



Microsoft Lync 2010 and Cisco VCS Deployment Guide

Cisco VCS X7.2
Microsoft Lync 2010

D14269.10

April 2013

Contents

Introduction	6
Objectives and intended audience	6
Deployment scenario.....	6
Clustered “Lync Gateway” VCS Control.....	8
Why add a “Lync Gateway” VCS Control?	8
“Lync gateway” and multiple Lync domains	9
Multiple “Lync gateway” per Lync domain.....	9
MCUs for ad hoc conferences from Lync.....	9
Small test/demo networks	10
Scaling up from a small test/demo network	10
Features and capabilities.....	10
Summary of configuration process.....	11
Different structures for Lync	11
Prerequisites prior to configuring Cisco VCS and Lync to interoperate	15
Benefits of using the B2BUA over legacy OCS Relay	15
 Video network: Check that calls between endpoints registered on VCS Controls operate as expected.....	 17
Video network VCS Control configuration summary	17
Ensure that the SIP domain of video network endpoints is configured in the VCS Control(s) in the video network	17
Lync configuration	17
Registering video endpoints to the video network.....	17
Video endpoint configuration.....	17
Confirming registrations	18
Testing the configuration	18
 Check that calls between Lync clients registered on Lync Server operate as expected 	 19
Cisco VCS Control configuration	19
 Enabling users for Lync.....	19
Registering Lync clients to the Lync Server	21
Lync client configuration.....	21
Testing the configuration	23
 Enabling endpoints registered on the video network to call Lync clients registered on Lync	 24
Video network: Cisco VCS Control configuration.....	24
Video network: Set up a neighbor zone to the “Lync gateway” VCS (cluster)	24
Video network: Set up a search rule to route calls to the Lync domain to the “Lync gateway” VCS (cluster).....	25
Video network: Set up search rules to route calls to any domains supported on Lync (but not in the video network) to the “Lync gateway” VCS (cluster)	26
“Lync gateway” VCS Control configuration (part 1).....	27
“Lync gateway”: Generate and load private key, CA certificate, and server certificate onto “Lync gateway” VCS Control (not needed if using a TCP connection)	27

“Lync gateway”: Set up the SIP domain of the “Lync gateway” VCS	28
“Lync gateway”: Configure DNS and local hostname	28
“Lync gateway”: Ensure that cluster name is configured	29
“Lync gateway”: Configure an NTP server	29
“Lync gateway”: Switch on TLS in SIP configuration	29
Lync Server configuration	31
Trust a “Lync Gateway” VCS (cluster)	31
Configure Lync Server media encryption capabilities	33
“Lync gateway” VCS Control configuration (part 2)	35
Configure the B2BUA on the “Lync gateway” VCS	35
Configure the B2BUA trusted hosts on the “Lync gateway” VCS	37
Set up a search rule to route calls to the shared Lync domain to Lync (via the B2BUA)	38
Set up a search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync (via the B2BUA)	39
Testing the configuration	40
Enabling Lync clients registered on Lync Server to call endpoints registered on the video network	41
“Lync gateway” VCS Control configuration	41
Configure the “Lync gateway” VCS with a neighbor zone that contains the video network	41
Set up search rules to route calls with video network domains to the video network	42
Lync Active Directory configuration for FindMe users	43
“Lync gateway” VCS FindMe configuration	46
Testing the configuration	48
Enabling Lync clients to see the presence status of endpoints registered on VCS Control	49
Cisco VCS configuration	49
Log in to the Lync client	50
Testing the configuration	50
Optional: MCUs	52
Configuration of Cisco VCS and Cisco MCUs	52
Adding a directly callable MCU	52
Adding an MCU using just the Autoattendant	52
Configure static routes to route MCU calls to the “Lync gateway” VCS	52
Enabling Microsoft Edge Server and VCS TURN capabilities	54
Appendix 1 – Troubleshooting	55
Troubleshooting checklist for X7.x	55
Problems connecting Cisco VCS Control local calls	55
Check for errors	56
Tracing calls	56
Presence not observed as expected	56
Video endpoint reports that it does not support the Lync client SDP	57
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	57
Lync client initiated call fails to connect	57
Lync responds to INVITE with ‘488 Not acceptable here’	57
Call connects but clears after about 30 seconds	58
Media problems in calls involving external Lync clients connecting via an Edge server	58

One way media: Lync client to VCS-registered endpoint.....	59
Lync rejects VCS zone alive OPTIONS checks with '401 Unauthorized' and INFO messages with '400 Missing Correct Via Header'	60
Lync client stays in 'Connecting ...' state	60
Call to PSTN (via Lync PSTN gateway) or other devices requiring caller to be authorized fails with 404 not found.....	60
Lync clients try to register with VCS Expressway	60
B2BUA problems	61
B2BUA users fail to register	61
Lync problems	61
Problems with certificates.....	61
Appendix 2 – Debugging on Lync	62
Use of Lync Logging tool	62
Appendix 3 – Enabling debug on Lync client.....	64
Appendix 4 – Known interoperating capabilities	65
SIP and H.323 endpoints making basic calls	65
Upspeeding from a voice call to a video call	65
Multiway generation of ad hoc conferences	65
Lync client accessing Lync server through Microsoft Edge Server	65
Appendix 5 – Known interoperating limitations	66
Video codecs	66
Video codec selection	66
Changing the “pre-configured” SDP	66
Joining a Lync conference (AV MCU)	66
Upspeeding from a voice call to a video call	66
Microsoft Mediation Server	66
Cluster calls to endpoints not registered using FindMe	67
Lync client reports no audio device	67
Microsoft Server	67
Call forward from Lync to a VCS FindMe or endpoint results in a 'loop detected' call	67
FindMe Caller ID set to FindMe ID causes calls from Lync client to fail	67
Appendix 6 – B2BUA registration on “Lync gateway” VCSs	68
What does “Register FindMe users as clients on Lync” do?	68
Registered users with a cluster of Cisco VCSs	69
Configuring domains.....	69
Appendix 7 – B2BUA and AM GW integration.....	70
Appendix 8 – TEL URI handling for Cisco VCS to Lync calls.....	71
Appendix 9 – Upgrading from non-B2BUA mode to B2BUA mode	72
Appendix 10 – IP port numbers.....	73
IP port numbers used between B2BUA and Lync	73
IP port numbers used between B2BUA and VCS Expressway hosting the TURN server.....	73
IP port numbers used with external Lync client.....	73
Appendix 11 – Media paths and license usage for calls through B2BUA	74

Lync client call to SIP video endpoint.....	74
Lync client call to H.323 video endpoint.....	75
Lync client call to a SIP video endpoint via AM gateway	76
Lync client call to H.323 video endpoint via AM gateway	77
An external Lync client calls an external video endpoint.....	78
An external Lync client calls an internal SIP video endpoint.....	79

Introduction

Objectives and intended audience

This deployment guide provides instructions on how to configure a Cisco TelePresence Video Communication Server (Cisco VCS) Control version X7.2 using the Back-2-Back-User-Agent (B2BUA) and Microsoft Lync 2010 (Lync) to interwork.

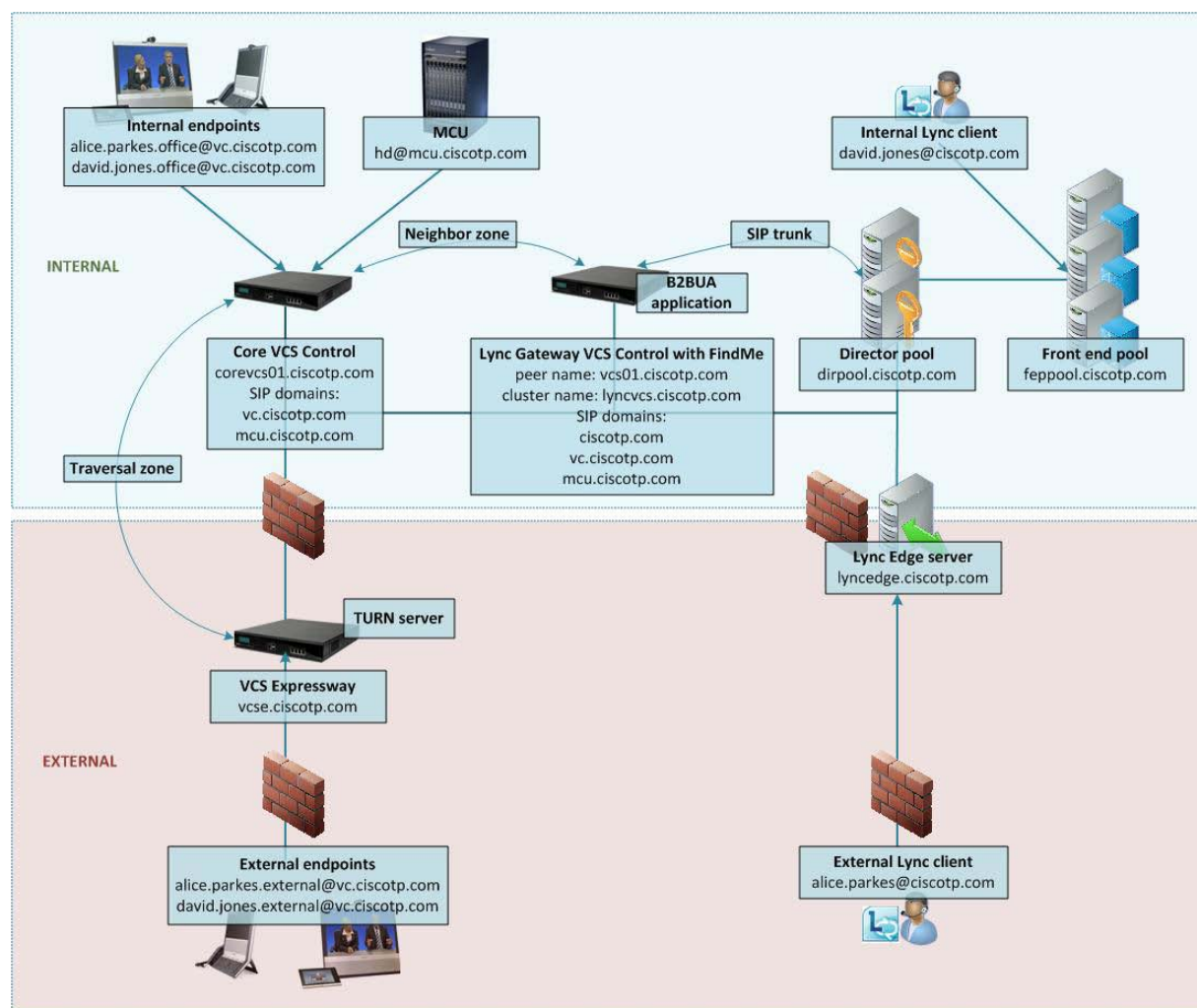
It also highlights the capabilities and limitations of interoperation of Cisco VCS Control and Lync.

For information about connecting Cisco VCS to Microsoft OCS, see *Microsoft OCS 2007, Lync 2010 and Cisco VCS Deployment Guide*.

Deployment scenario

A company is introducing a Lync environment into their network to provide Microsoft Lync clients on everybody's desk 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 environment consists of the following:

Lync deployment with:

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

Cisco video deployment with:

- Lync gateway VCS Control with peer FQDN *vcs01.ciscottp.com* and cluster FQDN *lynvcvs.ciscottp.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 with FQDN *corevcs01.ciscottp.com*
- VCS Expressway with FQDN *vcse.ciscottp.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 will typically be 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 deployment guide describes how to connect Lync and a Cisco VCS Control using a SIP trunk across an IP network. The example presented uses the following setup:

- A Cisco VCS Control (or cluster of Cisco VCS control peers) – the “Lync gateway” – to act as the link between the existing video network and Lync.
- The Lync’s SIP domain is **ciscottp.com**.

Note: 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 existing video network’s domain is **vc.ciscottp.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.ciscottp.com**).
- Lync clients registered to Lync are identified by URIs, for example:
 - David with a URI *david.jones@ciscottp.com*
 - Alice with a URI *alice.parkes@ciscottp.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.ciscottp.com*
 - Alice’s home office video endpoint with an alias of *alice.parkes.external@vc.ciscottp.com*
 - David’s internal video endpoint with an alias of *david.jones.office@vc.ciscottp.com*
 - David’s home office video endpoint with an alias of *david.jones.external@vc.ciscottp.com*
- On the “Lync gateway” VCS, FindMe accounts are setup – the B2BUA registers these into Lync so that Lync sees them as though they were Lync client registrations, for example
 - David with a URI *david.jones@ciscottp.com*, containing devices *david.jones.office@vc.ciscottp.com* and *david.jones.external@vc.ciscottp.com*
 - Alice with a URI *alice.parkes@ciscottp.com*, containing devices *alice.parkes.office@vc.ciscottp.com* and *alice.parkes.external@vc.ciscottp.com*

These FindMe users 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.

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.

- “Available”, “off-line” and “in-call” presence may be observed by Lync clients for users and MCU conferences associated with a FindMe account on the Cisco “Lync gateway” VCS (B2BUA is enabled). 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.
- 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), or by using a static SIP domain route from the Lync environment (suitable for ad-hoc conference aliases). The reason for using a separate domain for MCU registrations is to more easily prevent SIP traffic coming from Lync via a static route from propagating further into the video network than needed (by using search rules).
- “Available” and “off-line” presence may be observed by Lync clients for MCU conferences where the conferences do not have associated FindMe user entries on the “Lync gateway” VCS, however a maximum of 100 subscriptions per presentity are supported by VCS.

Clustered “Lync Gateway” VCS Control

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.

To provide 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.

Calls from Lync Server to VCS where there is no registration from VCS (e.g. for MCU calls) will typically arrive at a single VCS in the cluster, as Lync Server will use the static domain route (set up for the MCU domain), which has a single IP address for TCP connectivity and a single FQDN for TLS connectivity.

If using TLS and round-robin DNS for static route destinations, Lync server may change the VCS peer that it sends calls to, but only at a maximum rate of change of once per 5 seconds. In Lync it seems to keep sending all traffic to one VCS unless it loses connection to that VCS, and only then does it swap to another VCS – so this provides resilience rather than load balancing.

Why add a “Lync Gateway” VCS Control?

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 that the Enhanced collaboration option key needs to be purchased for and enabled on.

The presence server residing on the Lync Gateway VCS publishes presence information into the Lync environment via the B2BUA application. This presence server must be authoritative for the domain shared by Lync and the VCS (**ciscotp.com**). It must also be authoritative for the video domain (**vc.ciscotp.com**) and any dedicated MCU domains (**mcu.ciscotp.com**) in use, and hold the presence status of endpoints specified in the FindMe users 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).

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 Cisco VCS holding the relevant FindMe; having a “Lync gateway” helps funnel all calls through the correct place.

Lync Server can only send calls to:

- Cisco VCSs that have “same domain” FindMe users registered to the Lync Server; Lync Server sends the call to the VCS that is registering that user
- a single FQDN (though this may have a round robin DNS address to support a cluster of Cisco VCSs for resilience) for calls to MCUs accessible via a static domain route defined in Lync Server.

Lync server will only accept messages that it has been configured to trust. Having a dedicated “Lync gateway” VCS or Cisco 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.

“Lync gateway” and multiple Lync domains

If Lync supports multiple domains, and the video network is to support these domains as well, it is recommended 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.

Multiple “Lync gateway” per Lync domain

Apart from when the VCSs are in a single “Lync gateway” cluster, this is not a recommended architecture as 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 video infrastructure; this will cause users to lose video functionality such as duo video and far end camera control, and also possibly lose encryption and video quality.

MCUs for ad hoc conferences from Lync

Registering each possible conference ID to the Lync Server via B2BUA FindMe registrations is sometimes unachievable or impractical based on the number of URIs that need to be registered.

In this case, 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 available via registered FindMe entries – if set up – and 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 “Off-line”.
- If the conference has any participants, presence status will be “Available” (not “In-call”).

Calling an MCU conference from a Lync device will require 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 Control, the small video network being controlled by the same Cisco VCS that is the interface to Lync server.

Scaling up from a small test/demo network

As extra capacity, regional management and reduced license usage is required it is possible to 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

The versions of Cisco VCS and Lync 2010 software affect the capabilities of the deployed system.

- Version X6.1 or later is required to support Lync Standard edition and Lync Enterprise edition.
- Version X7.0 or later is required to support VCS B2BUA
- Beyond X7.x it is expected that OCS Relay will no longer be available; see *Microsoft OCS 2007, Lync 2010 and Cisco VCS Deployment Guide (X7.1)* for configuration details for non-B2BUA/OCS Relay deployments.

When using Cisco VCS X7.x (B2BUA mode) and Lync 2010:

- “Lync gateway” VCS can register FindMe users (in a single Lync domain) as Lync clients onto the Lync Server (using B2BUA FindMe registration). Lync server will fork calls to FindMe users at the same time as to Lync client users with the same name, so that calls can be taken on a Lync client or a video endpoint, as desired.
- Domain static route(s) can be set up on Lync Server to route calls to, for example an MCU domain – useful for ad-hoc conferences. (Care must be taken when using domain static routes; a static route means that Lync will send all traffic for that domain that it cannot handle to VCS).
- Search rules can be set up on VCS to route calls to secondary Lync domains – domains that the VCS is not registering FindMe users to.
- 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 Cisco VCS to Lync Server:
 - “Off-line”, “Available” and “In-call” are supported for B2BUA registered FindMe users
 - Use of ‘Available’ for registered endpoints is optional via PUA configuration
 - “Off-line” and “Available” (not “In-call”) are reported for users which are not B2BUA registered FindMe users (for up to 100 subscribers)
- Passing Lync presence to devices registered to Cisco VCS is not supported.
- Lync server connecting to a cluster of Cisco VCSs is supported when using B2BUA FindMe registration. The B2BUA shares the registrations across the Cisco VCS peers so that calls to video endpoints will be distributed across the VCS peers. If any peers go out of service, the remaining active peers will take over the registrations of the unavailable peers.
- Calls to Microsoft Mediation Servers work from endpoints in the Cisco VCS video network for SIP initiated calls, but do not work for calls interworked from H.323 (unless the workaround specified in “Appendix 5 – Known interoperating limitations” 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 Cisco VCS and OCS and the **Enhanced OCS collaboration** option key is added to the Cisco “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.

Note that although the Cisco TelePresence MCU could register directly to OCS R1, due to changes made by Microsoft, the MCU cannot register directly to Lync server. To use an MCU with Lync server, register the MCU to VCS; “Lync gateway” VCS handles the protocol differences on behalf of the MCU.

Summary of configuration process

This document describes how to configure Lync 2010 and the Cisco VCS Control version X7.x in B2BUA mode so that calls can be made 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.

Different structures for Lync

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 are recommending that DNS may be used in place of hardware load balancing for routing SIP traffic. Microsoft say:

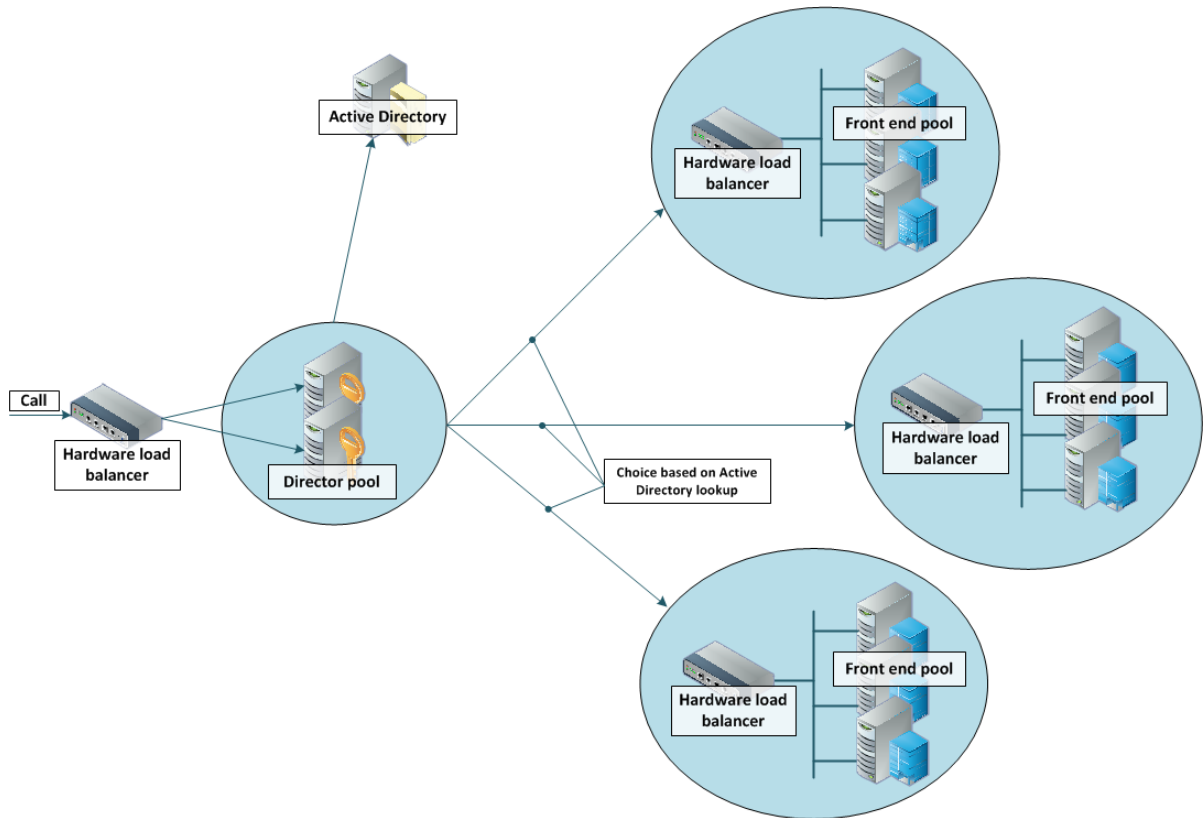
DNS Load Balancing

Microsoft Lync Server 2010 introduces DNS load balancing, a software solution that can greatly reduce the administration overhead for load balancing on your network. DNS load balancing balances the network traffic that is unique to Lync Server 2010, such as SIP traffic and media traffic.

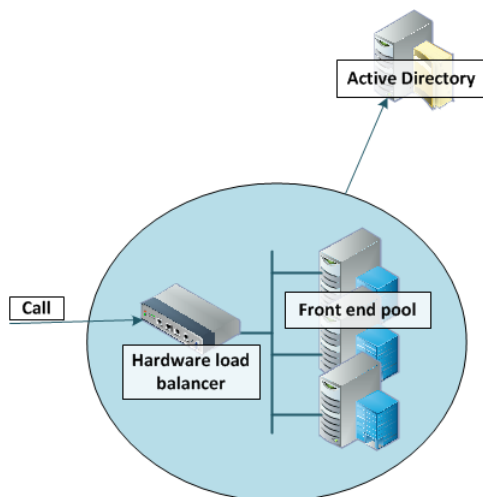
If you choose to deploy DNS load balancing, your organization's administration overhead for hardware load balancers will be greatly reduced. Additionally, complex troubleshooting of problems related to misconfiguration of load balancers for SIP traffic will be eliminated, and you can prevent server connections so that you can take servers offline. DNS load balancing also ensures that hardware load balancer problems do not affect such elements of SIP traffic as the basic routing of calls.

Using DNS load balancing may also enable you to purchase lower-cost hardware load balancers than if you used the hardware load balancers for all types of traffic. DNS load balancing is supported for Front End pools, Edge Server pools, Director pools, and stand-alone Mediation Server pools.

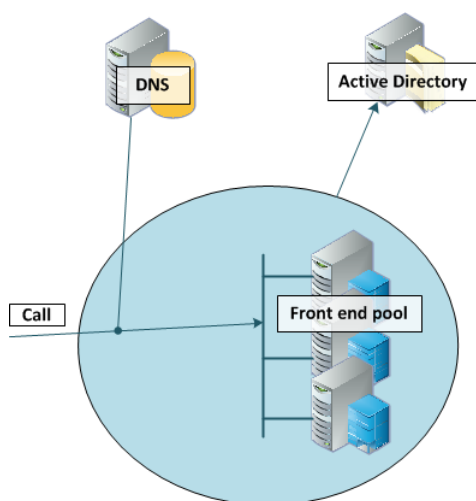
An example architecture is shown below:



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.

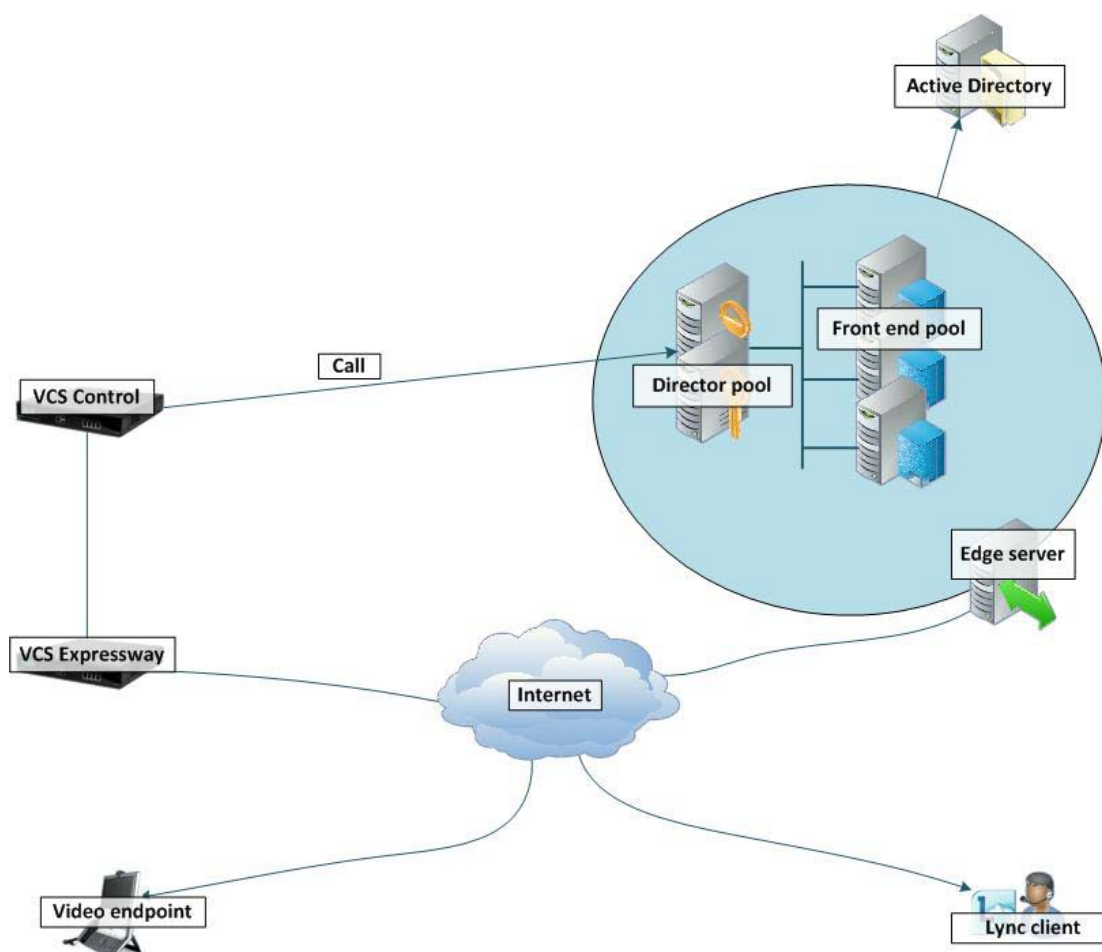


A Lync environment may use DNS instead of the Hardware Load Balancer, for example:



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 **Enhanced OCS Collaboration** option key installed, as this key allows for ICE to be used for media connectivity, which is required in this 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. In the case where SIP traffic is sent directly from a FEP to the VCS via a static SIP route, the FEP in question must be added to the B2BUA trusted host list.
- 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 MCU SIP domain (**mcu.ciscottp.com**) to the “Lync gateway” VCS cluster FQDN (or if only a single VCS, the FQDN of that VCS).
 - 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 MCU SIP domain (**mcu.ciscottp.com**) to the “Lync gateway” VCS cluster FQDN (or if only a single VCS, the FQDN of that VCS).
 - 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 MCU SIP domain (**mcu.ciscottp.com**) to the “Lync gateway” VCS cluster FQDN (or if only a single VCS, the FQDN of that VCS).

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 MCU SIP domain (**mcu.ciscottp.com**) to the “Lync gateway” VCS cluster FQDN (or if only a single VCS, the FQDN of that VCS).

“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 Cisco VCS and Lync to interoperate

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

- The “Lync gateway” VCS Control (cluster peers) must be running X7.0 code (or later)
- The “Lync gateway” VCS Control (cluster peers) must have at least the following option keys applied:
 - Non-traversal calls
 - FindMe (was User Policy)
- For Lync:
 - The version of Lync must be Lync 2010.
 - The operating system that Lync runs on must be Microsoft Server 2008 SP2 64 bit or Microsoft Server 2008 R2 64 bit.
 - The version of Lync client must be the version distributed with Lync 2010.
- 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 Cisco VCS Control 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).
- The video endpoints registered to the video network must support the H.263 video codec (unless the AM Gateway is part of the “Lync gateway” deployment) – this is the only video codec which is common to Lync clients and standard video endpoints.
- 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 OCS/Lync B2BUA was introduced in VCS X7. It provides an interface between OCS/Lync and the video network and replaces the legacy OCS Relay application.

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 VCS Expressway and Enhanced OCS Collaboration option key)
- TURN/ICE support embedded into the B2BUA (requires VCS Expressway and Enhanced OCS Collaboration option key)

The OCS/Lync B2BUA is the preferred method of integrating OCS/Lync with VCS. OCS Relay will be removed from future VCS software releases.

Video network: Check that calls between endpoints registered on VCS Controls operate as expected

This should already be operational.

Video network VCS Control configuration summary

The configuration of the VCS Control(s) 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 following item is configured:

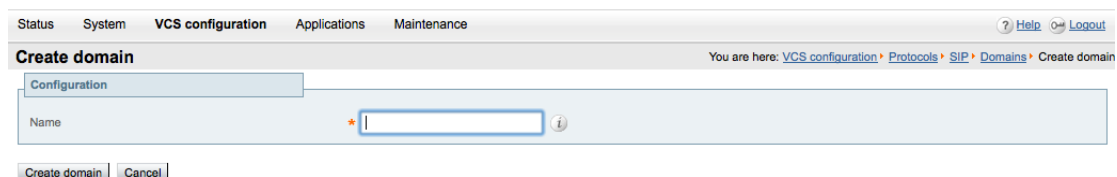
1. SIP domain of the video network - needed for SIP registration and presence handling.

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

Ensure that the SIP domain of video network endpoints is configured in the VCS Control(s) in the video network

SIP endpoints register with the Cisco 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 the **Domains** page (**VCS configuration > Protocols > SIP > Domains**).
2. Check that the domain is listed; if it is not listed:
 - a. Click **New**.
 - b. Set **Name** to, for example, **vc.ciscottp.com**.
 - c. Click **Create domain**.

The screenshot shows the 'Create domain' form in the Cisco VCS Control web interface. The breadcrumb trail at the top indicates the path: 'VCS configuration > Protocols > SIP > Domains > Create domain'. The form has a 'Name' field with a red asterisk indicating it is required. Below the field are 'Create domain' and 'Cancel' buttons.

3. Repeat for any other domains being used, e.g. **mcu.ciscottp.com**.

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.ciscottp.com)
- H.323 Call Setup = 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. It is possible to limit registrations by explicitly allowing or denying individual registrations (see the VCS Configuration section of *VCS Administrator Guide* for further details).

Calls can now be made between endpoints registered on Cisco 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 > Call history**).

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

This should already be operational.

Cisco VCS Control configuration

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

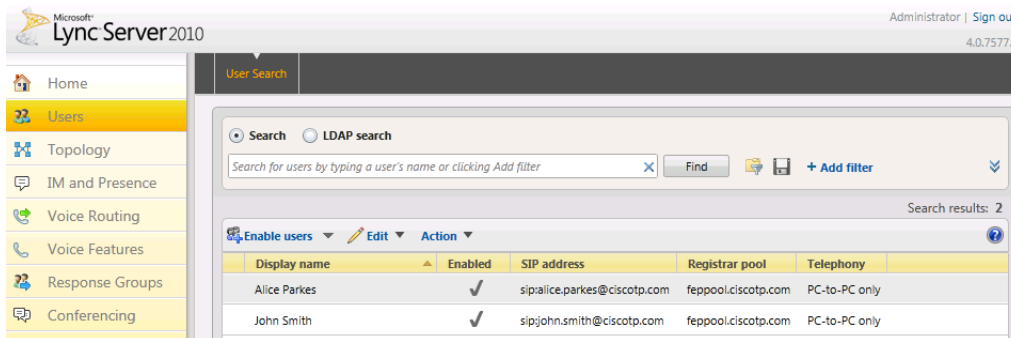
Enabling users for Lync

By default users do not support Lync. Check that users required to support Lync are enabled to do so, and if not enable them. This can be done both by Lync Server Control Panel or through Windows PowerShell commands.

To use Lync Server Control Panel, either from the start menu select Lync Server Control Panel, or if there is a desktop icon double click it:

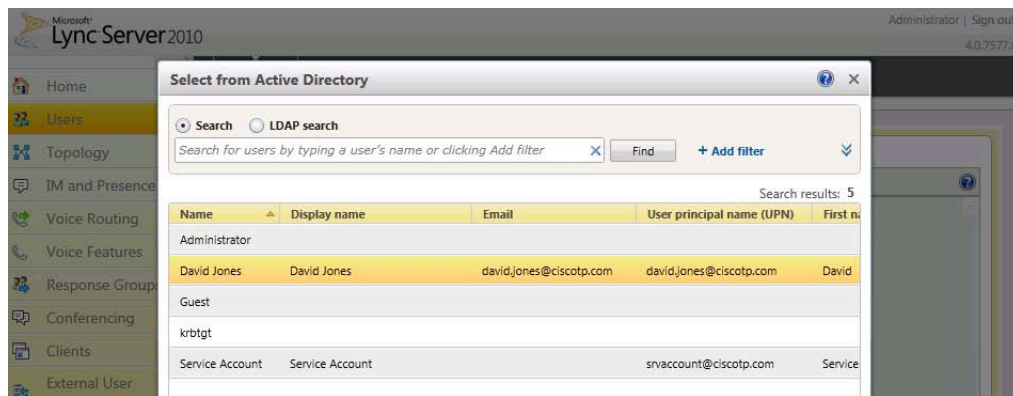


On Lync Server Control Panel go to the **Users** menu: you can see users already enabled for communication server.

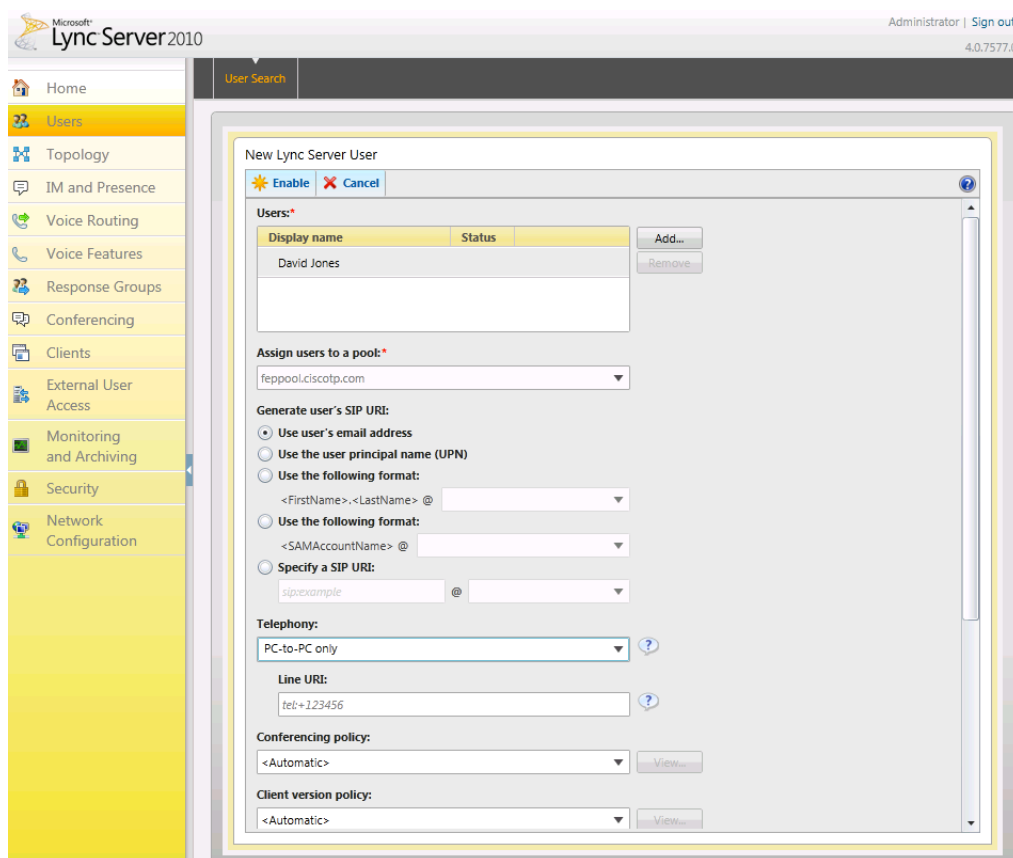


To add a new user:

1. Select **Enable users**.
2. Click **Add**.
3. 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.



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




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

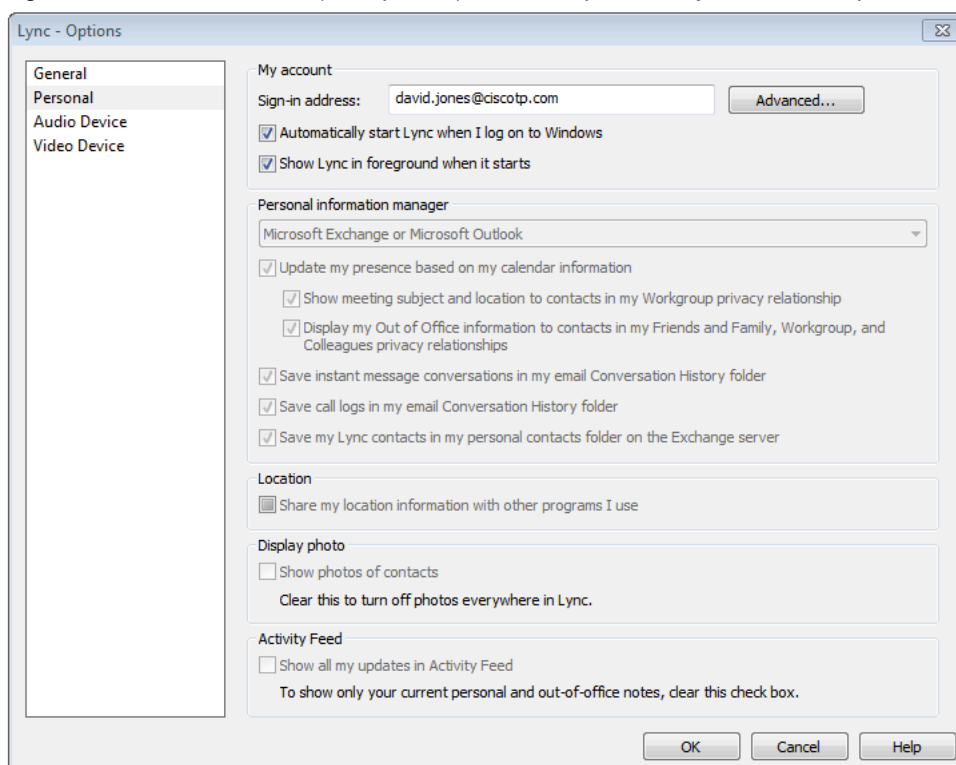
For example:

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

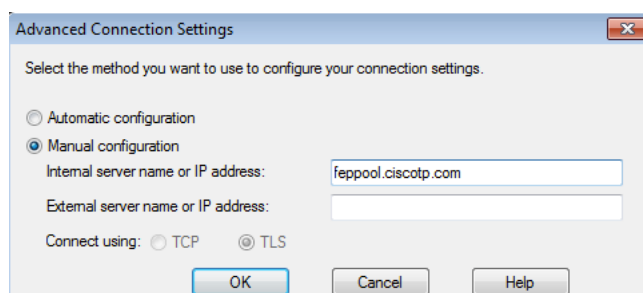
Registering Lync clients to the Lync Server

Lync client configuration

1. Install Lync client.
2. On the Sign in screen of the Lync client, 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; 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:



5. Click **Advanced**.

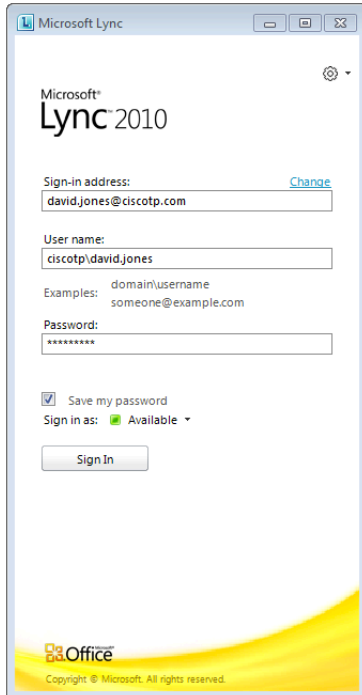


6. In a production environment ensure *Automatic configuration* is selected. If this proves not to work, select *Manual configuration* and set **Internal server name or IP address** to the FQDN of the Lync server.
7. Click **OK** to return to the **Options** dialog.
8. Click **OK** to return to the **Lync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

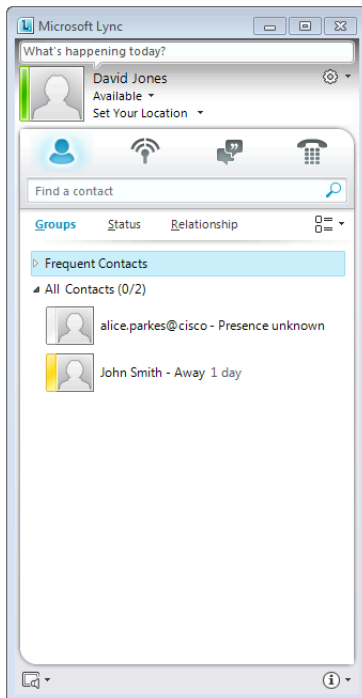
10. **User name** is the Active Directory name of the user. This may or may not be the same as the sign in address.

Note: 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. Enter the **Password** – this is the AD password for this user.



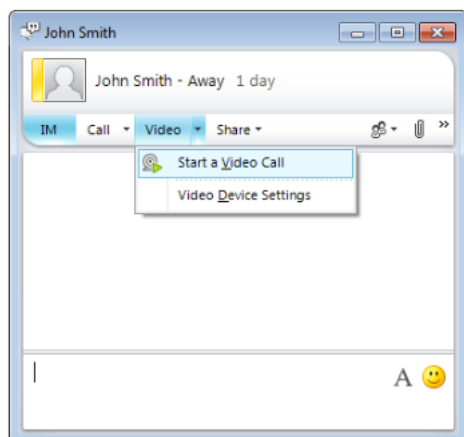
12. Click **Sign In**.



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 Lync clients registered on Lync

This is configured in 4 stages:

- Video network Cisco VCS Control configuration
- “Lync gateway” VCS Control configuration (Part 1)
- Lync Server configuration
- “Lync gateway” VCS Control configuration (Part 2)

Video network: Cisco VCS Control configuration

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

1. Set up a neighbor zone to the “Lync gateway” VCS (cluster).
2. Set up a search rule to route calls to the shared Lync domain to the “Lync gateway” VCS (cluster).
3. Set up search rules to route calls to any other domains supported on Lync (but not in the video network) to the “Lync gateway” VCS cluster — there may be none of these.

Note that in small test and demo networks this configuration is not necessary - the video network VCS is the Cisco “Lync Server Gateway” VCS. Go to “Lync gateway” VCS Control configuration (part 1)’ on page 27.

Video network: Set up a neighbor zone to the “Lync gateway” VCS (cluster)

1. Go to the [Zones](#) page ([VCS configuration > Zones > Zones](#)).
2. Click **New**.
3. Configure the following fields:

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>On</i>
In the Location section: Peer 1 address	IP address or FQDN of the “Lync gateway” VCS (or the 1 st VCS in the “Lync gateway” VCS cluster)
In the Location section: Peer 2 address to Peer 6 address	IP address or FQDN of the 2 nd to 6th “Lync gateway” cluster peers (if any)
In the Advanced section: Zone profile	<i>Default</i>

4. Click **Create zone**.

Status System **VCS configuration** Applications Maintenance

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

Create zone

Configuration

Name * To Lync gateway ⓘ

Type * Neighbor ⓘ

Hop count * 15 ⓘ

H.323

Mode On ⓘ

Port * 1719 ⓘ

SIP

Mode On ⓘ

Port * 5061 ⓘ

Transport TLS ⓘ

TLS verify mode Off ⓘ

Accept proxied registrations Allow ⓘ

Media encryption mode Auto ⓘ

Authentication

Authentication policy Do not check credentials ⓘ

SIP authentication trust mode Off ⓘ

Location

Peer 1 address vcs01.ciscotlp.com ⓘ

Peer 2 address ⓘ

Peer 3 address ⓘ

Peer 4 address ⓘ

Peer 5 address ⓘ

Peer 6 address ⓘ

Advanced

Zone profile Default ⓘ

Create zone Cancel

Video network: Set up a search rule to route calls to the Lync domain to the “Lync gateway” VCS (cluster)

1. Go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**).
2. Click **New**.
3. Configure the following fields:

Rule name	An appropriate name, for example “Route to Lync gateway”
Priority	Leave as default, for example 100
Source	Any
Mode	Alias pattern match
Pattern type	Regex
Pattern string	.+@ciscotlp.com.*
Pattern behavior	Leave

On successful match	<i>Continue</i>
Target	Select the Lync gateway zone, for example "To Lync gateway"

4. Click **Create search rule**.

Note that additional search rules must be created for any other SIP domains (other than 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).

The screenshot shows the 'Create search rule' configuration page. The 'On successful match' dropdown is set to 'Continue' and the 'Target' dropdown is set to 'To Lync gateway'. Other visible settings include Rule name: 'Route to Lync gateway', Priority: '100', Protocol: 'Any', Source: 'Any', Request must be authenticated: 'No', Mode: 'Alias pattern match', Pattern type: 'Regex', Pattern string: '.*@ciscotp1.com.*', Pattern behavior: 'Leave', and State: 'Enabled'.

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

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

1. Go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**).
2. Click **New**.
3. Configure the following fields:

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	<i>.+@<relevant domain>.*</i>
Pattern behavior	<i>Leave</i>
On successful match	<i>Stop</i>
Target	Select the Lync gateway zone, for example "To Lync gateway"

4. Click **Create search rule**.
5. 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 Control configuration (part 1)

This comprises the following steps:

- If “Lync gateway” is a cluster, unless this guide states that configuration is required on each peer, configure the Master 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 VCS.

You are recommended to use TLS connectivity between VCS and Lync. (TCP may not work for Lync configurations that include HLBs and / or Lync Director and use of TCP prevents use of encryption).

To configure a “Lync gateway” VCS Control:

1. Generate and load private key, root certificate and server certificate onto Cisco VCS.
2. Set up the SIP domain of the “Lync gateway” VCS.
3. Configure DNS.
4. Ensure that cluster name is configured.
5. Configure an NTP server.
6. Switch on TLS in SIP configuration.

“Lync gateway”: Generate and load private key, CA certificate, and server certificate onto “Lync gateway” VCS Control (not needed if using a TCP connection)

Obtain and load CA certificate, server certificate and private key into the Cisco VCS.

Note that for mutual TLS authentication the server certificate must be capable of being used as a client certificate as well.

Either a single server certificate can be created to cover the “Lync gateway” cluster, or a server certificate can be created for each Cisco VCS. If the “Lync gateway” is a non-clustered VCS then use the section “Server certificate for each Cisco VCS”

Details on how to create certificates for VCS are documented in *Cisco VCS Certificate Creation and Use Deployment Guide*.

Single server certificate that can be loaded into each cluster peer:

The certificate must specify:

- **Subject name:** the VCS cluster’s FQDN (DNS Local hostname concatenated with DNS Domain), e.g. *lynccvcs.ciscotp.com*
- **Subject Alternate Name:** a comma separated list of the VCS cluster’s FQDN and the VCS peers’ routable FQDNs e.g. *lynccvcs.ciscotp.com, vcs01.ciscotp.com, vcs02.ciscotp.com*

Server certificate for each Cisco VCS:

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. *lynccvcs.ciscotp.com, vcs01.ciscotp.com*

Load the certificates:

- The VCS’s trusted CA certificate is loaded on the [Trusted CA certificate](#) page ([Maintenance > Certificate management > Trusted CA certificate](#)).
- The VCS’s server certificate is loaded on the [Server certificate](#) page ([Maintenance > Certificate management > Server certificate](#)).

“Lync gateway”: Set up the SIP domain of the “Lync gateway” VCS

B2BUA registered FindMe users need the “Lync gateway” VCS be authoritative for the Lync server’s shared domain.

1. Go to the **Domains** page (**VCS configuration > Protocols > SIP > Domains**).
2. Click **New**.
3. Set **Name** to *ciscotp.com*.
4. Click **Create domain**.

“Lync gateway”: 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: if the DNS server IP address is 127.0.0.1 that means that Lync server is using a DNS server on its own hardware. Instead of entering 127.0.0.1 on the Cisco VCS, use the IP address of the Lync server platform instead.

On each “Lync gateway” VCS Control peer:

1. Go to the **DNS** page (**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.
 - c. Click **Save**.
3. If the VCS must use other DNS servers for normal calls and only the Lync DNS server for Lync access:
 - a. 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: Domain shared with Lync

- b. 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:

- On the **DNS** page (**System > DNS**) set:
 - Local host name** to a unique hostname for this Cisco VCS.
 - Domain name** to the domain name for this Cisco VCS.
- 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”: Ensure that cluster name is configured

This should be configured whether the Cisco VCS is part of a cluster or not; this value is used with FindMe as well as clustering.

For each “Lync gateway” VCS peer, ensure that **Cluster name** 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 “Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide (X7.0)”. If the cluster name needs changing follow the procedure in that document.

“Lync gateway”: Configure an NTP server

On each “Lync gateway” VCS Control peer:

- Go to the **Time** page (**System > Time**).
- Set **NTP server 1** to the IP address of an NTP server.
- Optionally set **NTP server 2** to the IP address of an additional NTP server.
- Set **Time zone** as appropriate to the location of the Cisco VCS.

The screenshot shows the 'Time' configuration page in the Cisco VCS management interface. The breadcrumb trail at the top indicates 'System > Time'. The page is divided into two main sections: 'NTP servers' and 'Time zone'.

NTP servers section: This section contains a table with five rows, each representing an NTP server (NTP server 1 through NTP server 5). Each row has two columns: 'Address' and 'Authentication'. The 'Address' column contains text input fields with the following values: 'ntp01.ciscottp.com', 'ntp02.ciscottp.com', and three empty fields. The 'Authentication' column contains dropdown menus, all of which are set to 'Disabled'. Each row also has an information icon (i) to its right.

Time zone section: This section contains a single row with a 'Time zone' label and a dropdown menu. The dropdown menu is set to 'Europe/London' and has an information icon (i) to its right.

At the bottom of the page, there is a 'Save' button.

Note that 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”: Switch on TLS in SIP configuration

- Go to the **SIP** page (**VCS configuration > Protocols > SIP > Configuration**).
- Ensure that **TLS mode** is *On*.

Status System **VCS configuration** Applications Maintenance

SIP You are here: [VCS configuration](#) > [Protocols](#) > [SIP](#) > Configuration

Configuration

SIP mode	<input type="button" value="On"/>	
UDP mode	<input type="button" value="Off"/>	
UDP port	<input type="text" value="5060"/>	
TCP mode	<input type="button" value="On"/>	
TCP port	<input type="text" value="5060"/>	
TLS mode	<input type="button" value="On"/>	
TLS port	<input type="text" value="5061"/>	
TCP outbound port start	<input type="text" value="25000"/>	
TCP outbound port end	<input type="text" value="29999"/>	
Session refresh interval (seconds)	<input type="text" value="1800"/>	
Minimum session refresh interval (seconds)	<input type="text" value="500"/>	
Require UDP BFCP mode	<input type="button" value="On"/>	
Require duo video mode	<input type="button" value="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” Cisco VCS and to route traffic to Cisco 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” Cisco VCS to communicate with Lync Server:

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

Trust a “Lync Gateway” VCS (cluster)

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:

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. Please note that this name must match the one specified in the certificate.
 - ComputerFqdn**: specifies the Lync Gateway VCS **peer** FQDN (Specify the master VCS FQDN if running a cluster), e.g. *vcs01.ciscotp.com*. Please note that this name must match the one specified in the certificate.
 - Registrar**: specifies the FQDN of the registrar for the Lync pool
 - site**: specifies the siteID on which this application pool is homed

Note: It is possible to 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)

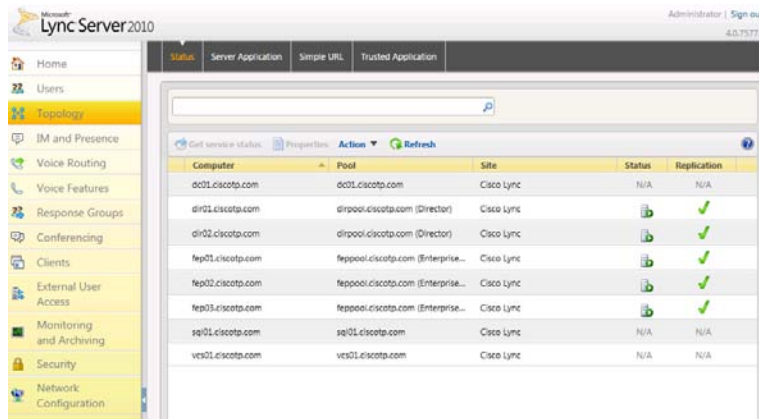
For example:

```
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
```

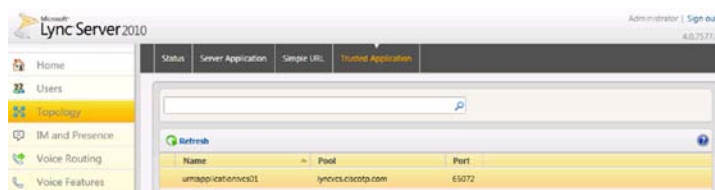
3. Use the Topology Builder to configure the IP address of the VCS as a trusted server (this is required for TCP deployments):

- 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.ciscotp.com*. Please note that this name must match the one specified in the 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.ciscotp.com*).
- For example:
- ```
C:\Users\Administrator.CISCOTP> New-CsTrustedApplicationComputer -Identity vcs02.ciscotp.com -Pool lyncvcs.ciscotp.com
```
5. Assign an application to a specific application pool:
- Use the command **New-CsTrustedApplication** with the following parameters:
    - ApplicationID**: specifies a label for the Lync Gateway 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 be used 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.ciscotp.com -Port 65072`
- For example, for TCP: `C:\Users\administrator.CISCOTP>New-CsTrustedApplication -ApplicationId VCSApplication1 -TrustedApplicationPoolFqdn lyncvcs.ciscotp.com -Port 65072 -EnableTCP`
6. Apply the configuration
- Use the command **Enable-CsTopology**.
- For example:
- ```
C:\Users\administrator.CISCOTP>Enable-CsTopology
```

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



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



Configure Lync Server media encryption capabilities

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

VCS has the capability to carry out on-the-fly modification of these headers if the **Enhanced OCS Collaboration** 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 **Enhanced OCS Collaboration** option key enabled?
If no, encryption must not be set to **require** on Lync server.
- Is the “Lync gateway” using the B2BUA?
If no, encryption must be the same on the Lync server and in the video network.
If the B2BUA is in use and **Encryption** (in B2BUA advanced settings) is set to *Auto*, the B2BUA will allow calls with Lync side encrypted and video side not, both sides encrypted and both sides unencrypted. However, the "Lync side encrypted and video side not" scenario can only occur when the B2BUA receives an empty INVITE from the VCS, for instance in an H.323 > SIP interworked call. If Lync is configured to require encryption, and the endpoint on the VCS side does not support media encryption, a call from Lync to this endpoint will fail as Lync will drop the call because of the encryption capability mismatch.
- 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*.

In Lync the values: **RequireEncryption**, **SupportEncryption**, **DoNotSupportEncryption** are allowed.

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 **Enhanced OCS Collaboration** option key is installed and the connection between the Cisco 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 Control configuration (part 2)

This comprises the following steps:

- Configure the B2BUA on the “Lync gateway” VCS.
- Configure the B2BUA trusted hosts on the “Lync gateway” VCS.
- Set up a search rule to route calls to the shared Lync domain to Lync (via the B2BUA).
- Set up search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync (via the B2BUA).
 - there may be none of these.

Configure the B2BUA on the “Lync gateway” VCS

When configuring the B2BUA, two of the fields to configure will be the destination address and destination port for the B2BUA to send signaling to in the Lync environment. The values that need to be entered will 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 the [Microsoft Lync B2BUA configuration](#) page ([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 <i>dirpool.ciscotp.com</i>
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>Yes</i>
Lync domain	Select Lync domain, e.g. <i>ciscotp.com</i>
Enable transcoders for this B2BUA	If no AM GW is to be used, set to <i>No</i> . If an AM GW is to be used, see “ <i>Appendix 7 – B2BUA and AMGW integration</i> ”
Offer TURN Services	<i>No</i>
Encryption	<i>Auto</i>
B2BUA media port range start	Leave at default 56000
B2BUA media port range end	Leave at default 57000
Hop count	Leave at default 70
Port on B2BUA for VCS communications	Leave at default 65070
Port on B2BUA for Lync call communications	Leave at default 65072

Port on B2BUA for Lync presence communications

Leave at default 10011

3. Click **Save**.

Status	System	VCS configuration	Applications	Maintenance
Microsoft OCS/Lync B2BUA configuration				
 Warning: The B2BUA is enabled but no search rules have been configured for the 'To Microsoft OCS/Lync server via B2BUA' zone.				
Configuration				
Microsoft OCS/Lync B2BUA		Enabled 		
OCS/Lync signaling destination address		dirpool.ciscotp.com  Configure trusted hosts		
OCS/Lync signaling destination port		* 5061 		
OCS/Lync signaling transport		TLS 		
Capabilities				
Register FindMe users as clients on OCS/Lync		Yes 		
OCS/Lync domain		ciscotp.com  Configure SIP domains		
Transcoders				
Enable transcoders for this B2BUA		No 		
TURN				
Offer TURN services		No 		
Advanced				
Advanced settings		Show advanced settings		
Save				

Enabling the B2BUA causes a non-configurable neighbor zone called “To Microsoft OCS/Lync server via B2BUA” to be automatically set up:

Status System **VCS configuration** Applications Maintenance ?

Edit zone You are here: VCS configuration > Zones > Zones > Edit zone

Info: This zone has been generated for the B2BUA service, edit it on the [Microsoft OCS/Lync B2BUA configuration page](#)

Configuration

Name * To Microsoft OCS/Lync server via B2 i

Type Neighbor

Hop count 15 i

H.323

Mode Off i

Port 1719 i

SIP

Mode On i

Port * 65070 i

Transport TLS i

TLS verify mode Off i

Accept proxied registrations Allow i

Media encryption mode Auto i

Authentication

Authentication policy Treat as authenticated i

SIP authentication trust mode Off i

Location

Peer 1 address localservice.localdomain i SIP: Active: 10.50.164.11:65070

Peer 2 address i

Peer 3 address i

Peer 4 address i

Peer 5 address i

Peer 6 address i

Advanced

Zone profile Microsoft OCS/Lync i

Configure 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 the **Microsoft Lync B2BUA trusted hosts** page (**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>

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

Set up a search rule to route calls to the shared Lync domain to Lync (via the B2BUA)

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 “Appendix 8 – TEL URI handling for Cisco VCS to Lync calls” 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 the **Search rules** page (**VCS 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	<i>Any</i>
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	.+@ciscotp\com.*
Pattern behavior	<i>Leave</i>
On successful match	<i>Stop</i>
Target zone	<i>To Microsoft Lync server via B2BUA</i>

4. Click **Save**.

See the Zones and Neighbors section of *VCS Administrator Guide* for further details.

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 a search rules to route calls to any other domains supported on Lync (but not in the video network) to Lync (via the B2BUA)

Lync may only support a single domain, the shared domain; if this is the case, no other search rule is required here.

If Lync does however support other domains and video endpoints should be able to call these devices, one or more additional search rules can be added.

1. Go to the **Search rules** page (**VCS 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>
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**.

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.

5. Repeat for all domains supported on Lync (that are not also 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 Cisco VCS Control.

Note that if Lync for Mac is used and no AMGW is installed, the call will result in an audio only call as Lync for Mac does not any video codecs supported by standards-based endpoints.

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

“Lync gateway” VCS Control configuration

- Configure the “Lync gateway” VCS with a neighbor zone that contains the video network.
- 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).

Note that in small test and demo networks this configuration is not necessary as the video network VCS is the “Lync Gateway” VCS. You can skip this section and go to “Lync Active Directory configuration for FindMe users” on page 43.

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

1. Go to the **Zones** page (**VCS 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 Cisco VCS for TLS mode SIP)
SIP transport	<i>TLS</i>
H.323 mode	<i>On</i>
In the Location section: Peer 1 address	IP address or FQDN of the video network Cisco VCS (or the 1 st Cisco VCS in the video network cluster)
In the Location section: Peer 2 address to Peer 6 address	IP address or FQDN of the 2 nd to 6th video network cluster peers (if any)
In the Advanced section: Zone profile	<i>Default</i>

4. Click **Save**.

Status System **VCS configuration** Applications Maintenance

You are here: VCS configuration > Zones > Zones > Create zone

Create zone

Configuration

Name ⓘ

Type Neighbor

Hop count ⓘ

H.323

Mode ⓘ

Port ⓘ

SIP

Mode ⓘ

Port ⓘ

Transport ⓘ

TLS verify mode ⓘ

Accept proxied registrations ⓘ

Media encryption mode ⓘ

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 ⓘ

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

1. Go to the **Search rules** page (**VCS 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\.ciscotp\.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**.

The screenshot shows the 'Create search rule' configuration window. The configuration is as follows:

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

At the bottom, there are buttons for 'Create search rule' and 'Cancel'.

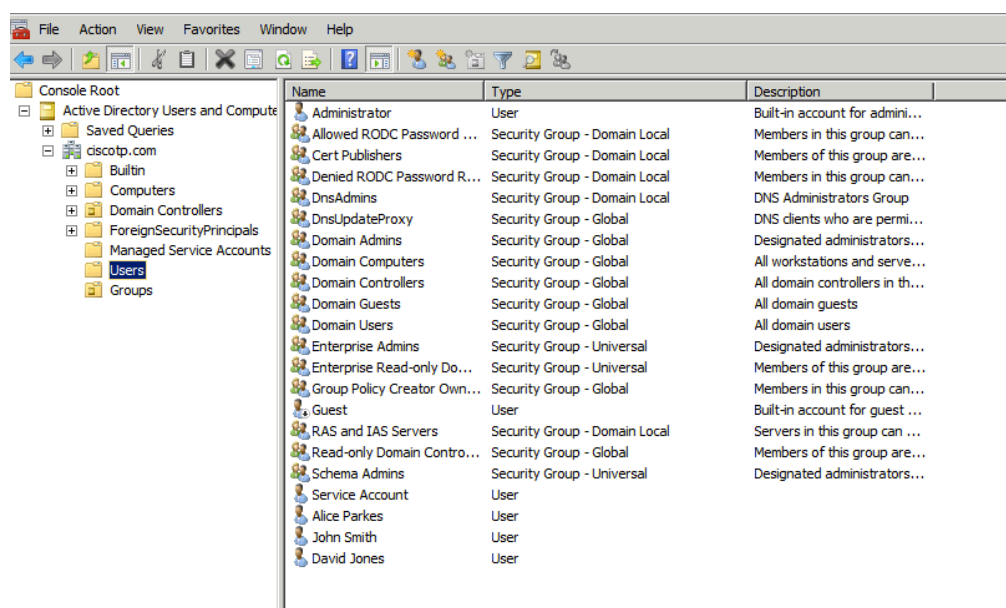
6. Repeat until there is a rule for each video network domain (for example, add a search rule for `.*@mcu.ciscotp.com`).

Lync Active Directory configuration 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).

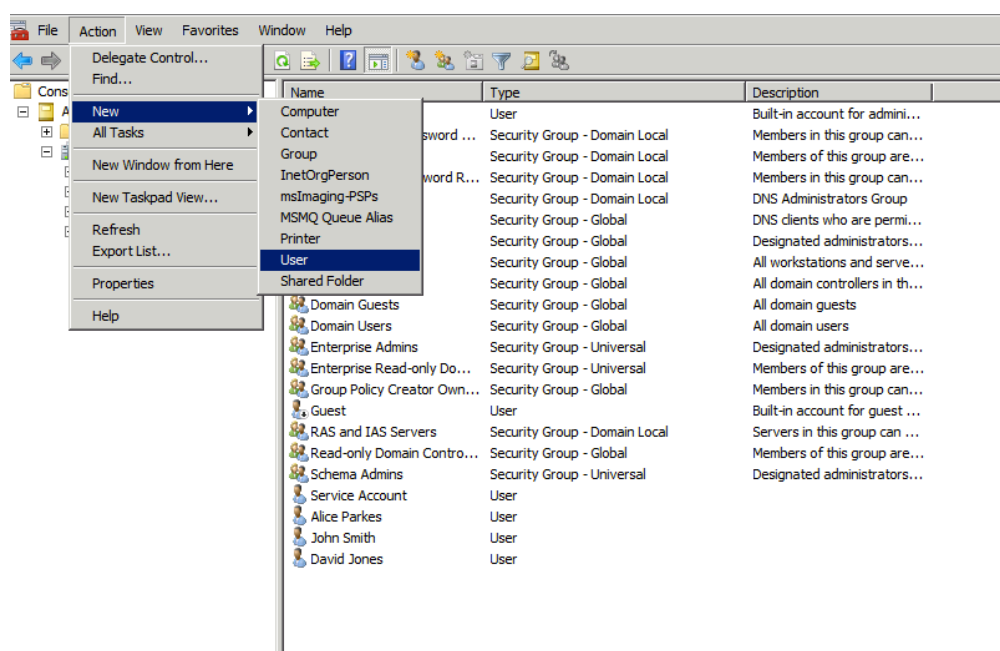
On the PC running the Active Directory for Lync users:

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:

- Click  **Create new user** in the current container or select **Action > New > User**:



- 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

- Click **Next**.
- Configure the following fields:

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

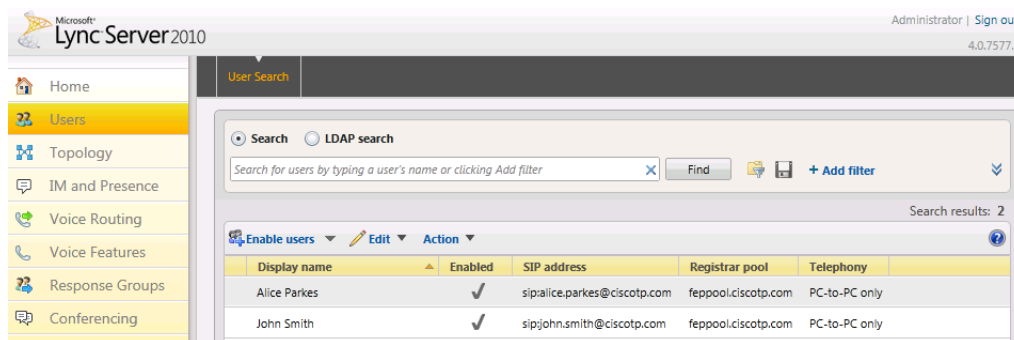
7. Click **Next**.
8. Click **Finish**.
9. Enable the user for Lync:

This can be done using Lync Server Control Panel (LSCP) or Windows PowerShell commands.

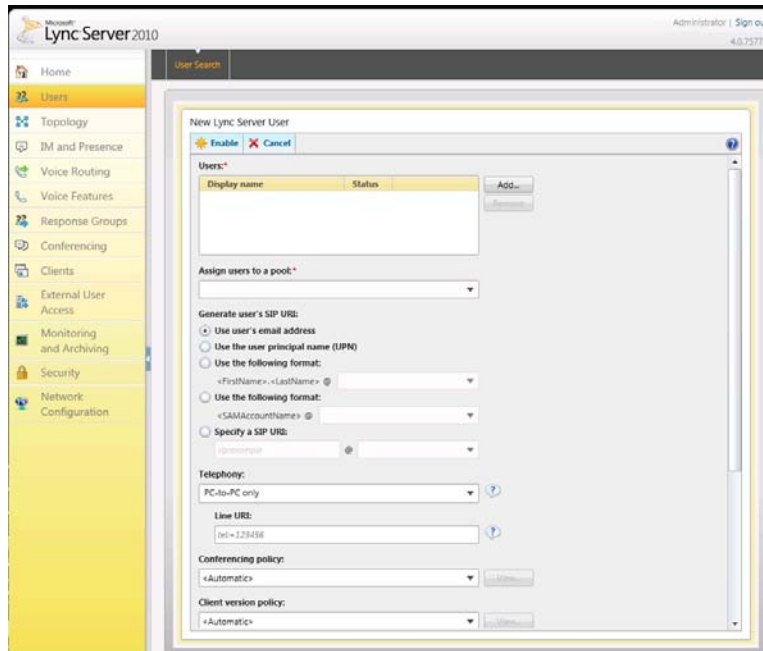
To use Lync Server Control Panel, either from the start menu select Lync Server Control Panel, or if there is a desktop icon double click it:



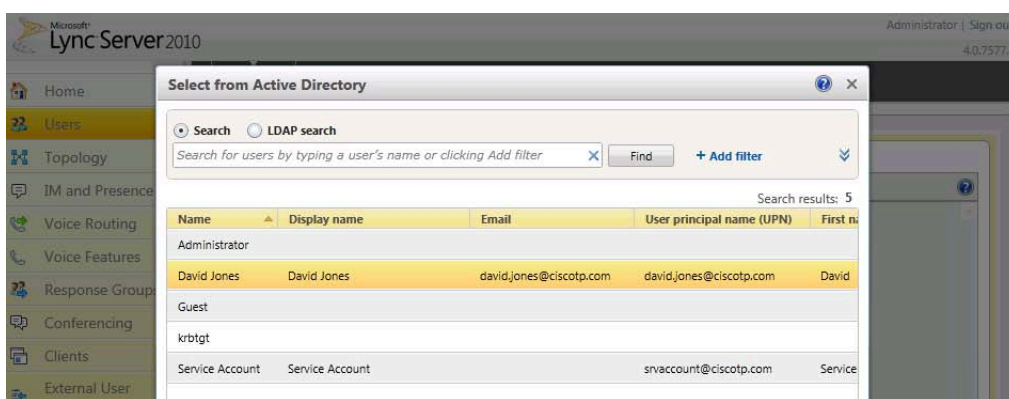
- a. On Lync Server Control Panel go to the **Users** menu. You can see the users already enabled for communication server.



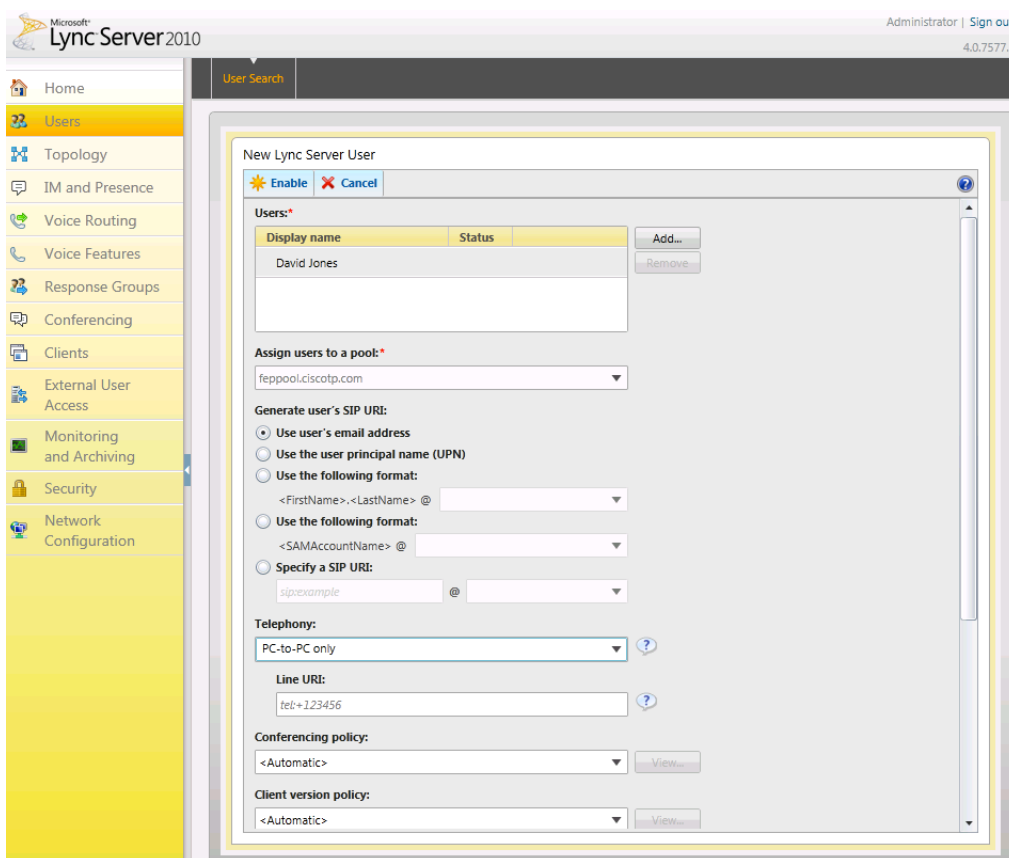
- b. To add a new user, select **Enable users**.



- c. Click **Add**.



- d. Search for and select the VCS FindMe user
 Note: to find the user it must already have been defined in Active Directory.



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

Note that 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
```

“Lync gateway” VCS FindMe configuration

- Go to the **Option keys** page (**Maintenance > Option keys**).
 Ensure that the “FindMe” key (116341U00-1-xxxxxxx) is listed.
- Go to the **FindMe Configuration** page (**Applications > FindMe > Configuration**).
 - Ensure **Mode** is set to **On**.

3. 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 – this means that when a called party rings the caller ID back, all FindMe endpoints will ring, not just the endpoint that made the initial call will ring.

4. Click **Save**.

5. Configure VCS to be authoritative for the Lync domain so that FindMe users with that domain can be handled by this VCS and register as Lync client devices to Lync.

Go to the **Domains** page (**VCS configuration > Protocols > SIP > Domains**).

6. Click **New**.7. In **Name** enter the domain shared with Lync (for example, ciscotp.com).8. Click **Create domain**.

9. 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 the **User accounts** page (**Maintenance > Login accounts > User accounts**).

b. Click **New**.

c. Configure the following fields:

Username	Username used by the FindMe user to log in to Cisco 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	Password needed by the FindMe user to log in to Cisco VCS to administer this account Not configurable if VCS is configured with User authentication source as Remote
Confirm password	As Initial password Not configurable if VCS is configured with User authentication source as Remote
FindMe type	<i>Individual</i>

10. Make sure 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 "Configure the DNS" above.

The screenshot shows the 'Create user account' form in the Cisco VCS Maintenance section. The form is titled 'Create user account' and has a breadcrumb trail: 'You are here: Maintenance > Login accounts > User accounts > Create user account'. The form is divided into two main sections: 'User details' and 'FindMe'. The 'User details' section includes fields for 'Username', 'Display name', and 'Phone number'. The 'FindMe' section includes fields for 'FindMe ID (dialable address)', 'Principal device address', 'Initial password', 'Confirm password', and 'FindMe type' (set to 'Individual'). The form has 'Save' and 'Cancel' buttons at the bottom.

Login 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 FindMe accounts are registered

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

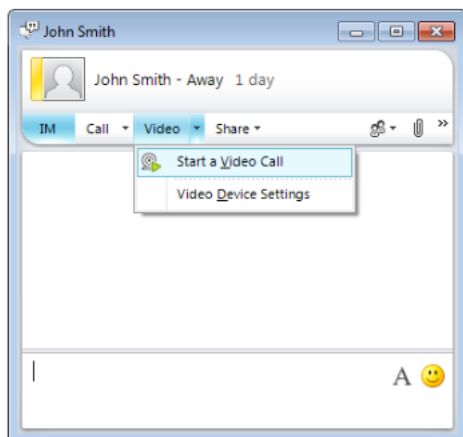
1. Go to the **Lync users status** page (**Status > Applications > Lync users**).
2. Verify the following for each FindMe user:
 - Registrations state is Registered
 - Presence state is Online (if **Default published status for registered endpoints** is set to *Online*, otherwise expect to see Offline)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

If the states are not as expected, verify 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:



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

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

- 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.
Also VCS only supports a maximum of 100 subscriptions per presentity.
- Using the B2BUA with FindMe IDs registered to Lync Server, “gray” (not available), “green” (available) and “In-call” states are provided to Lync Server.
- 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 Cisco 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 (currently only applies to Movi and E20).

In summary:

	... to Cisco VCS	... to Lync server
Cisco VCS to ... (user not registered)	Full presence available (to Movi and E20)	Presence = Available only
Cisco VCS to ... (FindMe user registered)	Full presence available (to Movi and E20)	Presence = Available and In-call
Lync server to ...	No presence information available	Full presence available

Cisco VCS configuration

If endpoints registered to the VCS Control supply their own presence information the VCS Control only needs to be a Presence Server, aggregating presence information and providing presence status to users who subscribe for the information.

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

- VCS PUA generates Presence = In-call if the endpoint is in a call
- VCS PUA optionally (and by default) generates Presence = 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: for H.323 devices to supply presence (via the PUA) the registered H323 ID of that endpoint must resemble a SIP URI. The PUA will publish presence for that URI.

To configure presence on the VCS Control:

1. Go to the **Presence** page (**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> (default) – select this to publish available if the endpoint is registered <i>Offline</i> – select this if the available / not-available decision is

	to be left to the Lync client / endpoint that publishes its own presence
SIP SIMPLE Presence Server	<i>On</i>

The screenshot shows the VCS Control web interface. The top navigation bar includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The 'Applications' tab is selected, and the 'Presence' sub-tab is active. The breadcrumb trail shows 'You are here: Applications > Presence'. The configuration area has two main sections: 'PUA' (Presence User Agent) and 'Presence Server'. In the 'PUA' section, 'SIP SIMPLE Presence User Agent' is set to 'On' and 'Default published status for registered endpoints' is set to 'Online'. In the 'Presence Server' section, 'SIP SIMPLE Presence Server' is set to 'On'. A 'Save' button is located below the configuration area. At the bottom, a 'Status' section shows a table with two rows: 'Presence User Agent' with status 'Active' and 'Presence Server' with status 'Active'.

Note: The “Lync gateway” VCS that connects to the Lync Server must be the presence server for the SIP domain that the “Lync gateway” VCS shares with Lync server. It should also be the presence server for any other 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.

The “Lync gateway” must also be the presence server 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.

The presence server will handle presence for all domains that VCS has been configured to be authoritative for, so check the correct domains are set up on the [Domains](#) page ([VCS configuration > Protocols > SIP > Domains](#))

For more details on presence see “Presence” in the Applications section of *VCS Administrator Guide*.

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.

Testing the configuration

Set up the endpoints registered on VCS Control 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:

- Registration state = Registered
- Subscription state = Subscribed
- Presence state = offline, online, or busy
- See the icon on Lync client change from gray to green when an endpoint is registered on VCS Control (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 Control (if **Default published status for registered endpoints** is set to *Online*).
- See the icon on Lync client change to in-call if the endpoint is in a call.

Optional: MCUs

Configuration of Cisco VCS and Cisco MCUs

The configuration of both the VCS and the Cisco MCU documented in *Multiway deployment guide* is the correct configuration for VCS and Cisco MCU when working with Lync server. See that document for further details.

Adding a directly callable MCU

MCUs must register to a VCS in order for Lync users to be able to join conferences (MCUs cannot register to Lync Server).

The MCU should be configured to support SIP access to conferences to avoid the need to interwork the Lync client calls.

- Register the Cisco MCU to a video network VCS using a dedicated MCU domain (e.g. mcu.ciscotp.com)
- Configure a search rule from the “Lync gateway” VCS to the video network VCS for the MCU domain (e.g. mcu.ciscotp.com) if the MCU is not registered to the “Lync gateway” VCS
- If access to ad-hoc conferences is required, set up a static domain route from Lync to the “Lync gateway” VCS for the MCU domain (e.g. mcu.ciscotp.com). This route should reside on the Director (pool) if present, otherwise on the FEP (pool).
- For static/permanent conferences, it is recommended to create a FindMe account for these, where the FindMe account contains the SIP URI of the conference as a device.

For statically routed/non-FindMe conferences, presence will show as:

- Available if conference has been created (and SIP-registered)
- Offline if conference has not been created (or not SIP-registered)

(The presence will never show as in-call, this would require a FindMe account for the conference)

Note: The VCS supports a maximum of 100 subscriptions per presentity

For FindMe-based permanent conferences, presence will show as:

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

Adding an MCU using just the Autoattendant

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. This method will however not leverage the 'In-call' presence status available for individual FindMe-based conferences.

Configure static routes to route MCU 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.
 - TLSRoute**: specifies that the route is TLS (recommended)

-**TCPRoute**: specifies that the route is TCP

-**Destination**: "" specifies the Lync Gateway VCS FQDN (or Lync Gateway VCS Cluster FQDN if using a VCS cluster) for TLS Routes. Use IP Address in case of TCP Routes.

-**MatchUri**: "" specifies the sip domain that Lync Gateway VCS is authoritative for

-**Port**: specifies TLS/TCP port to be used 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).

-**UseDefaultCertificate**: specifies 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 -TLSType -Destination "lyncvcs.ciscotp.com" -MatchUri "mcu.ciscotp.com" -Port 65072 -UseDefaultCertificate $true`

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=}**: assigns the route defined earlier to the specified Identity (note that brackets are "curly")

For example:

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

3. Verify static route assignment

- To verify the correct assignment of the route use the command "`Get-CsStaticRoutingConfiguration`".

For example:

```
C:\Users\administrator.CISCOTP> Get-CsStaticRoutingConfiguration
Identity: Global
Route:
{MatchUri=mcu.ciscotp.com;MatchOnlyPhoneUri=False;Enabled=True;Repla
ceHostInRequestUri=False}
```

Note: Static routes should only be set up where absolutely necessary, e.g. for allowing ad hoc calls to an MCU:

- ▶ When Lync Server tries to route a call:
 - Lync Server 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 user, 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 Lync Server will route the call to the destination specified.
 - ▶ The primary access to end users registered on Cisco VCS should be with the FindMe user registered to Lync server by the B2BUA.
 - ▶ Providing a static route for an MCU domain means that ad hoc MCU calls can be made by Lync clients (without having to set up FindMe IDs for all potential ad hoc call IDs).
 - ▶ 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.
-

Enabling Microsoft Edge Server and VCS TURN capabilities

Ensure that the Enhanced OCS Collaboration 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 the **Microsoft Lync B2BUA configuration** page (**Applications > B2BUA > Microsoft Lync > Configuration**).
2. Configure the fields as follows:

Offer TURN Services	Yes
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 the VCS Expressway has TURN configured to use
TURN services username	Username authenticated to use TURN server
TURN services password	Password for username to authenticate with TURN server

Appendix 1 – Troubleshooting

Troubleshooting checklist for X7.x

If experiencing a problem with the Lync integration, it is recommended to go through the following list when performing the initial faultfinding, 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). This can be done using the [Maintenance > Tools > Network utilities > DNS Lookup](#) page 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. This can be done using 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 Cisco VCS Control local calls

Look at search history to check the applied transforms

1. Go to the [Search history](#) page ([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 prioritized zone 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.)

If the search indicates:

- **Found:** False
- **Reason:** 480 Temporarily Not Available

this could be because the Cisco VCS's zone links are not correctly set up. From the command line execute:

```
xcommand DefaultLinksAdd
```

to set up the required links for Cisco VCS default zones. Also check 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 the **Call history** page (**Status > Call 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 Cisco VCS Control used to route the call.

Check for errors

Event Log

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

Tracing calls

Tracing calls at SIP / H.323 level

X7 or later:

1. Log in to Cisco VCS Control web interface as **admin**.
2. Go to **Maintenance > Diagnostics > Diagnostics logging**.
3. Ensure all log levels are set to **DEBUG** and click **Start new log**.
4. Retry the action for which the problem occurs (such as setting up a call or similar).
5. Click **Stop logging** followed by **Download log**.

The log file will contain information related to the events triggered by the action performed in step 4.

Presence not observed as expected

Presence Server status

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

No presence being observed

Check that there is no transform that may be inadvertently corrupting the presence Publication, Subscription or Notify – e.g. 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 (available from the web browser) 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:

- 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.

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 the VCS 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 enhanced collaboration 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.

Cisco VCS to Lync server calls fail – DNS server

Cisco 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.

Cisco VCS to Lync calls fail – Hardware Load Balancer

If the Lync environment has FEPs with an HLB in front, ensure that the Cisco 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 Lync client – registered to the FEP – to Cisco 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, e.g.:

```
a=candidate:1 1 UDP 2130706431 192.168.1.7 30580 typ host
a=candidate:1 2 UDP 2130705918 192.168.1.7 30581 typ host
a=candidate:2 1 TCP-ACT 1684798975 192.168.1.7 30580 typ srflx raddr 192.168.1.7 rport 30580
```

```
a=candidate:2 2 TCP-ACT 1684798462 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 e.g.:

```
a=candidate:1 1 UDP 2130706431 84.233.149.125 56056 typ host
a=candidate:1 2 UDP 2130706430 84.233.149.125 56057 typ host
a=candidate:4 1 UDP 16777215 194.100.47.5 60000 typ relay raddr 84.233.149.125 rport 56056
a=candidate:4 2 UDP 16777214 194.100.47.5 60001 typ relay raddr 84.233.149.125 rport 56057
```

- Host and Relay candidates 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 OCS/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, 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). In order 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 Enhanced Collaboration 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

Cisco VCS modifies the application part of INVITEs / OKs received from Lync clients to make them compatible with traditional SIP SDP messaging. Cisco 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 Cisco VCS registered endpoint), check the search history and ensure that the call is seen coming from

- a Lync neighbor zone (if not using B2BUA)
- a Lync trusted host (when using B2BUA)

If it is not, then the call may be coming from a FEP rather than the load balancer. See the section on configuring Cisco VCS and Hardware Load Balancers, and

- set up the relevant neighbor zones without any associated search rules, but with peer addresses containing the FEP IP addresses (if not using B2BUA)
- configure Lync trusted hosts containing the FEP IP addresses (when using B2BUA)

Lync rejects VCS zone alive 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 doesn't trust the sender of the message.
- A response '401 Unauthorized' response to OPTIONS is another indication that Lync doesn't 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 it is in a call with.

Call to PSTN (via Lync PSTN gateway) 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. This actually means that 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:

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

in that order to route calls to Cisco VCS.

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 Cisco 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 login first from a Lync client before the B2BUA can properly control the Lync user.

Lync problems

As a starting point, running the Lync Server 2010 'Best Practices Analyzer' will help identify configurations that may be incorrect on Lync Server. Details and the download can be found at:

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=030548df-0dc7-4f86-b8a9-2f5ec8de8ba5>

Problems with certificates

If a non-Lync application is used to create certificates to load onto Cisco VCS for use with Lync (e.g. 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 2 – Debugging on Lync

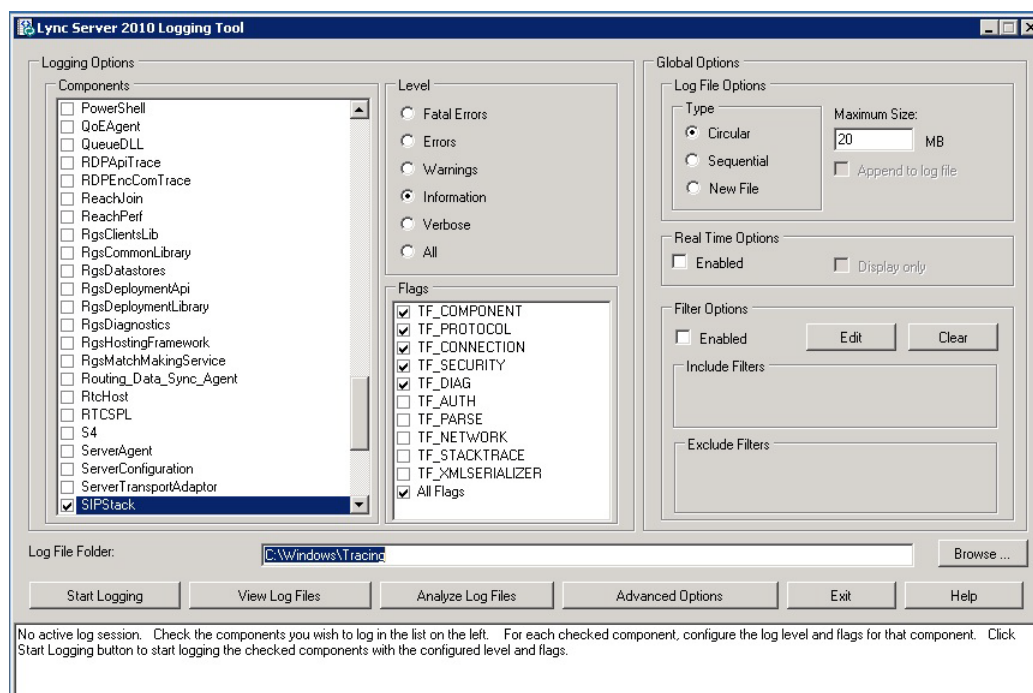
Use of Lync Logging tool

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.

On Lync

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

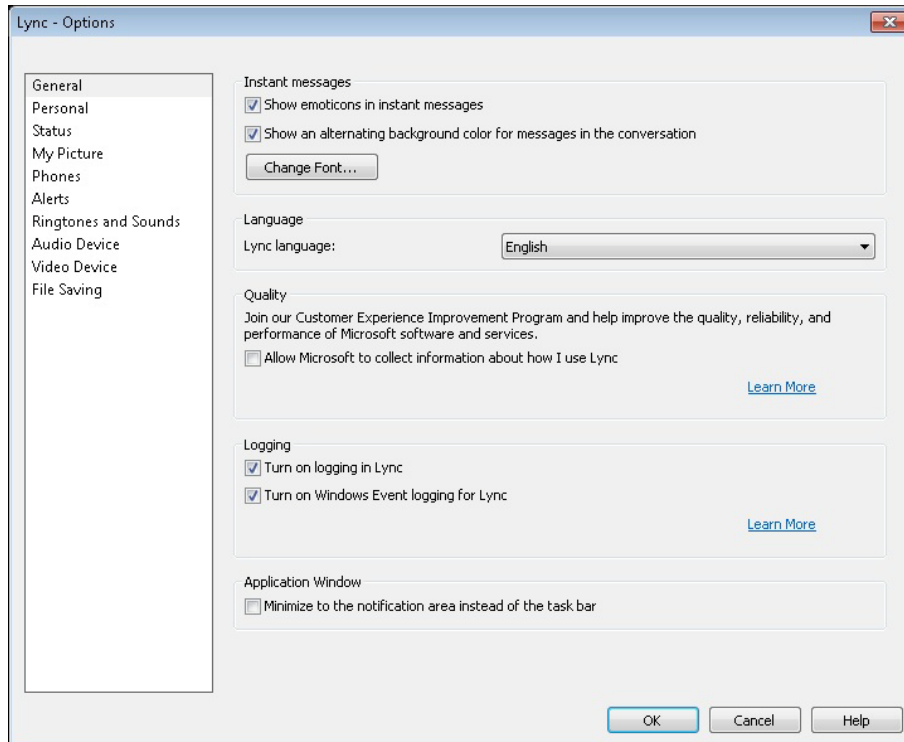


2. Select the logging option, for example SIPStack to look at SIP logs. (Details about the logging tool may be found at: <http://technet.microsoft.com/en-us/library/gg558599.aspx>.)
3. Click **Start Logging**.
4. Make the call, or perform the function that needs to be debugged.
5. Click **Stop Logging**.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

Appendix 3 – Enabling debug on Lync client

If the Lync client is not behaving as it should, then 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 – Known interoperating capabilities

SIP and H.323 endpoints making basic calls

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

Note that:

- 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.

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.

Lync client accessing Lync server through Microsoft Edge Server

When Lync registers to Lync through a Microsoft Edge Server, the sdp from Lync client needs to be specially processed by the “Lync gateway” VCS. This processing is available in the B2BUA available from VCS X7.0 when the **Enhanced OCS Collaboration** option key is loaded on the VCS.

Prior to X7.0, and without the B2BUA enabled and the **Enhanced OCS Collaboration** option key loaded, calls made from an endpoint registered to Cisco VCS to Lync client should work, but calls made from Lync client to an endpoint registered to VCS are likely to result in audio and video on the endpoint registered to VCS, but no video or audio at the Lync client.

Appendix 5 – Known interoperating limitations

Video codecs

If Lync 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 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 – in other words, 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.

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 VCS 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 into VCS.

Configure the “Lync gateway” VCS with a second zone to “To Microsoft Lync server via B2BUA”, select the *Custom* zone profile, select the same options as would be selected if the **Microsoft Office Communications Server 2007** zone profile had been selected and in addition set **Searches are automatically responded to** to *On*. Then configure one or more search rules so that calls destined for the mediation server are routed to this zone rather than to the standard “To Microsoft Lync server via B2BUA”.

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 Cisco 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.

Microsoft Server

Lync requires a 64 bit operating system; the operating system that Lync runs on must be:

- Microsoft Server 2008 SP2 64 bit or
- Microsoft Server 2008 R2 64 bit

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

If a call from Cisco 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:

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

the call will fail because Lync does not like the caller ID (From: header) being 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 6 – B2BUA registration on “Lync gateway” VCSs

The B2BUA 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 Cisco 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 Cisco 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 Cisco 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 Cisco VCS for that domain the call will be routed to Cisco 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.

Note that 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.

Note that the “Lync gateway” VCS (or VCSs) must host the presence server for the domain shared with Lync (**ciscottp.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.ciscottp.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 wishes 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.

Registered users with a cluster of Cisco VCSs

When the “Lync gateway” VCS is a cluster of Cisco VCSs, the shared domain FindMe users will be shared across cluster peers (using an algorithmic distribution scheme). Each cluster peer will register its FindMe users to Lync Server. When calls are made from Lync Server to the VCS B2BUA, Lync Server will send the call to the VCS peer that registered that user – hence the calls are statically load-shared across the VCS peers.

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.)

- It is strongly recommended 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 once the user is fully available on Lync server.

If a cluster of VCSs is used for the “Lync gateway” then TMS is required to replicate FindMe details across the cluster peers. See the relevant VCS cluster deployment guide for further details on this.

Appendix 7 – B2BUA and AM GW integration

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

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

Appendix 8 – TEL URI handling for Cisco VCS to Lync calls

If an endpoint wants to dial a telephone number rather than selecting a user from a directory, the Cisco 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>`

Cisco VCS Control can use transforms to appropriately format the telephone numbers. These transforms can either be implemented globally using **VCS 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 Bracknell UK whose telephone number is 781xxx, an extension number 1008 would need to be expanded to +441344781008.

This can be implemented 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	<i>(1...)@ciscotp\com(.*)</i>
Pattern behavior	<i>Replace</i>
Replace string	<i>+44134478\1;@ciscotp.com;user=phone\2</i>
On successful match	<i>Continue</i>
Target Zone	<i>To Microsoft Lync server via B2BUA</i>

Appendix 9 – Upgrading from non-B2BUA mode to B2BUA mode

After upgrading the Lync gateway VCS (cluster) to X7.0, the following procedure should be used to migrate from use of OCS Relay, neighbor zones and CPL to using the B2BUA and registered FindMe users.

On VCS:

1. Back up the VCS configuration: **Maintenance > Backup and restore > Create system backup file**. If using a VCS cluster, this has to be done on all cluster peers.
2. Go to **VCS configuration > Dial plan > Search rules** and delete all search rules targeting the neighbor zone(s) towards Lync.
3. Go to **VCS configuration > Zones > Zones** and delete all neighbor zones pointed towards Lync peers.
4. If previously using OCS Relay:
 - a. Go to **VCS configuration > Call Policy > Configuration** and click **Delete uploaded file**. If using a VCS cluster, this has to be done on all cluster peers. Please note that if the OCS Relay-specific CPL has been combined with other CPL, the OCS Relay-specific CPL needs to be removed from the active CPL script and the modified CPL re-loaded.
 - b. Go to **Applications > OCS Relay** and set **OCS Relay Mode** to *Off*.
5. Go to **VCS configuration > Protocols > Interworking** and set **H.323 <-> SIP interworking mode** to *Registered only*.
6. Configure the B2BUA as previously described (section “Configure the B2BUA on the “Lync gateway” VCS”).

On Lync Servers:

Make sure that no static domain routes exist from Lync to VCS for the Lync shared domain.

Appendix 10 – IP port numbers

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.

IP port numbers used between B2BUA and Lync

	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	UDP	56000 to 57000	Lync client media ports

IP port numbers used between B2BUA and VCS Expressway hosting the TURN server

	Protocol	B2BUA IP port	VCS Expressway IP port
All communications	UDP	56000 to 57000	3478

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

IP port numbers used with external Lync client

	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

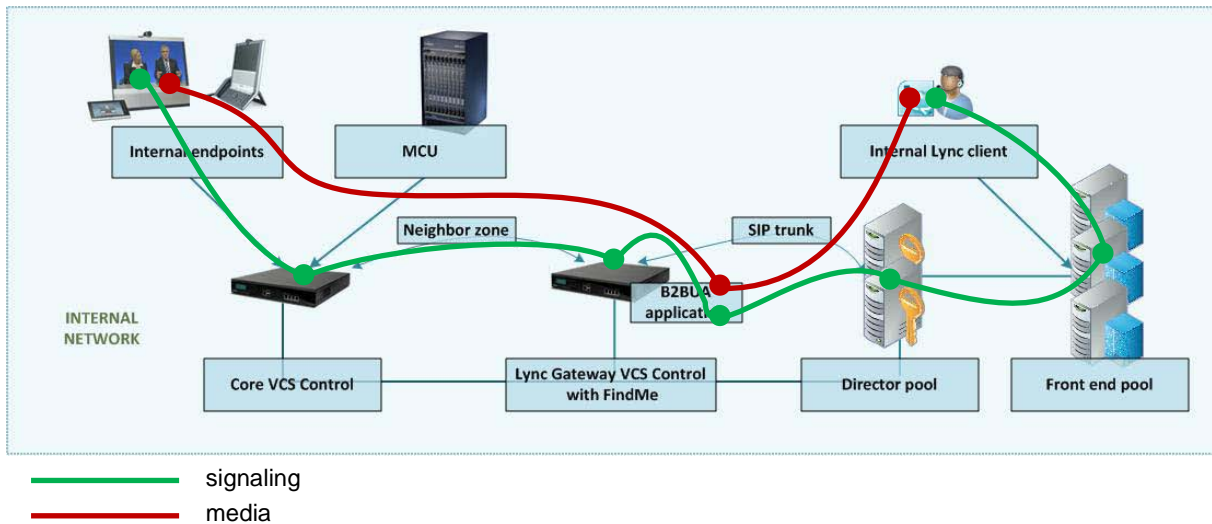
	Protocol	Lync client / Edge server	VCS Expressway
ICE messaging (STUN / TURN) if media is sent via the Expressway	UDP	3478	3478
UDP media if it is sent via the Expressway	UDP	1024-65535	60000-61799

Appendix 11 – Media paths and license usage for calls through B2BUA

Lync client call to SIP video endpoint

For a call of this type:

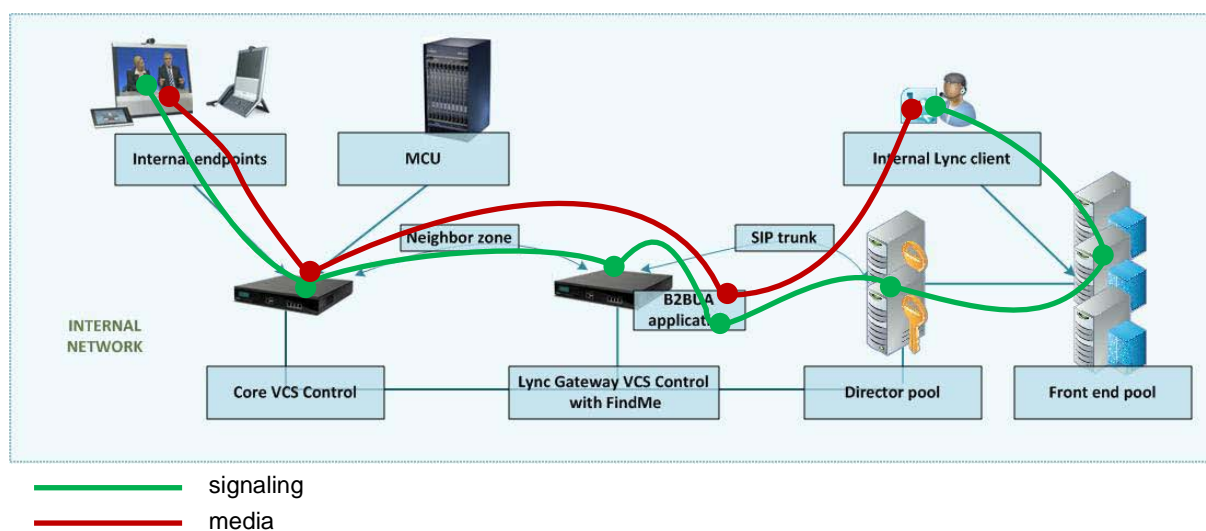
- Signaling flows through Lync, B2BUA, and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media is connected directly between the internal video endpoint and the B2BUA (as the call is SIP to SIP).
- Calls made in the opposite direction, internal video endpoint to Lync client will 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



Lync client call to H.323 video endpoint

For a call of this type:

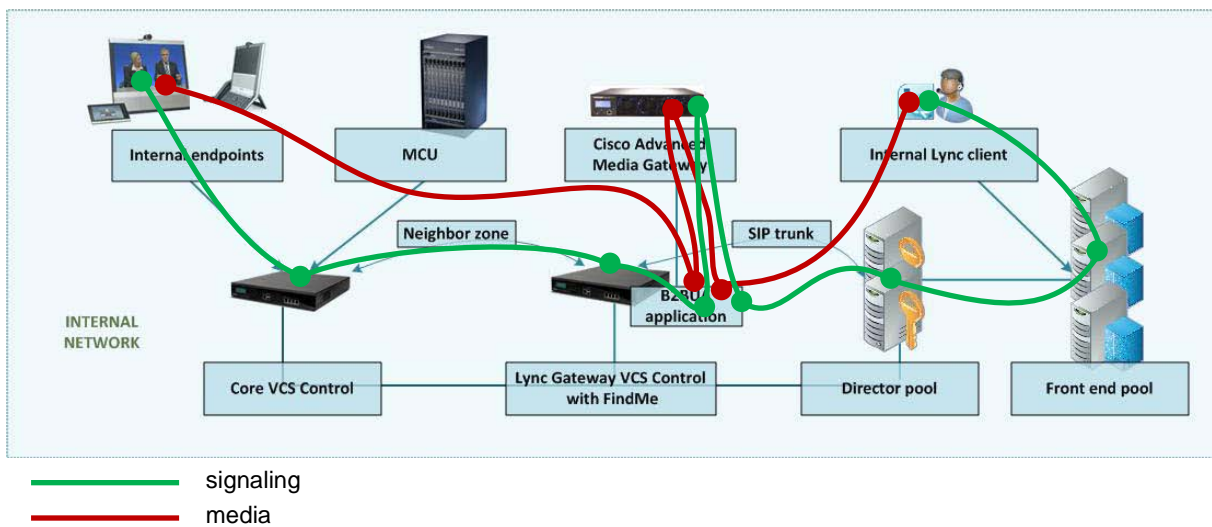
- Signaling flows through Lync, B2BUA, and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media from the internal video endpoint flows through the VCS Control and is then connected directly to the B2BUA.
- Calls made in the opposite direction, internal video endpoint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



Lync client call to a SIP video endpoint via AM gateway

For a call of this type:

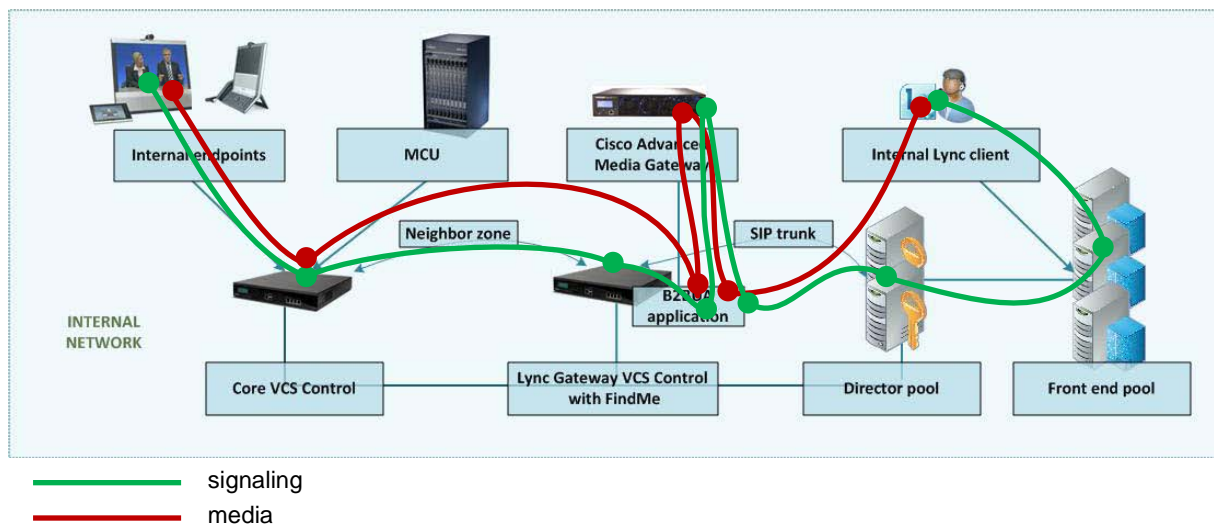
- Signaling flows through Lync, B2BUA, AM GW and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media is connected directly between the internal video endpoint and the B2BUA (as the call is SIP to SIP), and then flows to the AM GW and back to the B2BUA.
- Calls made in the opposite direction, internal video endpoint to Lync client will 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



Lync client call to H.323 video endpoint via AM gateway

For a call of this type:

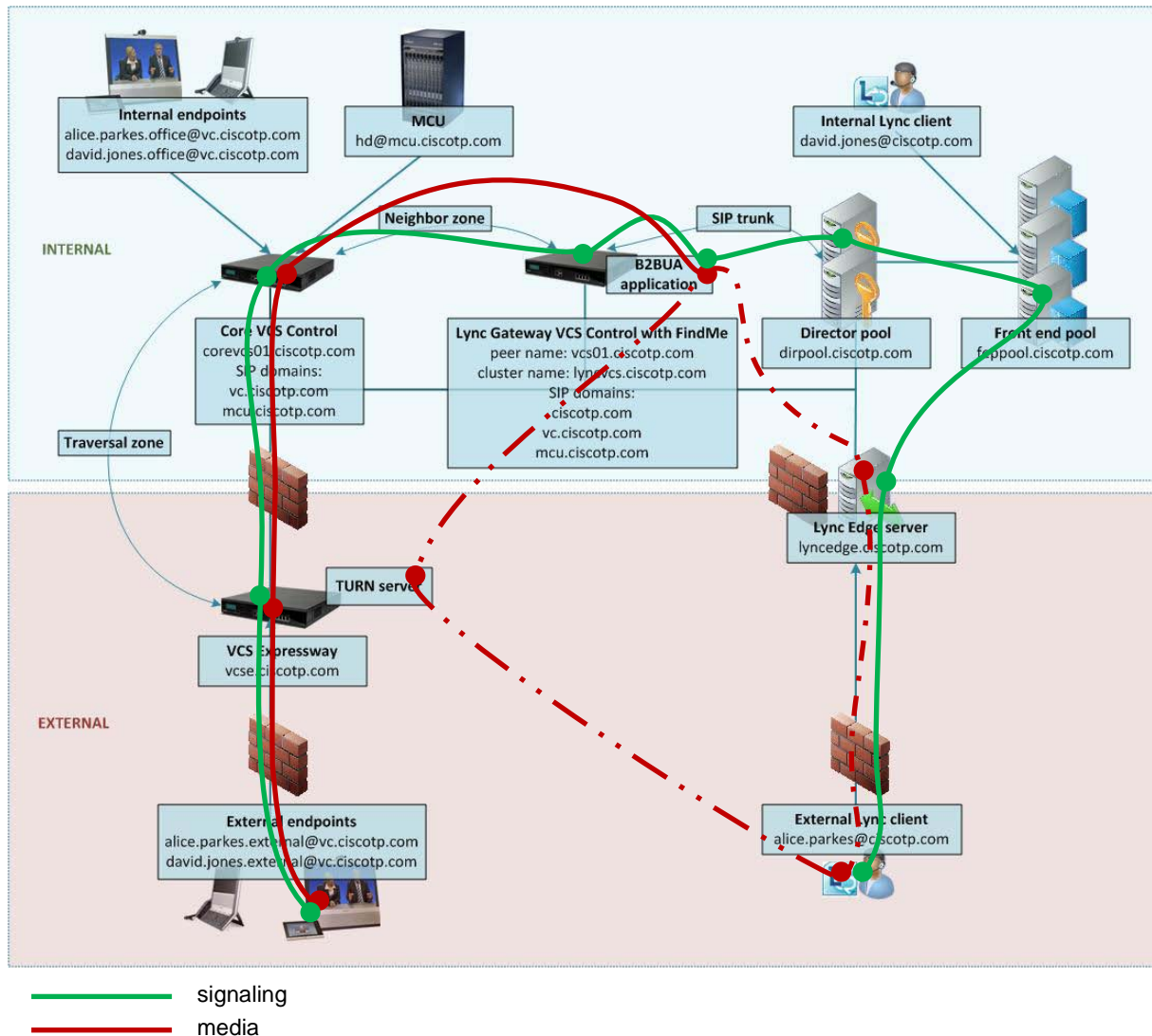
- Signaling flows through Lync, B2BUA, AM GW and VCS Control.
- Media is connected directly between the Lync client and the B2BUA.
- Media from the internal video endpoint flows through the VCS Control and is then connected directly to the B2BUA. It then flows to the AM GW and back to the B2BUA.
- Calls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



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).

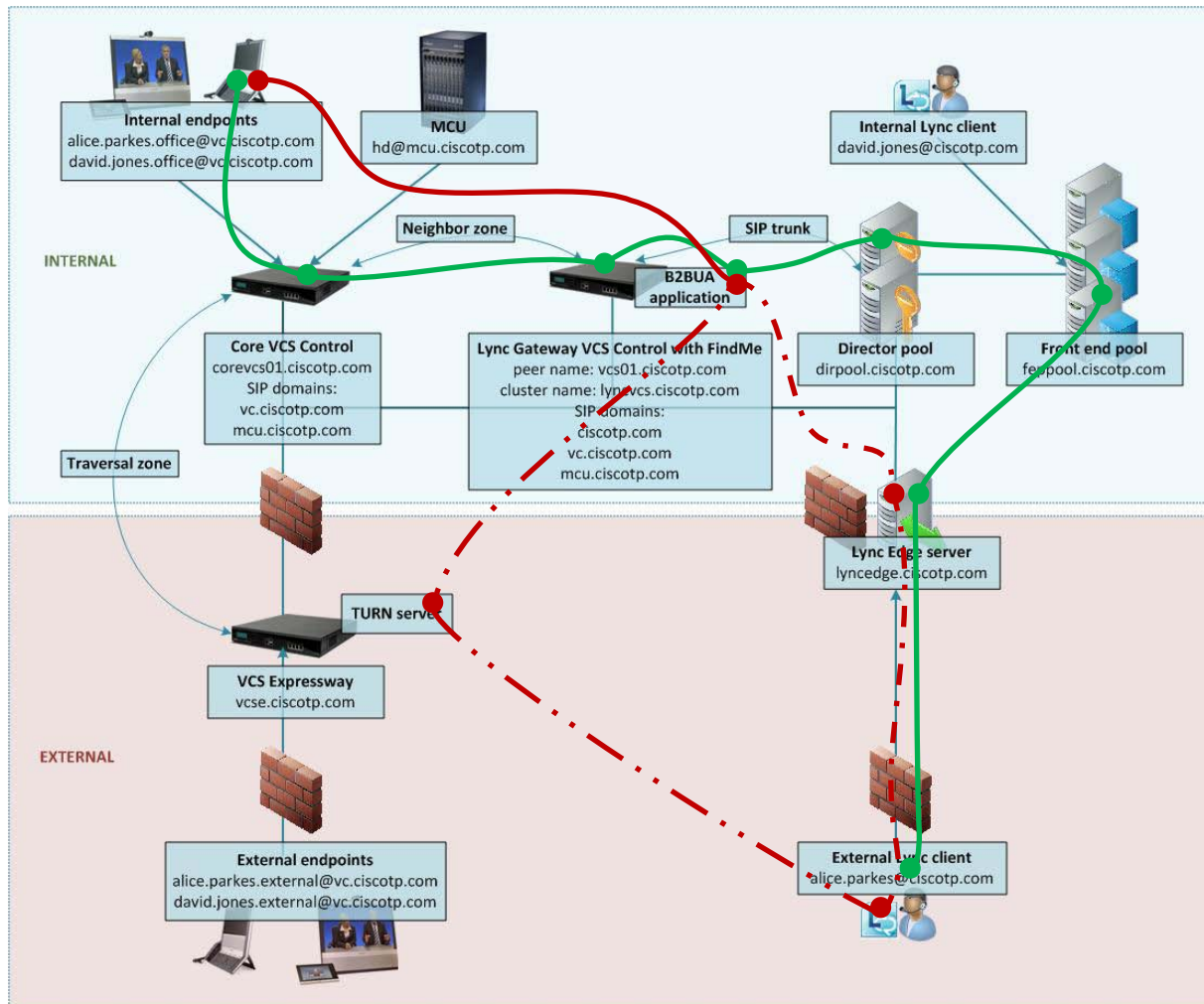
- Signaling flows through the Microsoft Edge Server, Lync, B2BUA, VCS Control and VCS Expressway.
- Media between the Lync client and the B2BUA flows either through the Microsoft Edge server or through the VCS Expressway TURN server – ICE searching is used to determine the ‘best’ path.
- Media between 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 would use the same signaling and media paths.
- Licensing
 - 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



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.
- Licensing
 - 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



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.

© 2013 Cisco Systems, Inc. All rights reserved.