule. The fields and their values are as follows:

- Rule name:** To Lync
- Description:** (empty)
- Priority:** 100
- Source:** Any
- Request must be authenticated:** No
- Mode:** Alias pattern match
- Pattern type:** Regex
- Pattern string:** .+@ciscotpl.com.*
- Pattern behavior:** Leave
- On successful match:** Stop
- Target:** To Microsoft Lync server via B2BUA
- State:** Enabled

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

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

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

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

3. Configure the search rule so that all calls to the relevant URI are routed to Lync.

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

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

Calls can now be made between SIP / H.323 endpoints registered on the video network to Lync clients registered on Lync Server.

Testing the configuration

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

For example, call david.jones@ciscotp.com or alice.parkes@ciscotp.com from both SIP and H.323 endpoints registered on VCS Control.

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

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

This is configured in 2 stages:

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

“Lync gateway” VCS configuration

This comprises the following steps:

1. Configure the B2BUA trusted hosts on the “Lync gateway” VCS.
2. Configure the “Lync gateway” VCS with a neighbor zone that contains the video network.
3. Set up one or more search rules to route calls with video network domains to the video network (include a rule for the MCU domain if used).

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

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

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

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

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

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

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

Configuration

Name

IP address

Type

Notes:

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

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

Note that in small test and demo networks, this step is not necessary as the video network VCS is the “Lync gateway” VCS.


1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
We recommend that the connection to the “Lync gateway” VCS uses SIP over TLS to communicate so that encrypted calls can be handled.
3. Configure the following fields:


| | |
|---|---|
| Name | “To Video network” |
| Type | <i>Neighbor</i> |
| SIP mode | <i>On</i> |
| SIP port | 5061 (or the value that is the same as that configured on the video network VCS for TLS mode SIP) |
| SIP transport | <i>TLS</i> |
| H.323 mode | <i>Off</i> |
| Location: Peer 1 address | IP address or FQDN of the video network VCS (or the 1st VCS in the video network cluster) |
| Location: Peer 2 to Peer 6 address | IP address or FQDN of the 2nd to 6th video network cluster peers (if any) |
| Advanced: Zone profile | <i>Default</i> |


4. Click **Save**.

Create zone You are here: [Configuration](#) > [Zones](#) > [Zones](#) > Create zone


Configuration

Name * 


Type 


Hop count * 


H.323


Mode 


SIP


Mode 


Port * 

Transport 


TLS verify mode 


Accept proxied registrations 

Media encryption mode 


ICE support 


Authentication


Authentication policy 


SIP authentication trust mode 


Location


Peer 1 address 

Peer 2 address 


Peer 3 address 

Peer 4 address 

Peer 5 address 

Peer 6 address 

Advanced

Zone profile 

Setting up search rules to route calls with video network domains to the video network

Note that in small test and demo networks, this step is not necessary as the video network VCS Control is the “Lync gateway” VCS.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the following fields:
4. Configure the search rule to match the domain supported in the video network:

| | |
|----------------------------|---|
| Rule name | An appropriate name, for example “Route to Video network” |
| Priority | Leave as default, for example 100 |
| Source | <i>Any</i> |
| Mode | <i>Alias pattern match</i> |
| Pattern type | <i>Regex</i> |
| Pattern string | Anything in the video network domain, for example <code>.*@vc\.ciscotpl\.com.*</code> |
| Pattern behavior | <i>Leave</i> |
| On successful match | <i>Continue</i> |
| Target zone | Select the video network zone, for example “To Video network” |

5. Click **Save**.

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

Configuration

| | |
|-------------------------------|---|
| Rule name | * Route to Video network i |
| Description | i |
| Priority | * 100 i |
| Protocol | Any i |
| Source | Any i |
| Request must be authenticated | No i |
| Mode | Alias pattern match i |
| Pattern type | Regex i |
| Pattern string | * .*@vc\.ciscotpl\.com.* i |
| Pattern behavior | Leave i |
| On successful match | Continue i |
| Target | * To Video network i |
| State | Enabled i |

Create search rule Cancel

6. Repeat these steps to add a rule for each video network domain, including the mcu domain (for example, `.*@mcu.ciscotpl.com`).

Configuring Lync Server domain static routes

This involves configuring domain static routes that route calls to the video and MCU domains to the “Lync gateway” VCS.

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

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

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

For example, for TLS:

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

For example, for TCP:

```
C:\Users\administrator.CISCOTP> $Route1=New-CsStaticRoute -TCPRoute -Destination "10.0
.0.2" -MatchUri "vc.ciscotp.com" -Port 65072
```

2. Assign a static route.
Use the command **Set-CsStaticRoutingConfiguration** with the following parameters:
-Identity: specifies where to apply the route. It can be at the global level or on a specific pool.
-Route @{Add=}: the route (defined earlier) to assign to the Identity (note that brackets are “curly”).
For example:

```
C:\Users\administrator.CISCOTP> Set-CsStaticRoutingConfiguration -Identity global -Route
te @{Add=$Route1}
```
3. Verify the static route assignment. Use the command :
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
4. Repeat the process for the mcu domain mcu.ciscotp.com and any other domains in the video network.
To do this for the mcu domain, create and assign the static route using the same commands as above, but use a different label (\$Route2) and specify **-MatchUri "mcu.ciscotp.com"**.

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, VCS will receive any requests to that domain that Lync cannot handle, and thus may receive significant volumes of mis-dial traffic.

Testing the configuration

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

Enabling Lync clients to see the presence of endpoints registered on VCS Control

Lync and VCS support for presence is as follows:

- Using SIP-SIMPLE, Lync Server only supports the reception of the “available” status, so presence is limited to buddies indicating “gray” (not available), or “green” (available). “In-call” and other rich presence states are not handled. VCS only supports a maximum of 100 subscriptions per presentity.
- Lync Server does not supply presence status information about its registered endpoints using SIP-SIMPLE and so no presence information can be supplied to endpoints registered on VCS about endpoints registered on Lync Server.
- Lync clients registered to Lync Server can see the presence status of other Lync clients registered to Lync Server.
- Endpoints registered to VCS Control can see the presence status of other endpoints registered to VCS Control.

In summary:

| | ... to VCS | ... to Lync Server |
|---------------------------|-----------------------------------|---------------------------|
| VCS to ... | Full presence available | Presence = Available only |
| Lync Server to ... | No presence information available | Full presence available |

Note that if you configure your system to register FindMe IDs to Lync Server, “In-call” states are also provided to Lync Server. See [Using FindMe for enhanced deployments \[p.46\]](#)

VCS Control configuration

We recommend that the Presence Server is enabled on the VCS Control.

If endpoints registered to the VCS Control do not support the generation of presence information, the VCS Control can generate it on their behalf by enabling the PUA (Presence User Agent):

- PUA generates Presence of *In-call* if the endpoint is in a call
- PUA optionally (and by default) generates Presence of *Available* if the endpoint is registered

If an endpoint is generating presence and the PUA is enabled, the VCS Presence Server will use the endpoint generated presence information.

Note that for H.323 devices to supply presence (via the PUA), the registered H323 ID of that endpoint must resemble a SIP URI (in the format name@domain). The PUA will publish presence for that URI.

To configure presence on the VCS Control:

1. Go to **Applications > Presence**.
2. Configure the following fields:

| | |
|---------------------------------------|---|
| SIP SIMPLE Presence User Agent | <i>On</i> (if VCS Control is to generate presence information for registered endpoints) |
|---------------------------------------|---|

| | |
|--|---------------|
| Default published status for registered endpoints | <i>Online</i> |
|--|---------------|

| | |
|-----------------------------------|-----------|
| SIP SIMPLE Presence Server | <i>On</i> |
|-----------------------------------|-----------|

3. Click **Save**.

Presence You are here: [Applications](#) > Presence

PUA

SIP SIMPLE Presence User Agent On ⓘ

Default published status for registered endpoints Online ⓘ

Presence Server

SIP SIMPLE Presence Server On ⓘ

Save

"Lync gateway" VCS configuration

Ensure that the Presence Server is **not** enabled on the "Lync gateway" VCS.

Testing the configuration

Set up the endpoints registered on VCS as buddies in Lync clients.

- Check the status of the Lync users on the "Lync gateway" VCS by looking at the [Lync user status](#) page ([Status](#) > [Applications](#) > [Lync users](#)). Check that:
 - Registration state = Registered
 - Subscription state = Subscribed
 - Presence state = offline or online
- See the icon on Lync client change from gray to green when an endpoint is registered on VCS (if **Default published status for registered endpoints** is set to *Online*).
- See the icon on Lync client change from green to gray if the endpoint becomes de-registered from VCS (if **Default published status for registered endpoints** is set to *Online*).

Enabling Microsoft Edge Server and VCS TURN capabilities

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

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

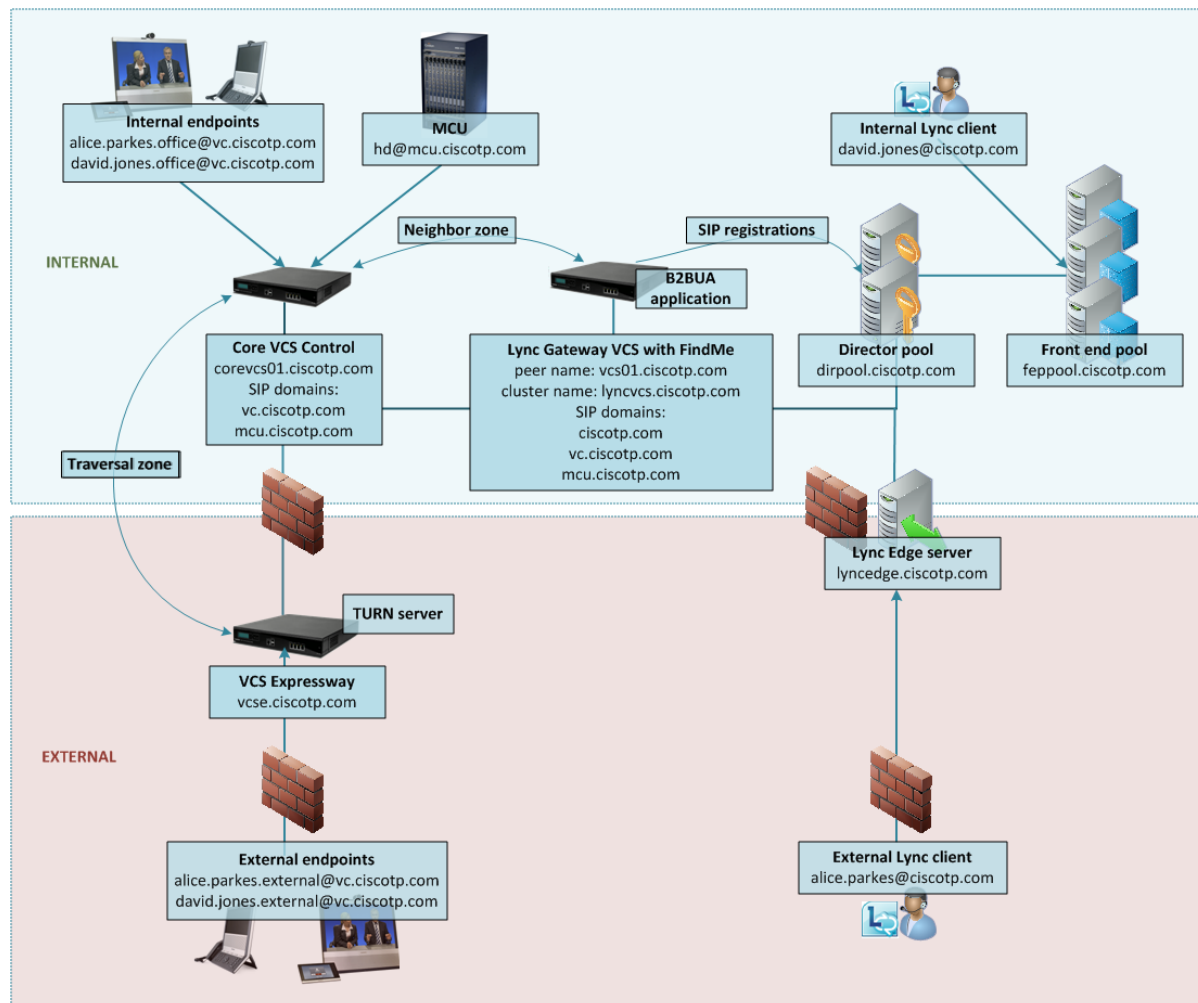
4. Click **Add address**.
5. Repeat the above steps if additional TURN servers are required.
6. Go to **Applications > B2BUA > Microsoft Lync > Configuration**.
7. Configure the fields as follows:

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

8. Click **Save**.

Using FindMe for enhanced deployments

You can optionally extend the deployment described in this guide by configuring your video network deployment to use FindMe. This provides richer presence and a more integrated environment. It uses the example deployment depicted below:



Deployment information

This deployment configuration consists of:

- FindMe accounts (also known as FindMe users) on the “Lync gateway” VCS that use the Lync network’s domain (ciscotp.com in this example). The B2BUA registers these FindMe accounts into Lync so that Lync sees them as though they were Lync client registrations, for example:
 - David with a URI david.jones@ciscotp.com, containing devices david.jones.office@vc.ciscotp.com and david.jones.external@vc.ciscotp.com
 - Alice with a URI alice.parkes@ciscotp.com, containing devices alice.parkes.office@vc.ciscotp.com and alice.parkes.external@vc.ciscotp.com

These FindMe accounts specify single or multiple endpoints as primary devices to call; the primary devices can be located anywhere in the video network or anywhere accessible via the video network.

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 a registration is to a B2BUA registered FindMe account, Lync Server will send the call to the B2BUA.
- 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 a corresponding Lync client also exists from a PC, the Lync client on the PC and the video endpoints specified in the FindMe will ring simultaneously when called, whether called from an endpoint communicating with VCS, or whether called from an endpoint communicating with Lync.

For calls into Lync (from whichever video endpoint the user wants to call from) to have a Caller ID / call back ID that works, FindMe must re-write the caller ID of calls to Lync with the relevant Lync SIP user ID. For FindMe to be able to do this, calls must be routed through the VCS holding the relevant FindMe; having a “Lync gateway” helps funnel all calls through the correct place.

- MCUs that will receive calls from Lync can register conferences to the video network with a dedicated MCU domain (mcu.ciscotp.com) and make these available to Lync users via a FindMe account (suitable for static conference aliases). Alternatively, you can still use a static SIP domain route from the Lync environment (suitable for ad-hoc conference aliases).
- The Lync static routes defined in the basic solution are no longer required (apart from those used for ad-hoc conference aliases).
- The Presence Server must reside on the “Lync gateway” VCS, and the “Lync gateway” VCS must be authoritative for the domain shared by Lync and the VCS (ciscotp.com), and all of the other domains used in the video network. It must hold the presence status of endpoints specified in the FindMe accounts in the Lync domain existing on this “Lync gateway” VCS (cluster), as FindMe presence only represents the presence of devices whose presence is known on that VCS (cluster).
- “Available”, “off-line” and “in-call” presence may be observed by Lync clients for users and any MCU conferences that are associated with a FindMe account on the “Lync gateway” VCS. Note: this requires that the primary video devices within the FindMe account have a URI-based alias, for example `firstname.lastname@domain` and that their presence is also held on the Presence Server on the “Lync gateway” VCS.

Clustered “Lync gateway” VCS

To provide enhanced load balancing, the “Lync gateway” VCS peers will distribute the shared domain FindMe users between themselves, and register their set with Lync Server. When Lync Server makes a call to one of these user IDs, the call will be presented to the VCS that made the registration – hence the calls are statically load-shared across the cluster.

If any peers go out of service, the remaining active peers take over the registrations of the unavailable peers.

“Lync gateway” VCS and multiple Lync domains

If Lync supports multiple domains, and the video network is to support these domains as well, we recommend that one “Lync gateway” VCS or VCS cluster is used to handle each domain. This is because the B2BUA only supports registering a single domain.

If some domains are not used in the video network, but need calls to be routed to them, there does not need to be a “Lync gateway” VCS for those domains. Search rules can be added to support routing to these domains.

If different Lync SIP domains are handled by different “Lync gateway” VCSs or VCS clusters, take care to ensure that each “Lync gateway” VCS or VCS cluster is authoritative for the presence information that is required for the B2BUA registered FindMe users for that one shared domain and all endpoints that are referenced by those FindMe entries.

MCU configuration for ad hoc conferences from Lync

We recommend that FindMe accounts are created for static/permanent conferences, where the FindMe account contains the SIP URI of the conference as a device. For FindMe-based permanent conferences, presence will show as:

- *Available* if conference does not have participants
- *In-Call* if conference has participants

Optionally, a FindMe account can be created which contains the SIP URI of the MCU's auto attendant. This will allow Lync users to join any conference via the auto attendant. However, this method will not utilize the 'In-call' presence status available for individual FindMe-based conferences.

Prerequisites

The FindMe option key must be installed on the "Lync gateway" VCS.

Configuring the "Lync gateway" VCS for FindMe

The "Lync gateway" VCS FindMe configuration consists of the following steps:

1. Configure all the required SIP domains.
2. Configure the B2BUA to register FindMe users to Lync.
3. Enable FindMe and create FindMe user accounts for each user that is to share Lync client and VCS endpoints.

Configure all the required SIP domains

B2BUA-registered FindMe users need the "Lync gateway" VCS to be authoritative for the Lync server's shared domain (ciscothp.com). It also needs to be authoritative for any other domains in the video network (to support the Presence Server, and to aggregate presence information for devices associated to the FindMe accounts).

1. Go to **Configuration > Domains**.
2. Click **New**.
3. Set **Name** to *ciscothp.com*.
4. Click **Create domain**.
5. Repeat for all the other domains in the video network, including vc.ciscothp.com and mcu.ciscothp.com.

Create domain You are here: [Configuration](#) > [Protocols](#) > [SIP](#) > [Domains](#) > Create domain

Configuration

Name ciscothp.com ⓘ

Configure the B2BUA to register FindMe users to Lync

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

| | |
|---|---|
| Register FindMe users as clients on Lync | Yes |
| Lync domain | Select the shared Lync domain, e.g. ciscotp.com |

- Click **Save**.

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

Configuration

Microsoft Lync B2BUA Enabled

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

Lync signaling destination port ★

Lync signaling transport TLS

Capabilities

Register FindMe users as clients on Lync Yes

Lync domain ciscotp.com [Configure SIP domains](#)

Transcoders

Enable transcoders for this B2BUA No

TURN

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

Advanced

Advanced settings [Show advanced settings](#)

Save

Enable FindMe and create FindMe user accounts for each user that is to share Lync client and VCS endpoints

- Go to **Maintenance > Option keys** and ensure that the **FindMe** key is listed.
- Go to **Applications > FindMe**.
 - Set **Mode** to *On*.
 - Set **Caller ID** to *FindMe ID*.
Setting FindMe to present the FindMe ID (rather than the endpoint ID) means that any device in the primary list of FindMe devices will provide the FindMe ID as the Caller ID. Thus, if a called party rings the caller ID back, all FindMe endpoints will ring, not just the endpoint that made the initial call.
 - Click **Save**.
- For each user that is to share Lync client and VCS endpoints, create a FindMe user account on the VCS with the same URI as the Lync client:

- a. Go to **Users > FindMe accounts**.
(If you are using Cisco TMSPE you must set up the accounts via Cisco TMS instead.)
- b. Click **New**.
- c. Configure the following fields:

| | |
|--|--|
| Username | Username used by the FindMe user to log in to VCS to administer this account. |
| Display name | Full name of this user. |
| Phone number | E164 number to use when outdialing to a gateway. |
| FindMe ID | URI with Lync's domain that will register to Lync Server as though it were a Lync client. |
| Principal device address | Routable endpoint URI / E164 or H.323 ID to call when this FindMe is called. |
| Initial password and Confirm password | Password needed by the FindMe user to log in to VCS to administer this account. (Not configurable if VCS is configured with User authentication source as <i>Remote</i> .) |
| FindMe type | <i>Individual</i> |

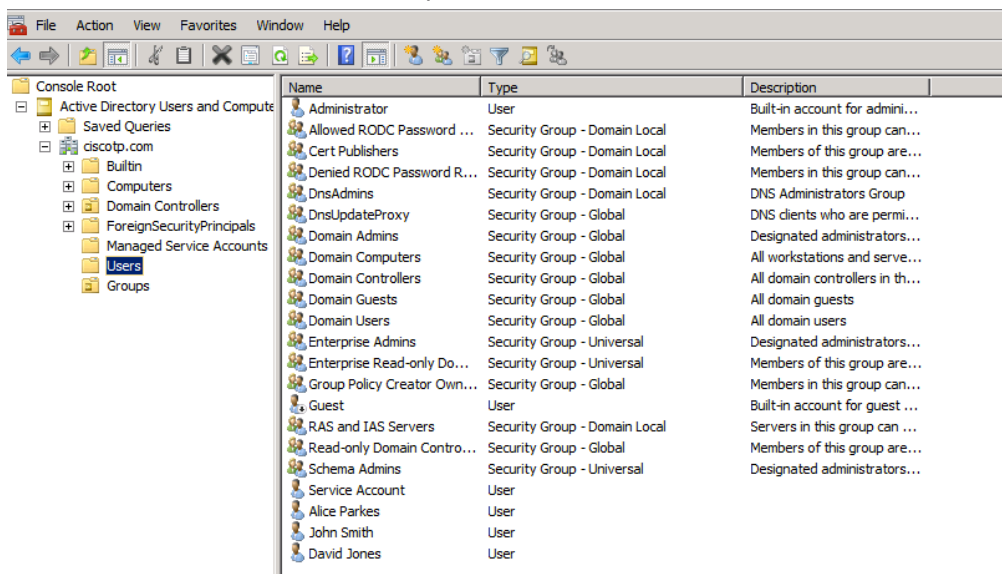
4. Ensure that the domain shared with the Lync is resolvable by the DNS server; this is usually best achieved by using the same DNS server that Lync Server uses. See ["Lync gateway" VCS: Configure DNS and local hostname \[p.28\]](#).

Configuring Lync Active Directory for FindMe users


Ensure that Active Directory user accounts exist for all FindMe accounts on the "Lync gateway" VCS(s) that will register to Lync Server (FindMe accounts that have the same domain as Lync).

On the PC running the Active Directory for Lync users:

1. Select **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
or **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Select the 'Users' folder under the required domain:



For each new user that needs to be created:

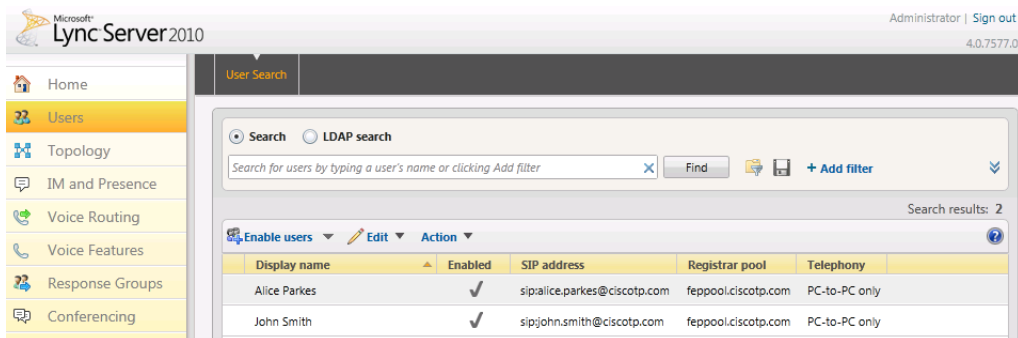
1. Click  **Create new user** in the current container or select **Action > New > User**.
2. Configure the following fields:

| | |
|------------------------|-----------------------|
| First name | The user's first name |
| Last name | The user's last name |
| User logon name | The user's logon name |

3. Click **Next**.
4. Configure the following fields:

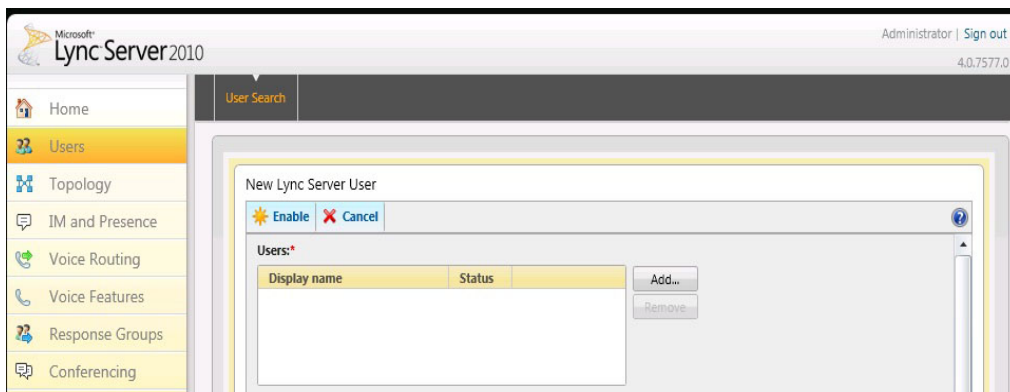
| | |
|-------------------------------|------------------------|
| Password | The user's password |
| Confirm password | Retype the password |
| Password never expires | Select this check box. |

5. Click **Next**.
6. Click **Finish**.
7. Enable the user for Lync:
 - a. Bring up the Lync Server Control Panel (either from the start menu select Lync Server Control Panel, or if there is a desktop icon double click it).
 - b. On Lync Server Control Panel go to the **Users** menu: you can see users already enabled for communication server.

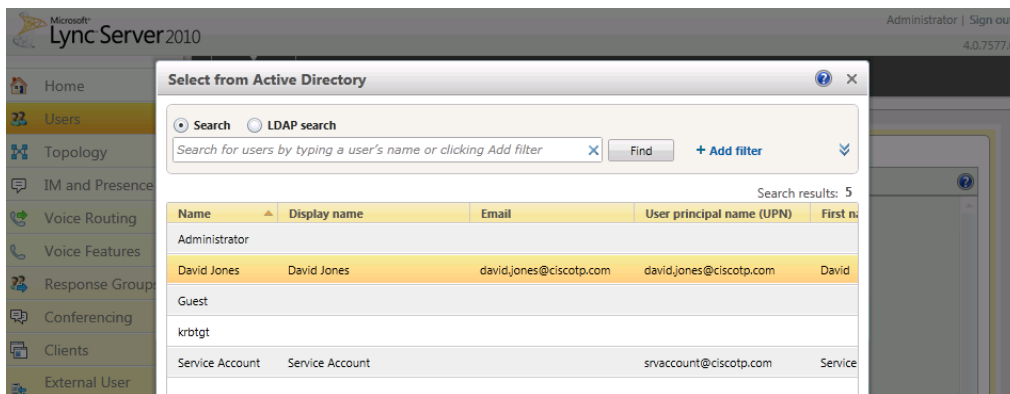


To add a new user:

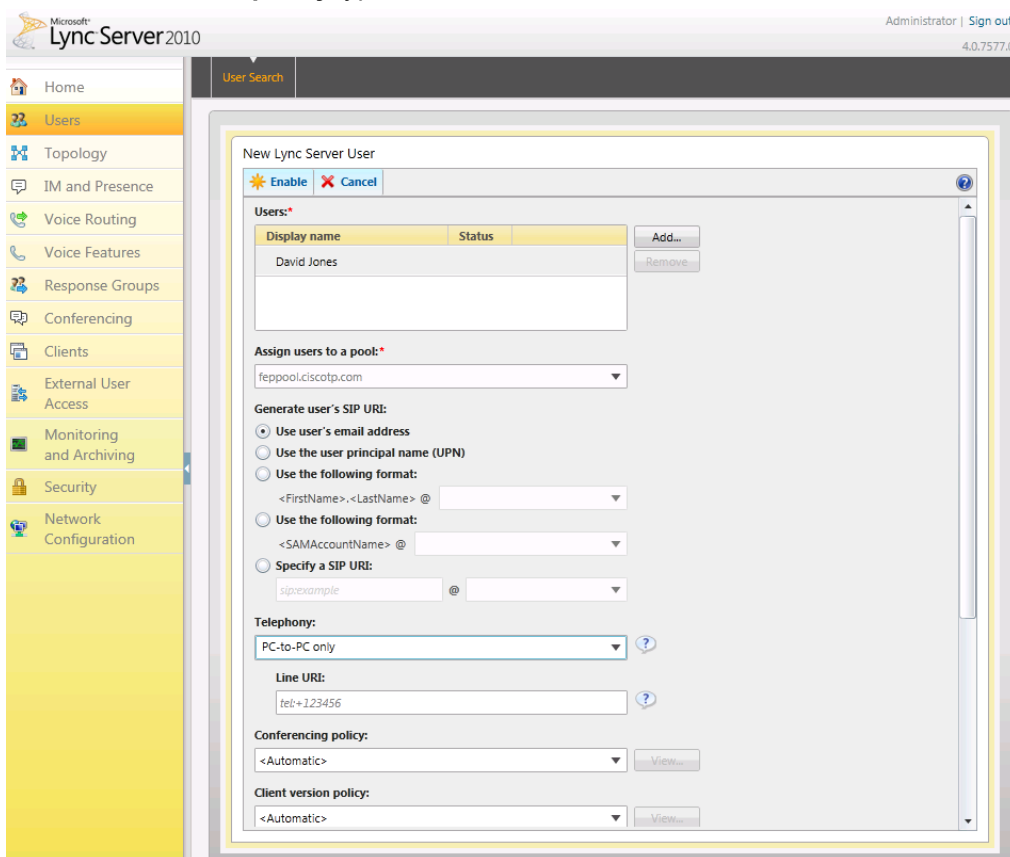
- a. Select **Enable users** and click **Add**.



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



- c. Select the communication server pool to assign to the user.
 d. Select your preferred method to **Generate user's SIP URI**.
 e. Select the user's **Telephony** type.



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

For example:

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

Log in to each Lync client

Lync Server will not provide presence for FindMe users to other Lync clients until the Lync client associated with a FindMe has been signed into using a Lync client registered to Lync Server.

For each FindMe user that has been created:

1. Log into a Lync client as that user.
2. Log out.
3. Repeat for all users.

Verify that the FindMe accounts are registered

After the FindMe accounts have been configured for at least 60 seconds:

1. On the "Lync gateway" VCS, go to **Status > Applications > Lync users**.
2. Verify the following for each FindMe user:
 - Registrations state is Registered
 - Presence state is Online (if **Default published status for registered endpoints** is set to *Online*, otherwise expect to see Offline)
 - Subscription state is Subscribed

If the states are not as expected, check that the FindMe and Lync (Active Directory) registered names are identical.

Testing the configuration

Test calls from Lync clients registered on Lync Server to endpoints registered on VCS Control. For example, call david.jones@ciscotp.com or alice.parkes@ciscotp.com from a Lync client registered on Lync Server.

Double-click on the buddy then click "Video->Start a Video Call" to make a video call.

1. Test that calls to Lync registered FindMe users from VCS registered endpoints fork to VCS registered endpoints listed in the FindMe entry and also to the Lync client for this user.
2. Test that calls to Lync registered FindMe users from Lync clients fork to the Lync client and also to VCS registered endpoints listed in the FindMe entry for this user.

Enabling Lync clients to see the presence of endpoints registered on VCS Control

When using FindMe:

- The Presence Server must be enabled on the "Lync gateway" VCS (and disabled on the VCS Control).
- The "Lync gateway" VCS must be authoritative for the shared Lync/FindMe domain (ciscotp.com) and for the domains of all devices that are referenced in the FindMe users that register to Lync, as FindMe will only aggregate presence data for devices where their presence state is known on the same VCS as the FindMe resides.
- When the B2BUA is configured to register FindMe IDs to Lync Server, "gray" (not available), "green" (available) and "In-call" states are provided to Lync Server.

VCS Control configuration

Disable the Presence Server on the VCS Control

To disable the Presence Server on the VCS Control:

1. Go to **Applications > Presence**.

- Configure the following fields:

| | |
|--|---|
| SIP SIMPLE Presence User Agent | <i>On</i> (if VCS Control is to generate presence information for registered endpoints) |
| Default published status for registered endpoints | <i>Online</i> |
| SIP SIMPLE Presence Server | <i>Off</i> (the "Lync gateway" VCS will be the Presence Server) |

Presence You are here: [Applications](#) > Presence

PUA

SIP SIMPLE Presence User Agent On ⓘ

Default published status for registered endpoints Online ⓘ

Presence Server

SIP SIMPLE Presence Server Off ⓘ

Configure a search rule to route messages to the Presence Server on the "Lync gateway" VCS

The PUA on the VCS Control needs to be able to route PUBLISH messages from its domain endpoints to the Presence Server running on the "Lync gateway" VCS. To do this, a search rule is required:

- Go to **Configuration > Dial plan > Search rules**.
- Click **New**.
- Configure the following fields:

| | |
|----------------------------|---|
| Rule name | An appropriate name, for example "Route publish messages to Lync gateway" |
| Priority | Leave as default, for example 100. Note that this should be a lower priority (a larger number) than the priority configured for the LocalZoneMatch. |
| Source | <i>Any</i> |
| Mode | <i>Alias pattern match</i> |
| Pattern type | <i>Regex</i> |
| Pattern string | Configure the pattern to match the domain supported in the video network, for example: .*@vc\.ciscotp\.com |
| Pattern behavior | <i>Leave</i> |
| On successful match | <i>Continue</i> |
| Target | Select the Lync gateway zone, for example "To Lync gateway" |

- Click **Create search rule**.
Note that this search rule does not conflict with Local Zone searches (which may contain the same pattern match string) because the PUA is not treated as a Local Zone registered device.
- Create additional search rules for any other SIP domains (such as mcu.ciscotp.com) supported by this

VCS (i.e. for endpoints that are registered to the VCS Control) otherwise Presence will not work (messages will not get forwarded).

“Lync gateway” VCS configuration

Enable the Presence Server on the “Lync gateway” VCS

On the “Lync gateway” VCS:

1. Go to **Applications > Presence**.
2. Configure the following fields:

| | |
|--|---------------|
| SIP SIMPLE Presence User Agent | <i>Off</i> |
| Default published status for registered endpoints | <i>Online</i> |
| SIP SIMPLE Presence Server | <i>On</i> |

Presence You are here: [Applications](#) > Presence

PUA

SIP SIMPLE Presence User Agent Off ⓘ

Default published status for registered endpoints Online ⓘ

Presence Server

SIP SIMPLE Presence Server On ⓘ

Save

Ensure the Presence Server can receive presence messages

Ensure that the zone to the video network has an authentication policy of *Treat as authenticated* (the Presence Server accepts PUBLISH messages only if they have been authenticated):

1. Go to **Configuration > Zones > Zones**.
2. Select the “To Video network” zone.
3. Ensure that **Authentication policy** is set to *Treat as authenticated*.

Authentication

Authentication policy **Treat as authenticated** ⓘ

SIP authentication trust mode Off ⓘ

Notes:

- The “Lync gateway” VCS that connects to the Lync Server must be the presence server for any SIP domains that Lync Server might want to look at for presence; this limits the number of VCSs that Lync server’s presence requests will travel through.

- Presence requests use up SIP resources and with Lync typically having thousands of Lync clients connected that may be requesting presence, it is best to limit the range of where the presence requests can go, especially not letting them reach VCSs that may already be heavily used for taking calls.

Lync client configuration

Set up **Sign-in address** as required. This is the SIP URI of the Lync user; if this user also has video endpoints on the video network, this URI will be the same URI as that configured as the B2BUA registered FindMe user ID (set up later), for example david.jones@ciscotp.com:

Log in to the Lync client

Lync Server will not provide presence for FindMe users to other Lync clients until the Lync client associated with a FindMe has been signed into using a Lync client registered to Lync Server.

For each FindMe user that has been created and not already been signed into:

1. Sign into a Lync client as that user.
2. Sign out.
3. Repeat for all users.

Appendix 1: Federation

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

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

Partitioned Intra-Domain Federation

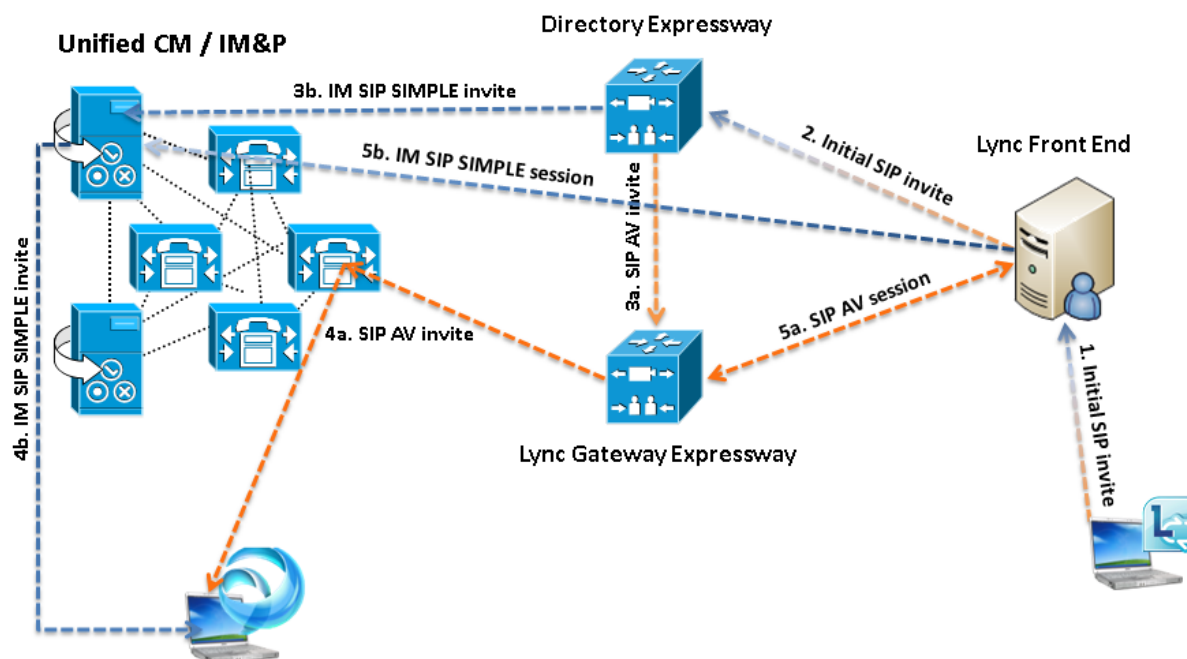
Partitioned Intra-Domain Federation is the sharing of enterprise Instant Messaging (IM), Presence, audio, and video between Unified Communications systems within a single presence / SIP domain. This model is used here as a migration tool from Microsoft Lync to Cisco infrastructure and Cisco Jabber.

Partitioned Inter-Domain Federation

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

Solution overview

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

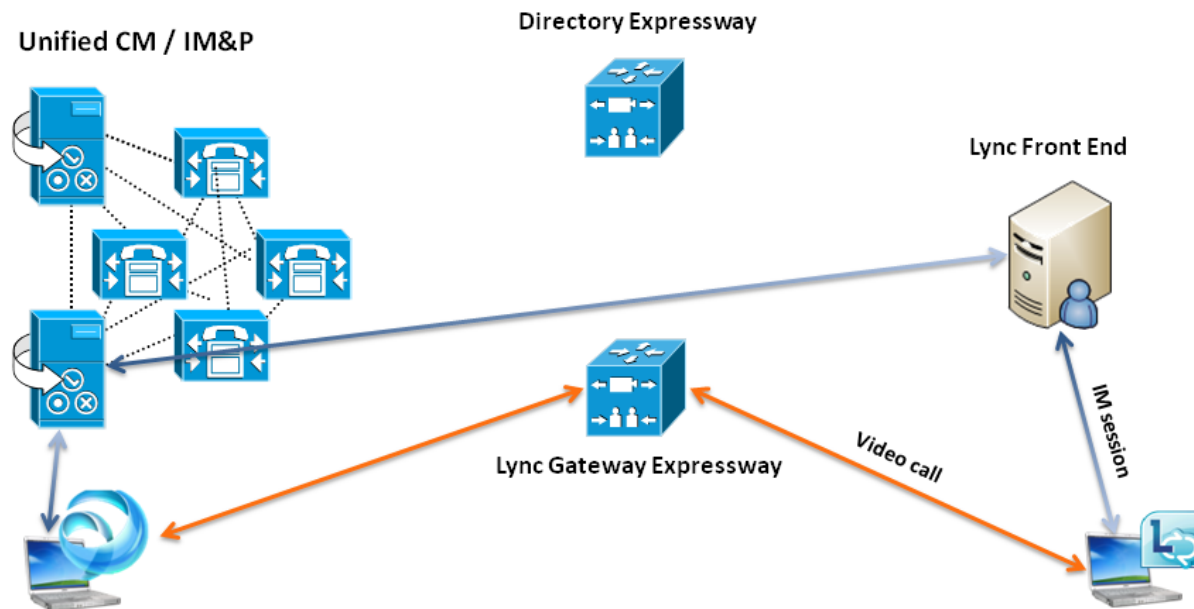


The IM&P and audio / video (AV) signaling flows are as follows:

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

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

The resulting IM and media paths are shown below:



Note that:

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

Configuring the directory VCS

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

The directory VCS configuration that is required is summarized below:

1. Ensure that the VCS has non-traversal call licenses installed (**Maintenance > Option keys**).
We recommend a minimum of 10 non-traversal call licenses.

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

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

Example CPL

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

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

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

Modifying the Lync static route configuration

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

Appendix 2: Troubleshooting

Troubleshooting checklist

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

- Ensure that video endpoints and infrastructure devices are running up-to-date software. Doing so lowers the chances for interoperability issues between the video environment and Lync.
- Ensure that all "Lync gateway" VCSs can successfully look up all Lync Server A-record FQDNs in DNS (this includes both Director and FEPs). You can use **Maintenance > Tools > Network utilities > DNS lookup** on the VCS.
- Ensure that all Lync servers can successfully look up all "Lync gateway" VCS 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 VCS (on the **Status > Applications > Lync B2BUA** page, Status = Alive is the desired state for both), and, if using FindMe, that the B2BUA has successfully registered FindMe accounts to Lync (on the **Status > Applications > Lync users** page **Registration state** = *Registered* and **Subscription state** = *Subscribed* are the desired states).

Problems connecting VCS Control local calls

Look at search history to check the applied transforms

1. In VCS, go to **Status > Search history**.
Search history entries report on any searches initiated from a SETUP/ARQ /LRQ in H323 and from an INVITE/OPTIONS in SIP. The summary shows the source and destination call aliases, and whether the destination alias was found.
2. Select the relevant search attempt. The search history for that search attempt shows:
 - the incoming call's details
 - any transforms applied by pre-search transforms or CPL or FindMe
 - in priority order, zones which matched the required (transformed) destination, reporting on:
 - any transforms the zone may apply
 - found or not found status
 - if not found, the error code as seen in the zone's search response
 repeated until a zone is found that can accept the call, or all matches have been attempted
(The search may be 'not found' due to lack of bandwidth or because the search from the zone resulted in an H.323 rejection reason or a non 2xx response to a SIP request.)
3. If the search indicates:
 - Found: False
 - Reason: 480 Temporarily Not Available
 this could be because the VCS's zone links are not correctly set up. From the command line execute:
xcommand DefaultLinksAdd
 to set up the links for the default zones. Also check that the links for other zones that have been created.

Note that each H.323 call will have 2 entries in the search history:

- An ARQ to see if the endpoint can be found.
- The SETUP to actually route the call.

The ARQ search does not worry about links or link bandwidth, and so if links do not exist or link bandwidth is insufficient it may still pass, even though the SETUP search will subsequently fail.

Each SIP call will usually only have a single search history entry for the SIP INVITE.

Look at 'Call History' to check how the call progressed

1. Go to **Status > Calls > History**.
The summary shows the source and destination call aliases, the call duration and whether the call is a SIP, H.323 or SIP< -->H.323 interworking call.
2. Select the relevant call attempt.
The entry shows the incoming and outgoing call leg details, the call's status and the zones that the VCS Control used to route the call.

Check for errors in the Event Log

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

Tracing calls

Tracing calls at SIP / H.323 level

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

Presence not observed as expected

Presence Server status

- Go to **Status > Applications > Presence > Publishers** to check who is providing presence information to the VCS Presence Server.
- Go to **Status > Applications > Presence > Presentities** to check whose presence is being watched for (on domains handled by VCS Presence Server).
- Go to **Status > Applications > Presence > Subscribers** to check who is watching for presence (of one or more entities in domains handled by VCS Presence Server):

No presence being observed

Check that there is no transform that may be inadvertently corrupting the presence Publication, Subscription or Notify, for example that there is no transform modifying the presence URI. (Notifies are sent to the subscription contact ID, typically <name>@<IP address>:<IP port>;transport=xxx. Any transforms that modify this are likely to stop the presence Notify being routed appropriately.)

Lync client fails to update status information

If a Lync client is started before the Presence Server is enabled, the Lync client may need to be signed out and signed back in again before it will display the correct presence information.

Check for errors

Checking for presence problems should be carried out in the same way as checking for errors with calls: check the Event Log and the logging facilities mentioned in the 'Check for errors' section above.

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 VCS incoming IP port, rather than the B2BUA IP port that should be receiving the incoming SIP messages.
2. Reconfigure Lync Server to send calls to the B2BUA IP port.

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

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

Lync client initiated call fails to connect

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

Lync responds to INVITE with '488 Not acceptable here'

There can be two causes for this message:

From IP address

This is normally seen if the B2BUA forwards an INVITE from a standards-based video endpoint where the 'From' header in the SIP INVITE only contains the IP address of the endpoint, e.g. "From:

<sip:10.10.2.1>;tag=d29350afae33". This is usually caused by a misconfigured SIP URI in the endpoint. In future versions of B2BUA, the "From"-header will be manipulated if necessary to avoid this issue.

Encryption mismatch

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

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

Call connects but clears after about 30 seconds

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

VCS to Lync Server calls fail – DNS server

VCS 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.

VCS to Lync calls fail – Hardware Load Balancer

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

(Calls from Lync client – registered to the FEP – to VCS 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/VCS Expressway)

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

One way media: Lync client to VCS-registered endpoint

When using Microsoft Edge Server

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

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

When using a Hardware Load Balancer in front of Lync

VCS modifies the application part of INVITEs / OKs received from Lync clients to make them compatible with traditional SIP SDP messaging. VCS 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 VCS registered endpoint), check the search history and ensure that the call is seen coming from a Lync trusted host. Otherwise, the call may be coming from a FEP rather than the load balancer. See ["Lync gateway" VCS configuration \(part 2\) \[p.32\]](#) and configure Lync trusted hosts containing the FEP IP addresses.

Lync rejects VCS 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 VCS 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 VCS (Lync sees calls coming from the hardware load balancer rather than from the VCS).

Lync client stays in 'Connecting ...' state

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

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

In some Lync configurations, especially where Lync PSTN gateways are used, calls are only allowed if the calling party is authorized. Thus, the calling party's domain must be the Lync Server shared domain.

- For calls from endpoints that are not part of a FindMe, this means that the endpoints must register to the video network with a domain that is the same as the Lync domain.
- For calls from endpoints that are part of a FindMe, the endpoints can register with any domain so long as the FindMe ID has the same domain as the shared Lync domain and in the FindMe configuration **Caller ID** is set to *FindMe ID* (instead of *Incoming ID*).

Lync clients try to register with VCS Expressway

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

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

Lync clients use:

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

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

B2BUA problems

B2BUA users fail to register

If B2BUA registration fails to register FindMe users (Registration status = failed), check:

1. The FindMe name is correctly entered into Active Directory.
2. A Lync client can register as the FindMe name – you need to log in first from a Lync client before the B2BUA can properly control the Lync user.

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

Check that the VCS application has been added to the Lync trusted application pool and is configured to contact the VCS B2BUA via port 65072 . See [Trust a "Lync gateway" VCS \[p.30\]](#) for more information.

Lync problems

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

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

Problems with certificates

If a non-Lync application is used to create certificates to load onto VCS 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 [VCS Certificate Creation and Use Deployment Guide](#).

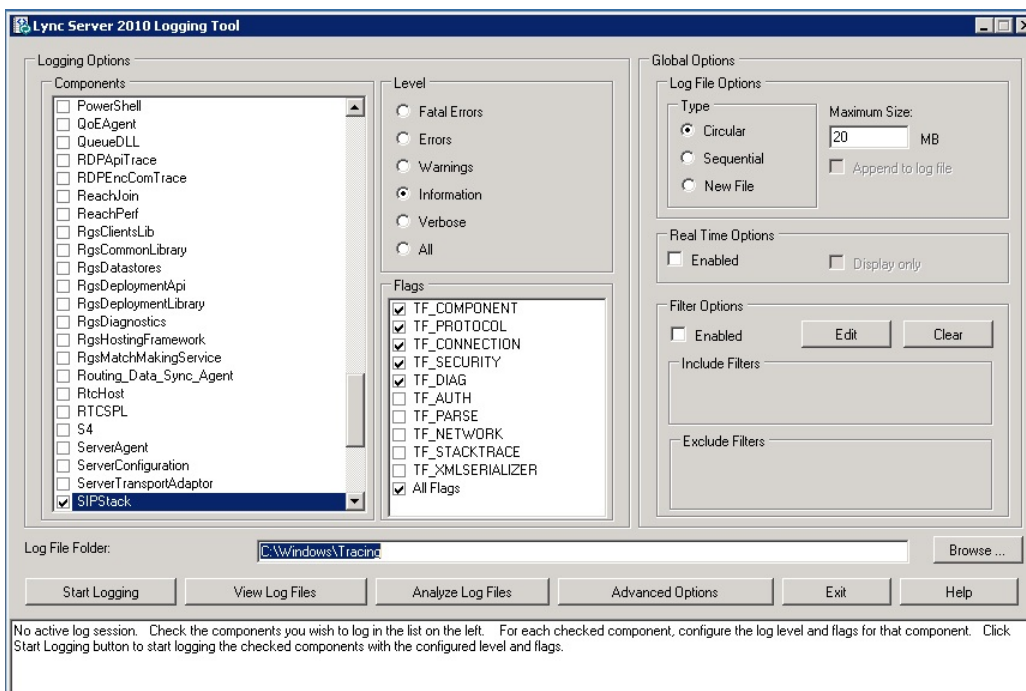
Appendix 3: Debugging on Lync

Use of Lync Server Logging Tool

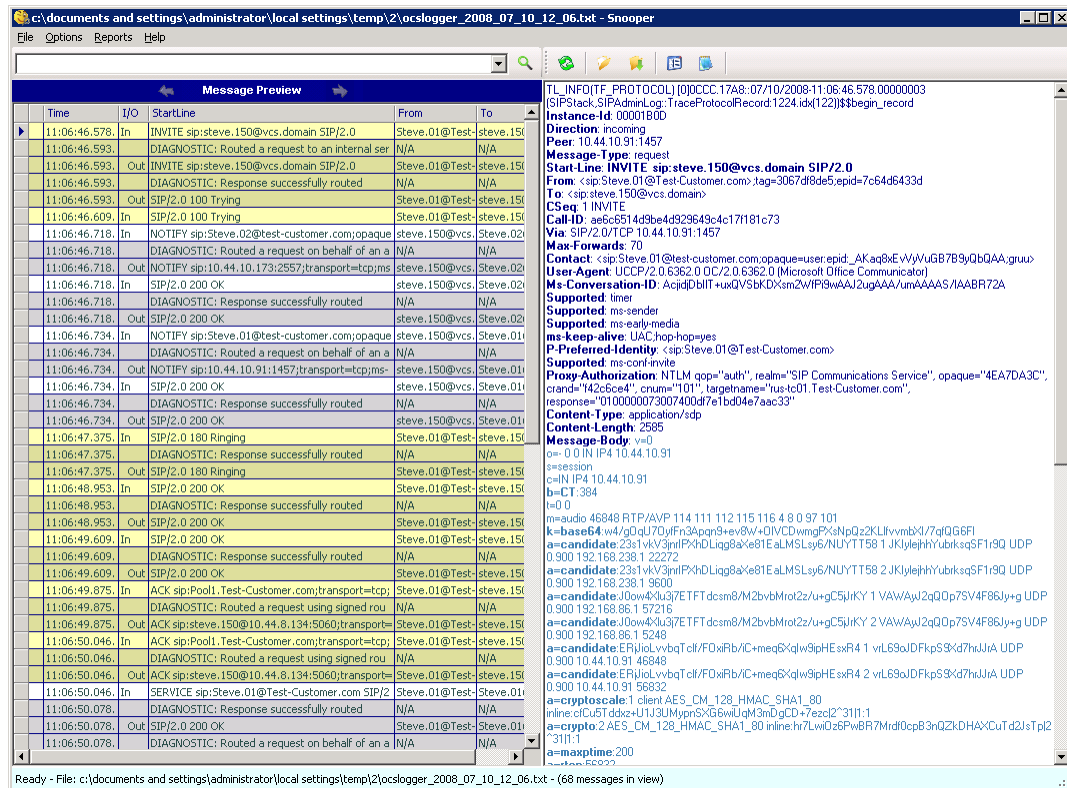
For debugging it is important to enable the logging on the appropriate Lync pool. If a Lync Director is in use, tracing here is a good starting point.

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

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



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



Enabling debug on Lync client

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

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

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

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

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

Appendix 4: Interoperating capabilities and limitations

Known interoperating capabilities

SIP and H.323 endpoints making basic calls

- SIP and H.323 endpoints can make calls via VCS Control to Lync clients registered to Lync Server.
- Lync clients registered to Lync can make calls to SIP and H.323 endpoints on VCS Control.

Upspeeding from a voice call to a video call

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

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

Maximum call resolution

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

Multiway generation of ad hoc conferences

Endpoints can join Lync clients into an ad hoc conference using the Multiway feature. When a Lync client is transferred into a Multiway conference, the client will connect using audio only. The Lync user will then manually have to enable video on the client after connecting to the conference.

Known interoperating limitations

Video codecs

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

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

Video codec selection

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

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

Changing the “pre-configured” SDP

The settings for the pre-configured SDP are configurable via the CLI only, using the **xConfiguration Zones Zone [1..1000] [Neighbor/DNS] Interworking SIP** commands.

MXP endpoints

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

Joining a Lync conference (AV MCU)

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

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

Neither VCS Control nor standards-based video endpoints support the Microsoft proprietary signaling. Note, however use of Multiway on endpoints can join Lync clients into an ad hoc conference (see *Cisco TelePresence Multiway Deployment Guide*).

Upspeeding from a voice call to a video call

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

Microsoft Mediation Server

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

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

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

1. Create a new neighbor zone and select *Custom* in the **Zone profile** field.
2. Configure the zone with the values shown in [Table 1: Custom neighbor zone attributes to work around Mediation Server limitation \[p.70\]](#)
3. Configure one or more search rules, with the correct priority, such that the appropriate subset of calls destined for the Mediation Server are routed through the new zone rather than the standard "To Microsoft Lync Server via B2BUA" zone.
4. You may also need to change the **On successful match** action from *Stop* to *Continue* on the search rule in the "To Microsoft Lync Server via B2BUA" zone. See [Set up a search rule to route calls to the Lync domain to Lync \[p.34\]](#).

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

| Setting | Lync Server zone configuration |
|----------------------------|--------------------------------|
| Monitor peer status | Yes |
| Call signaling routed mode | Auto |

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

| Setting | Lync Server zone configuration |
|---|--------------------------------|
| Automatically respond to H.323 searches | Off |
| Automatically respond to SIP searches | On |
| Send empty INVITE for interworked calls | Off |
| SIP poison mode | On |
| SIP encryption mode | Microsoft |
| SIP SDP attribute line limit mode | On |
| SIP SDP attribute line limit length | 130 |
| SIP multipart MIME strip mode | On |
| SIP UPDATE strip mode | On |
| Interworking SIP search strategy | Info |
| SIP UDP/BFCP filter mode | Off |
| SIP Duo Video filter mode | On |
| SIP record route address type | Hostname |
| SIP Proxy-Require header strip list | <blank> |

Cluster calls to endpoints not registered using FindMe

This can occur, for example, with MCU calls where MCU is in its own dedicated domain.

- Lync does not have a way of load balancing calls to a cluster of VCSs.
- Lync does not support DNS SRV, but it does allow the DNS record to be a Round-Robin record listing all VCSs in the “Lync gateway” cluster. Lync seems to continue to use just a single VCS until it loses connectivity to that VCS. At that time it will choose a different VCS from the Round-Robin DNS record.

Use of VCS clusters with Lync without B2BUA FindMe registration therefore provides resilience, not extra capacity / load balancing.

Lync client reports no audio device

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

Call forward from Lync to a VCS FindMe or endpoint results in a 'loop detected' call

If a call from VCS is made to a Lync client which has a forward to another VCS registered endpoint or a FindMe, then VCS sees this as a looped call.

FindMe Caller ID set to FindMe ID causes calls from Lync client to fail

If all of the following are true:

- FindMe Caller ID is set to *FindMe ID*
- a Lync client's URI is in the active location of a FindMe
- a call is made from that Lync client to a SIP destination

the call will fail because Lync does not expect the caller ID (From: header) to be modified.

If the call is interworked on the "Lync gateway" VCS, the call will work as required.

Best practice is that a Lync client should never be included as a FindMe device. Lync clients and video endpoints are related to one another using B2BUA registration of FindMe IDs where the FindMe URI is the same as the Lync client URI.

Appendix 5: Port reference

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

Between B2BUA and Lync

| Purpose | Protocol | B2BUA IP port | Lync IP port |
|--|----------|----------------|--|
| Signaling to Lync Server | TLS | 65072 | 5061 (Lync signaling destination port) |
| Signaling from Lync Server | TLS | 65072 | Lync ephemeral port |
| Presence to Lync Server | TLS | 10011 | 5061 (Lync signaling destination port) |
| Presence from Lync Server | TLS | 10011 | Lync ephemeral port |
| Media (the Lync B2BUA should be deployed on a separate "Lync Gateway" VCS and thus there should be no conflict with the standard traversal media port range) | UDP | 56000 to 57000 | Lync client media ports |

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

Between B2BUA and VCS (internal communications)

| Purpose | Protocol | B2BUA IP port | VCS IP port |
|--|----------|---------------|-----------------------|
| Internal communications with VCS application | TLS | 65070 | SIP TCP outbound port |

Between B2BUA and VCS Expressway hosting the TURN server

| Purpose | Protocol | B2BUA IP port | VCS Expressway 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 VCS Expressway.

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

External Lync client and Edge server

| Purpose | Protocol | Edge server | Lync client |
|--|----------|-------------|-------------|
| SIP/MTLS used between Lync Client and Edge server for signaling (including any ICE messaging to the Edge Server) | TCP | 5061 | 5061 |
| SIP/TLS | TCP | 443 | 443 |
| STUN | UDP | 3478 | 3478 |
| UDP Media | UDP | 50000-59999 | 1024-65535 |
| TCP Media | TCP | 50000-59999 | 1024-65535 |

External Lync client / Edge server and VCS Expressway

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

** The default TURN relay media port range of 24000 – 29999 applies to new installations of X8.1 or later. The previous default range of 60000 – 61799 still applies to earlier releases that have upgraded to X8.1.

Between B2BUA and transcoder

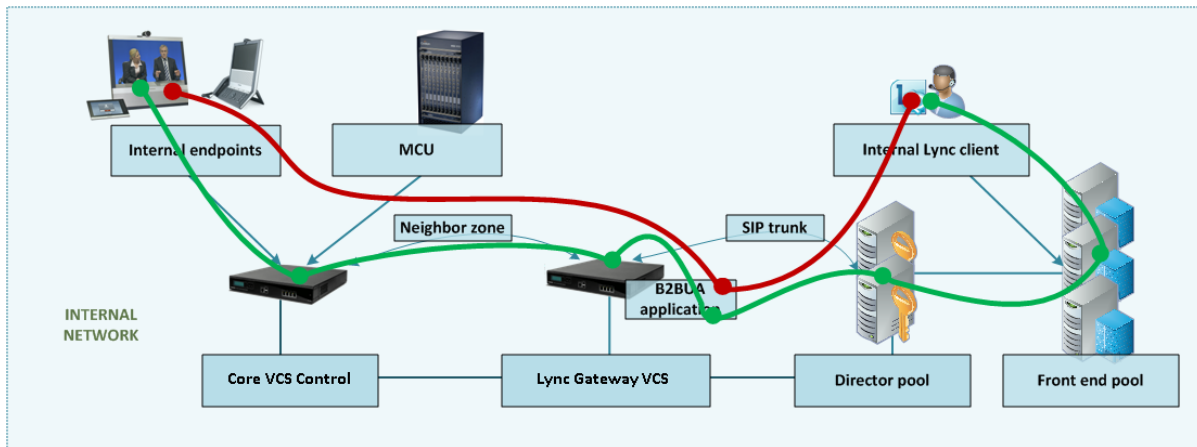
| Purpose | Protocol | B2BUA IP port | Transcoder |
|--|----------|---------------|------------|
| B2BUA communications with transcoder (Cisco AM GW) | TLS | 65080 | 5061 |

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

Lync client call to SIP video endpoint

For a call of this type:

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

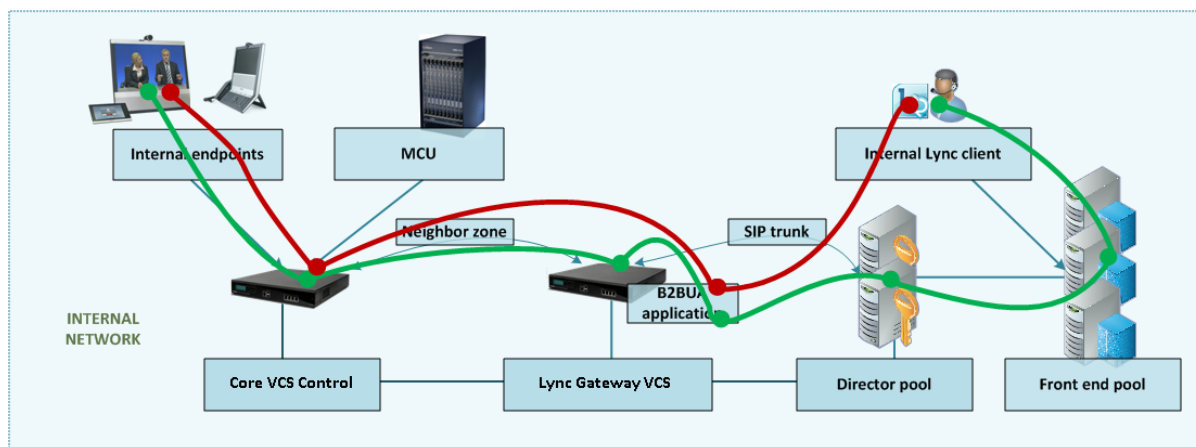


— Signaling
— Media

Lync client call to H.323 video endpoint

For a call of this type:

- Signaling flows through Lync, B2BUA, and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media from the internal video endpoint flows through the VCS Control and is then connected directly to the B2BUA.
- Calls made in the opposite direction, internal video endpoint to Lync client use the same signaling and media paths.
- Licenses:
 - 1 traversal call license on VCS Control
 - 1 non-traversal call license on “Lync gateway” VCS



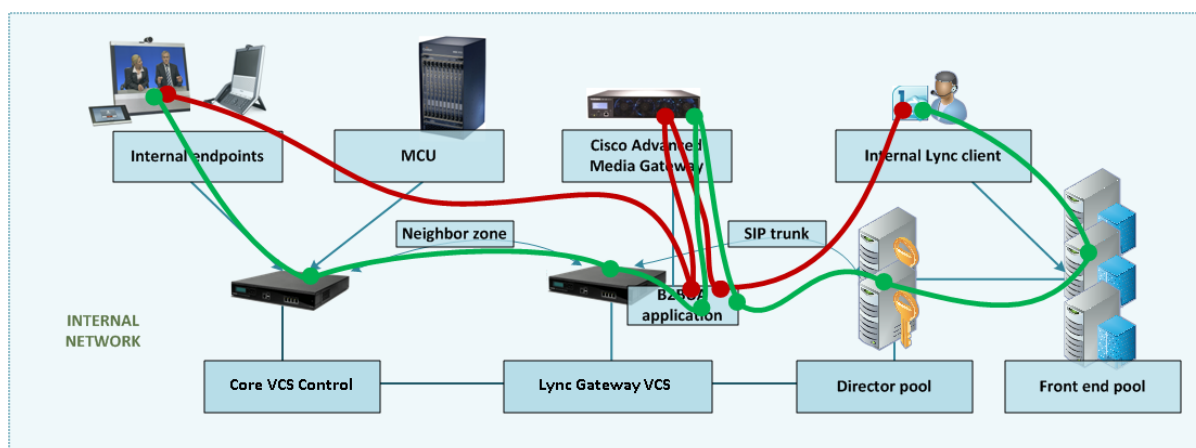
— Signaling

— Media

Lync client call to a SIP video endpoint via Cisco AM GW

For a call of this type:

- Signaling flows through Lync, B2BUA, Cisco AM GW and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media is connected directly between the internal video endpoint and the B2BUA (as the call is SIP to SIP), and then flows to the Cisco AM GW and back to the B2BUA.
- Calls made in the opposite direction, internal video endpoint to Lync client use the same signaling and media paths.
- Licenses:
 - 1 non-traversal call license on VCS Control
 - 1 non-traversal call license on “Lync gateway” VCS



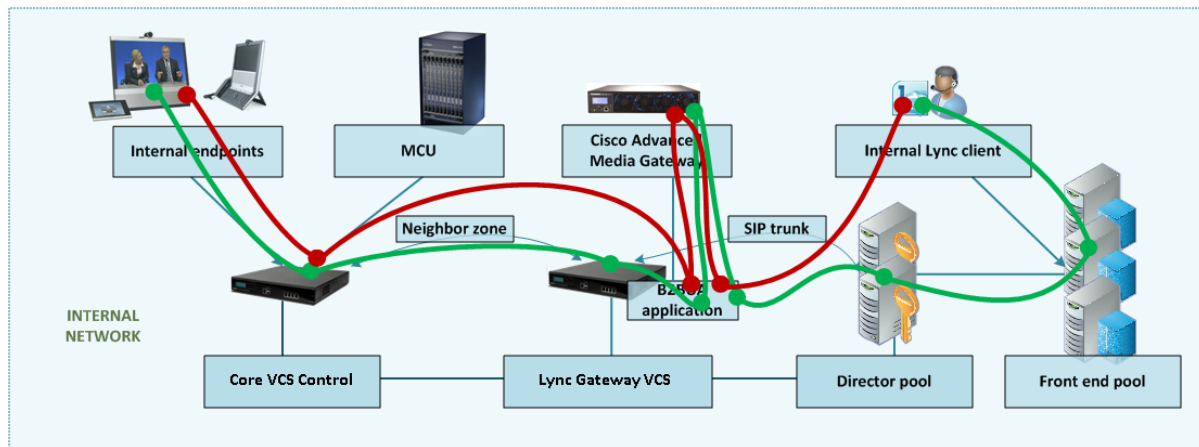
— Signaling

— Media

Lync client call to H.323 video endpoint via Cisco AM GW

For a call of this type:

- Signaling flows through Lync, B2BUA, Cisco AM GW and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media from the internal video endpoint flows through the VCS Control and is then connected directly to the B2BUA. It then flows to the Cisco AM GW and back to the B2BUA.
- Calls made in the opposite direction, internal video endpoint to Lync client use the same signaling and media paths.
- Licenses:
 - 1 traversal call license on VCS Control
 - 1 non-traversal call license on “Lync gateway” VCS

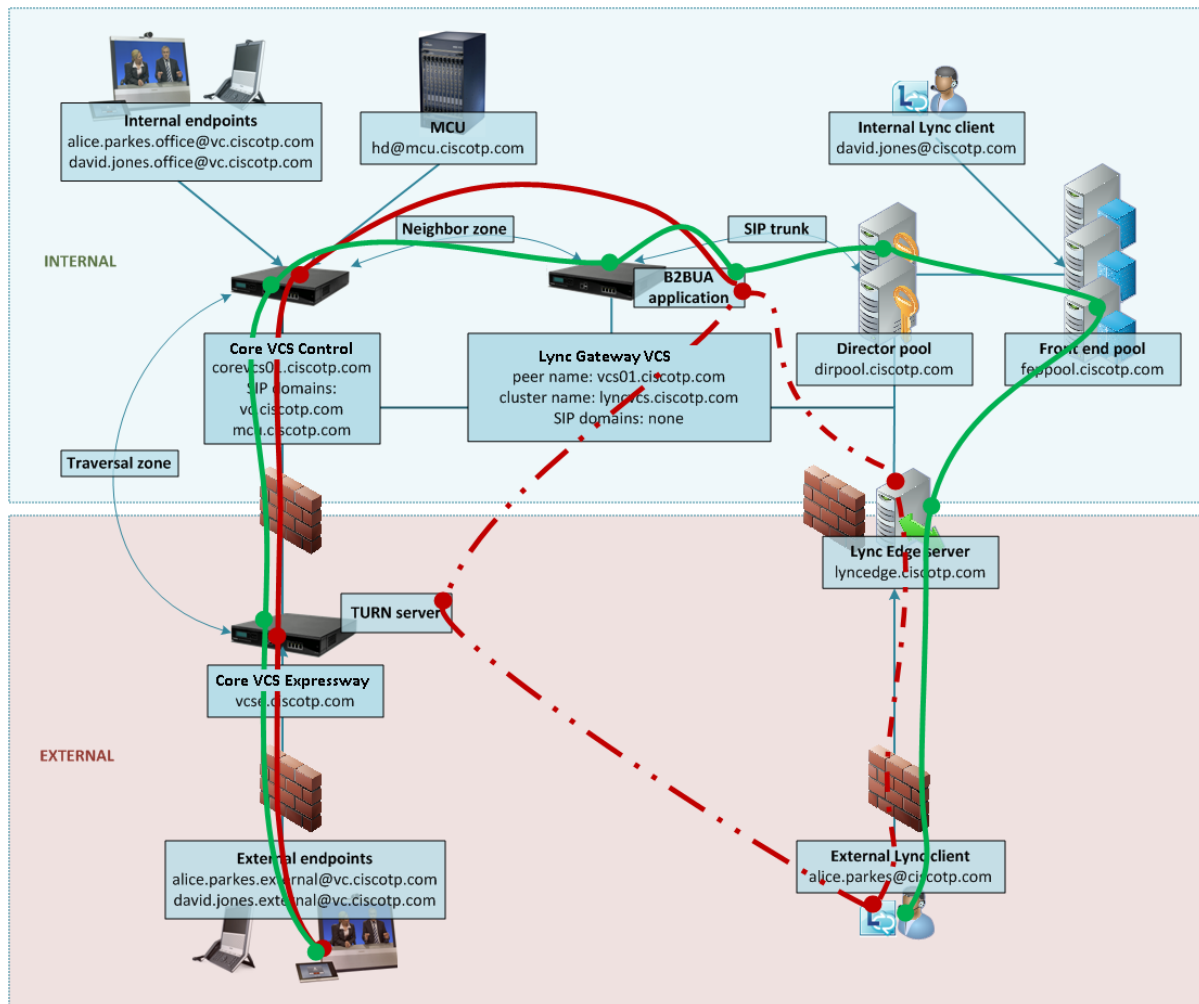


— Signaling
— Media

An external Lync client calls an external video endpoint

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

- Signaling flows through the Microsoft Edge Server, Lync, B2BUA, VCS Control and VCS Expressway.
- Media between the Lync client and the B2BUA flows either through the Microsoft Edge server or through the VCS Expressway TURN server – ICE searching is used to determine the ‘best’ path.
- Media between the external video endpoint and the B2BUA flows through the VCS Control / VCS Expressway traversal link.
- Calls made in the opposite direction, external video endpoint to external Lync client use the same signaling and media paths.
- Licenses:
 - 1 traversal call license and up to 18 TURN licenses on the VCS Expressway
 - 1 traversal call license on the VCS Control
 - 1 non-traversal call license on the “Lync gateway” VCS

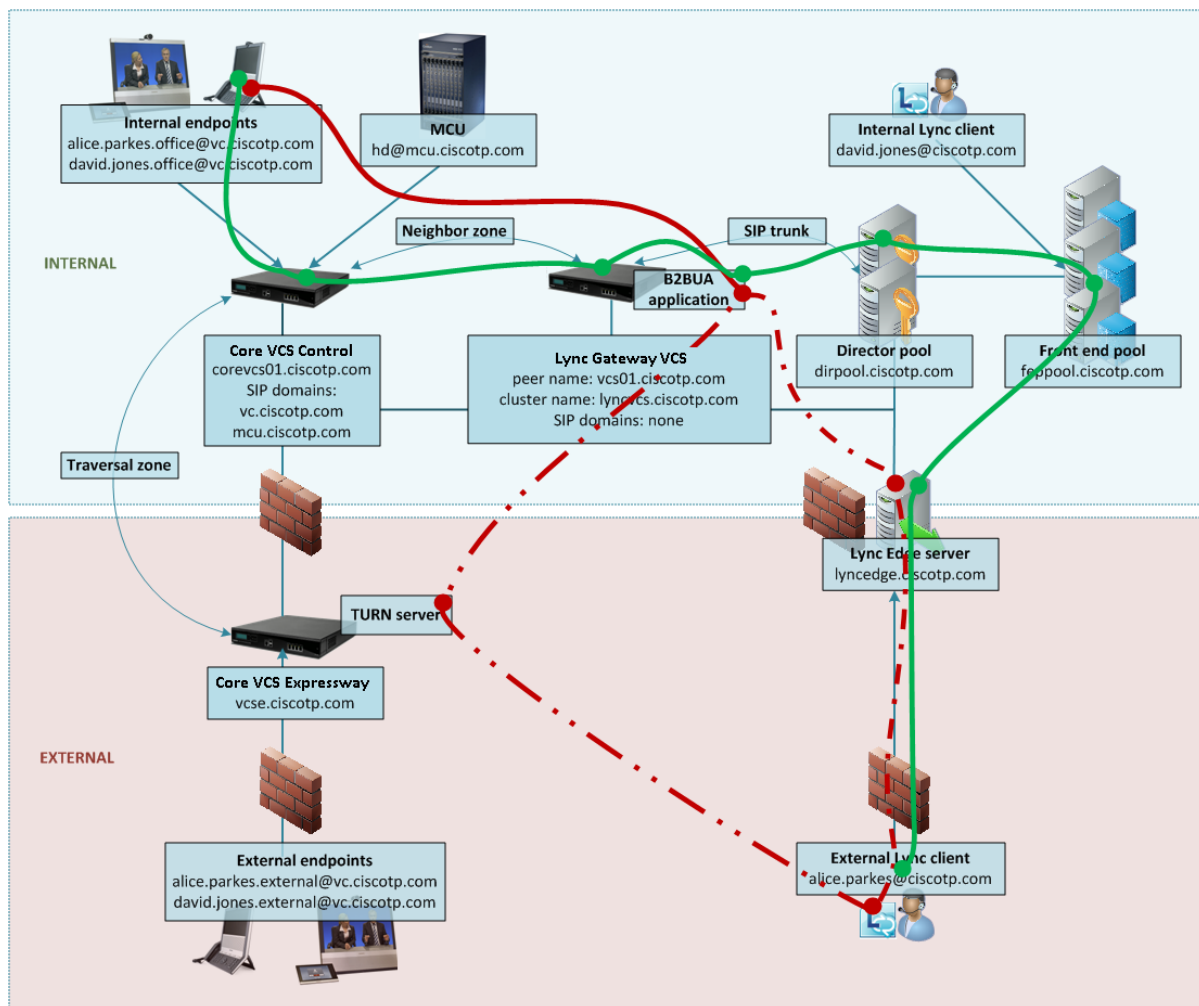


— Signaling
— Media

An external Lync client calls an internal SIP video endpoint

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

- Signaling flows through the Microsoft Edge Server, Lync, B2BUA, and VCS Control.
- Media between the Lync client and the B2BUA flows either through the Microsoft Edge server or through the VCS Expressway TURN server – ICE searching is used to determine the ‘best’ path.
- Media is connected directly between the internal video endpoint and the B2BUA (as the call is SIP to SIP).
- Calls made in the opposite direction, internal video endpoint to external Lync client will use the same signaling and media paths.
- Licenses:
 - 1 non-traversal call license on the VCS Control, as it is a SIP endpoint (an H.323 endpoint would use 1 traversal call license on the VCS Control)
 - 1 non-traversal call license on the “Lync gateway” VCS



— Signaling

— Media

Appendix 7: Additional information

B2BUA registration on “Lync gateway” VCSs

The B2BUA FindMe registration function allows personal video endpoints to appear in a similar manner to an endpoint registered directly to Lync Server with the same credentials as an existing Lync user, but still maintain the benefits of having the endpoint register to the VCS which is designed to support video calling.

The B2BUA registration function also means that the user credentials are no longer needed on each individual video endpoint. This is possible because the VCS B2BUA is configured as a trusted host to Lync Server. This simplifies the long term endpoint management since passwords do not need to be regularly updated on the video endpoints.

What does “Register FindMe users as clients on Lync” do?

When enabled, FindMe users that are in the shared domain with Lync are registered to Lync Server so that they appear like Lync clients.

This means that if a Lync client registers to Lync Server, and a FindMe user is registered as that same user to Lync Server, when the user is called by another Lync client, the call will be forked to both the registered Lync client and also to the VCS's FindMe. This means that Lync clients and all video endpoints configured as primary devices in the FindMe will ring when called at the Lync client address.

Without registering the shared domain FindMe user, Lync Server will not fork the call to VCS, but:

- if a Lync client is registered with the called address then just that Lync client will ring.
- if there is no Lync client registered but there is a static domain route to the VCS for that domain the call will be routed to VCS to handle.
- if there is no Lync client registered and there is no static domain route for this call then the call will just fail.

Lync Server only allows FindMe users to register if the FindMe ID being registered is a valid user in the Lync Active Directory (in the same way that Lync clients can only register if they have a valid account enabled in the Lync AD).

Registering FindMe users also allows the presence of these users to be provided to Lync Server and for ‘in-call’ as well as ‘available’ and ‘off-line’ status to be provided. Endpoint devices and FindMe entries that are not registered to Lync Server can only communicate ‘available’ and ‘off-line’ status to Lync Server. The “Lync gateway” VCS (or VCSs) must host the presence server for the domain shared with Lync (ciscotp.com) in order for presence to be provided to Lync Server.

The “Lync gateway” VCS must also host the presence server for the domain of the video network (vc.ciscotp.com). This is because presence of a FindMe entry can only be provided if the presence status of the device(s) in the active location of the FindMe entry are hosted on the “Lync gateway” VCS. If FindMe entries contain multiple devices in the active location, VCS will aggregate the presence of those devices whose presence is hosted on the “Lync gateway” VCS and present the appropriate overall presence status.

Use of FindMe also allows any endpoint that is referred to in the FindMe to take on the caller ID of that FindMe entry. This means that whichever video endpoint makes the call, the receiving Lync client and video endpoints will see the call as having come from the FindMe ID. This is especially useful when the called party wants to return the call; the return call calls the FindMe ID resulting in all endpoints relating to this FindMe and any Lync clients registered with this ID all ringing simultaneously – rather than the return call being addressed directly to the single endpoint that made the call.

Configuring domains

It is best practice to keep the video endpoints in their own domain, and just have the FindMe users on the “Lync gateway” VCS with the same domain as Lync Server. This avoids any confusion as to what functionality will be received for each entity. When a call arrives for the FindMe user, FindMe will forward calls appropriately to the defined endpoints, whichever domain they are in.

For example, when `alice.parkes@ciscotp.com` is called, the call will fork to the Lync client with the same name, and also to `alice.parkes.office@vc.ciscotp.com` and `alice.parkes.external@ciscotp.com` (assuming that these two devices are listed as primary devices in Alice Parkes’ FindMe.)

We strongly recommend that the user is created on the Lync Server first and signed in to at least once from a Lync client. 5 to 10 minutes later the FindMe account can be created on the “Lync gateway” VCS when the user is fully available on Lync Server.

B2BUA and Cisco AM GW integration

For full instructions about how to configure the Microsoft Lync B2BUA with a Cisco TelePresence Advanced Media Gateway (Cisco AM GW), see *Microsoft Lync 2010, VCS and Cisco AM GW Deployment Guide*.

Previous versions of that document are also available for earlier, non-B2BUA VCS and Cisco AM GW deployments.

TEL URI handling for VCS to Lync calls

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

VCS Control can use transforms to appropriately format the telephone numbers. These transforms can either be implemented globally using [Configuration > Dial plan > Transforms](#) or just for the Lync neighbor zone or B2BUA neighbor zone by configuring the transform in the appropriate search rules.

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

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

Document revision history

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

| Date | Description |
|---------------|--|
| December 2014 | Updated for X8.5. |
| July 2014 | Reissued X8.2 document to address CSCup55116. |
| June 2014 | Reissued X8.2 document to include Federation information. |
| June 2014 | Republished for X8.2. |
| December 2013 | Updated for VCS X8.1 and Lync 2013. Modified the guide to first describe static route-based deployments, and to place FindMe-based deployment configuration into a separate section. |
| April 2013 | Removed Appendix 12 Federation. |
| December 2012 | Revised B2BUA and AM GW integration appendix to refer to external document. |
| August 2012 | Updated for VCS X7.2. |
| June 2012 | Updated for VCS X7.1. |
| November 2011 | Updated for VCS X7.0, OCS 2007 R2 and Lync 2010. |
| May 2011 | Updated for VCS X6.1 and Lync 2010. |
| November 2010 | Updated for VCS X5.2. |
| December 2009 | Updated for VCS X5. |
| August 2009 | Updated for VCS X3 and X4, OCS 2007 R1 and R2. |
| October 2008 | Initial release: VCS X3.0, OCS 2007v3.0. |

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

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

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

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

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

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

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

© 2014 Cisco Systems, Inc. All rights reserved.