Microsoft Lync 2010 and Cisco VCS

Cisco TelePresence Deployment Guide

Cisco VCS X6.1
Microsoft Lync Server 2010

D14269.05

May 2011

Contents

Introduction

Objectives and intended audience

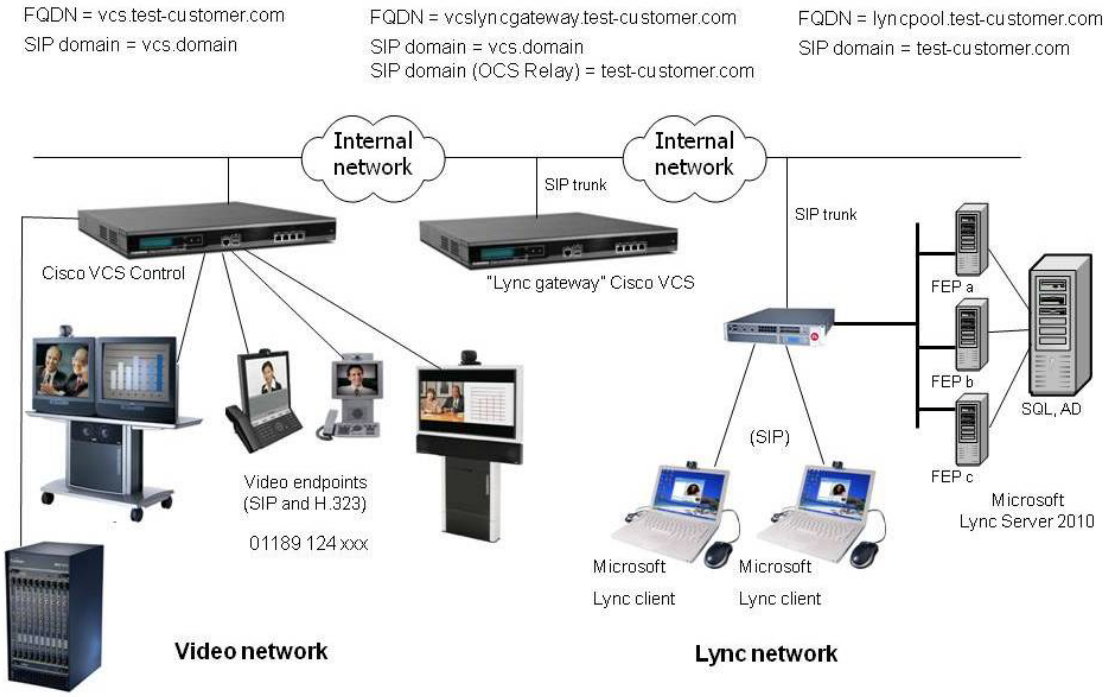
This deployment guide provides instructions on how to configure a Cisco TelePresence Video Communication Server (Cisco VCS) Control version X6.1 and Microsoft Lync Server 2010 to interwork.

This guide also highlights the capabilities and limitations of interoperation of Cisco VCS Control and Lync Server.

Note: For information about connecting Cisco VCS to Microsoft OCS, see 'Cisco VCS deployment guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control (X5.2) - D14269.04'.

Deployment scenario

A company is introducing a Lync system into their network to provide Microsoft Lync Clients on everyone's desk to supply 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, and for Lync to see the presence of the video endpoints.



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

This deployment guide describes how to connect Lync Server and a Cisco VCS Control using a SIP trunk across an IP network. The example presented uses the following setup:

- A new 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 Server.
- The Lync Server's SIP domain is **test-customer.com**.

Note that the SIP domain for Lync Server need not be the same as the AD domain of Lync users (the Lync user's 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 **vcs.domain**, and can, if desired, also include devices registering with the domain **test-customer.com**.
- Endpoints registered to the Video Network may be SIP or H.323 endpoints; they must register with an ID in the format name@domain, where domain is a domain hosted on the Video Network (for example **vcs.domain**, or if desired **test-customer.com**).
- Lync clients registered to Lync Server are identified by URIs, for example:
  - User1 with a URI user1@test-customer.com
  - User2 with a URI user2@test-customer.com
- Endpoints registered to the Video Network are identified by URIs, frequently including the location of the endpoint, for example:
  - User2 with an h.323 ID user2.office@vcs.domain
  - User2 with a SIP URI user2.external@vcs.domain
  - User1 with an H.323 ID user1.office@vcs.domain
  - User1 with a SIP URI user1.external@vcs.domain
- When using OCS Relay functionality on Cisco VCS, together with Lync Server:
  - The "Lync Gateway" Cisco VCS Control supports the **test-customer.com** domain for OCS Relay FindMe™ users.
  - OCS Relay FindMe™ user names are constructed in exactly the same way as Lync URIs, for example:
    - User1 with a URI user1@test-customer.com
    - User2 with a URI user2@test-customer.com
  - These OCS Relay FindMe™ users (with the same domain as Lync Server) register to Lync Server as though they are Lync clients. If a corresponding Lync client also exists on a PC, the Lync endpoint on the PC and the Video endpoints specified in the FindMe™ will ring simultaneously when called, whether called from an endpoint communicating with Cisco VCS, or whether called from an endpoint communicating with Lync Server.
  - These OCS Relay FindMe™ users can specify single or multiple endpoints as primary devices to call; the primary devices can be located anywhere in the Video Network or be accessible via the Video Network.
- "Available", "off-line" and "in-call" presence may be observed by Lync clients for OCS Relay FindMe™ users registered by the "Lync Gateway" Cisco VCS (when OCS Relay is enabled). "Available" and "off-line" presence may be observed by Lync clients for other devices or FindMe™ users which provide presence information in the Video Network.
- It is assumed that the "Lync Gateway" Cisco VCS Control is running X6.1 code (or later) and has at least the following option keys applied:
  - H323-SIP interworking
  - Registrations
  - Traversal calls
  - Non-traversal calls
  - User Policy (FindMe™) - optional but recommended; necessary to take advantage of the OCS Relay functionality.
- Traversal call and non-traversal call option keys are both needed on the "Lync Gateway" Cisco VCS Control
  - Lync Server to SIP calls that do not use encryption are non-traversal calls
  - Lync Server to H.323 calls are traversal calls as they need to be interworked from SIP RTP to H.323 RTP

- The version of operating system that Lync Server runs on must be the 64-bit editions of the following operating systems:
  - Windows Server 2008 R2 Standard/Enterprise/Datacenter operating system
  - Windows Server 2008 Standard/Enterprise/Datacenter operating system with Service Pack 2 (SP2)

Why add a "Lync Gateway" Cisco VCS Control?

The "Lync Gateway" Cisco VCS is an interface between an existing working video network and the Microsoft Lync system. There are a number of settings that need to be configured on the "Lync Gateway" that are different from the recommended configurations for standard video routing Cisco VCSs. For instance the "Lync Gateway" Cisco VCS requires that **Call routed mode** be set to *Always*, as the Cisco VCS has to modify the Lync Server SIP signaling to make it suitable for standard video endpoints, MCUs etc. The knock-on effect of this is that call licenses are always used on this "Lync Gateway" Cisco VCS. It also requires interworking to be *On* rather than *Registered only* which can cause calls to be interworked when they need not.

Having the separate "Lync Gateway" Cisco VCS and making it the video network presence server also allows this Cisco VCS or cluster of Cisco VCS peers to handle the subscriptions and presence requests from Lync Server for video network users. Handling them in the "Lync Gateway" prevents the Lync Server presence requests being "spammed" into the existing video network and adversely affecting the run time operation of the previously working system.

OCS Relay requires dedicated CPL. If CPL is required anywhere else in the network (for example, to limit which calls are allowed to be routed to ISDN gateways or other resources) it is hard to merge different CPL scripts.

For FindMe™ to re-write the caller ID, 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" OCS Relay FindMe™ users registered to the Lync Server, and
- a single FQDN (though this may have a round robin DNS address to support a cluster of Cisco VCSs for resilience) for calls to endpoints accessible via a static domain route defined in Lync Server

If Lync Server supports multiple domains, all domains can be handled by a single "Lync gateway" Cisco VCS / cluster, or one "Lync gateway" Cisco VCS / cluster can be used for each domain.

- If different Lync Server domains are handled by different "Lync gateway" Cisco VCSs or Cisco VCS clusters, take care to ensure that each "Lync gateway" Cisco VCS or Cisco VCS cluster is authoritative for the presence information that is required for the OCS Relay FindMe™ users and all endpoints that are referenced by those FindMe™ entries.
- If one "Lync gateway" Cisco VCS or Cisco VCS cluster is used, note that only one domain can be handled by OCS Relay.

Having a dedicated "Lync gateway" Cisco VCS or Cisco VCS cluster also limits the number of trusted devices that need to be configured in Lync Server.

Although in the example, nothing is shown registered to the "Lync gateway" Cisco VCS, it is often a good place to register an MCU if significant numbers of Lync callers are going to be sharing conferences with standard video endpoint users.

Small test and demo networks?

For small test and demo networks, video endpoints may be registered to the "Lync gateway" Cisco 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 and 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" Cisco VCS connected to video network approach. This is achieved by adding video network Cisco VCSs and neighboring them (directly, or indirectly through other Cisco VCSs) to the Lync gateway" Cisco VCS. Endpoints can be added to the video network Cisco VCSs and endpoints and other devices then gradually migrated off the "Lync gateway" Cisco VCS onto the video network Cisco VCSs.

Features and capabilities

Cisco VCS works equally well with Lync Server 2010 Standard edition and Lync Server 2010 Enterprise edition.

Cisco VCS X6.1 and Lync Server 2010

- Cisco VCS can be in:
  - the same domain as Lync Server
  - a separate domain from Lync Server
  - the same and separate domains from Lync Server
- Same domain is used by FindMe™ entries on Cisco VCS, which register as Lync devices on Lync Server (using OCS Relay):
  - domain static route(s) are set up on Lync Server to route calls to Cisco VCS's separate domain(s)
- Presence is only supported Cisco VCS to Lync Server:
  - "Off-line" and "Available" are "In-call" are supported for "same domain" OCS Relay FindMe™ users
  - "Off-line" and "Available" (not "In-call") are reported for "separate domain" users
  - "Off-line" and "Available" (not "In-call") are reported for "same domain" users which are not OCS Relay FindMe™ users
- Passing Lync presence to devices registered to Cisco VCS is not supported.
- Same domain calls Lync Server to Cisco VCS can be made to "same domain" OCS Relay FindMe™ users and also to other devices with that domain which are routable from the "Lync gateway" Cisco VCS.
- Lync Server accepts and handles call hold (and resume) requests.
- Lync clients can be joined into a Multiway™ conference.
- Lync devices registering through a Microsoft Edge Server and then calling Cisco VCS registered endpoints is not supported:
  - Cisco VCS registered devices calling Lync Server registered devices will work, but Lync devices registering through an Edge server get no video if they call a Cisco VCS registered endpoint
- Calls to Microsoft Mediation Servers work from endpoints in the Cisco VCS Video Network for SIP initiated calls, but do not work for interworked H.323 initiated calls.
- A single Cisco VCS can communicate to a pool of Lync Server FEPs via a hardware load balancer. Lync systems may use hardware load balancers for resilience and capacity. Microsoft Lync Server 2010 introduces DNS load balancing, a software solution that reduces the administration overhead for load balancing on a network. DNS load balancing balances the network traffic that is unique to Lync Server 2010, such as SIP traffic and media traffic.
- A "lack of video on Lync" problem occurs due to Lync clients not displaying video until a full video frame has been received. A full frame is sent either when requested by a fast picture update

request, or when the video stream is paused and then re-started. Lync does not request fast picture updates.

- latest versions of endpoints recognize when they are connected in a SIP call to a Lync Server and will send appropriate full frames to allow Lync to display video
- MCU code 3.1 and later recognizes when it is connected in a SIP call to an Lync Server and will send appropriate full frames to allow Lync to display video
- third party SIP endpoints are unlikely to allow video to be displayed on Lync

- Lync Server can be connected to a cluster of Cisco VCS peers.
- Lync Director is supported.
- Media encryption (SRTP) is supported when TLS is used between Cisco VCS and Lync Server and the **Enhanced OCS collaboration** option key is added to the Cisco VCS.

Note: To use an MCU with Lync Server, register the MCU to Cisco VCS; Cisco VCS handles the protocol differences on behalf of the MCU.

Summary of configuration process

This document describes how to configure both the Lync Server and the Cisco VCS Control (version X6.1) 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.
- 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 Server.
- 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.

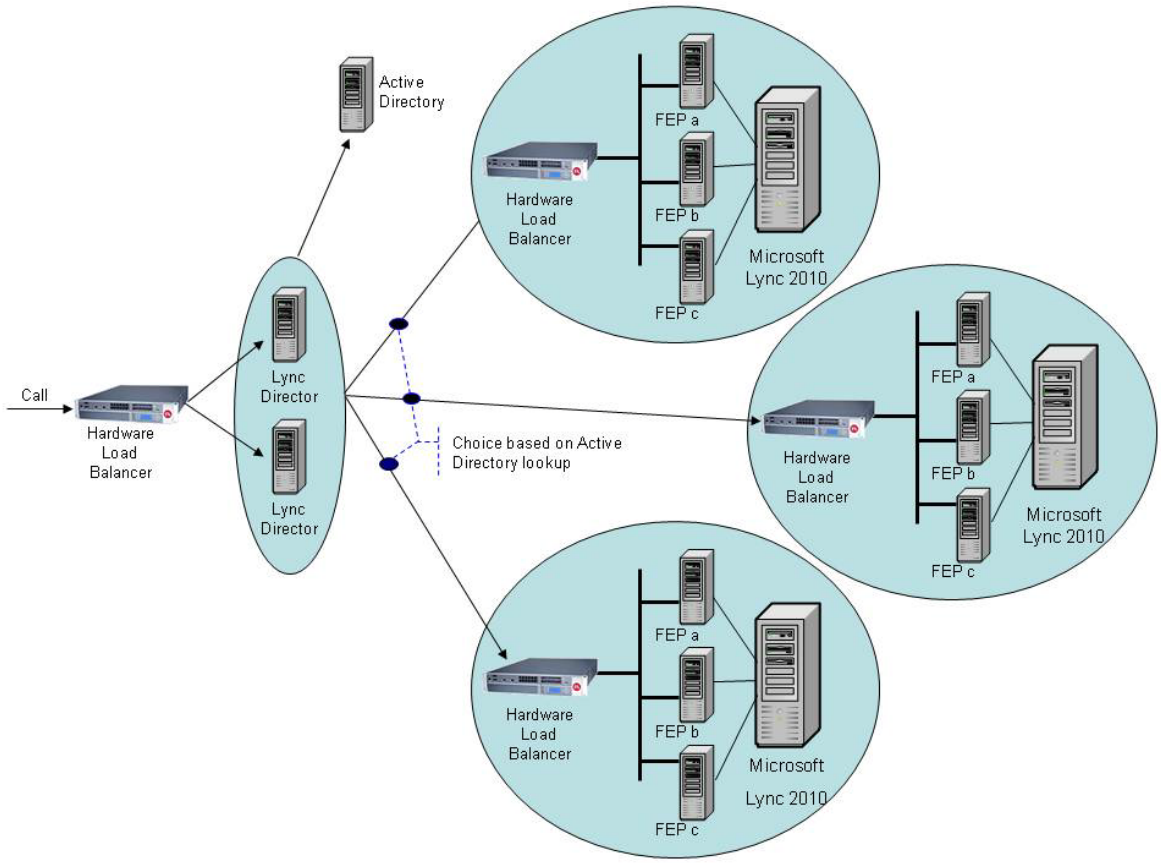
An advanced configuration stage (OCS Relay configuration of “Lync gateway” Cisco VCS) is also documented for systems running Cisco VCS X6.1 or later and Lync Server 2010, which enables Cisco VCS to register FindMe™ users as though they are Lync clients, so that:

- “In-call” as well as “Available” and “Off-line” can be seen for these FindMe™ users.
- Lync Server will fork calls to FindMe™ users at the same time as Lync users with the same name, so that calls can be taken on Lync or a video endpoint, as desired.

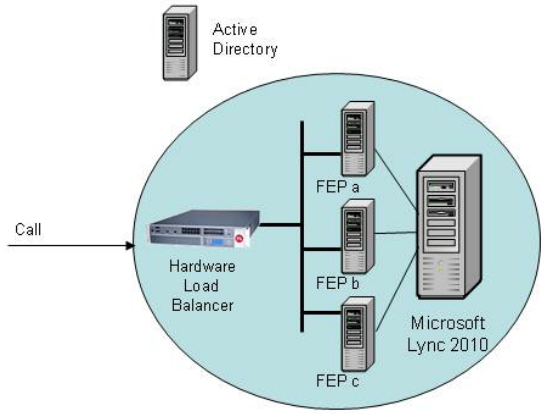
Different structures for Lync Server

Lync systems have a number of building blocks, and so Lync systems may be constructed in many ways.

A full scale Lync Server deployment is likely to use Lync Director, Hardware Load Balancers (HLBs), Front End Processors (FEPs) in enterprise pools, and a redundant AD server. For example:



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.



The simplest deployment will have AD and FEP on a single server, with no Hardware Load Balancer needed as Lync is a single server.

Lync Server deployments may also contain Edge servers to allow Lync clients to register from outside the local network through the Edge server to Lync Server. This is not shown in the diagrams above, because currently the Cisco VCS implementation only supports interoperation with Lync devices directly registered to Lync Server.

Lync Server should be configured so that:

1. If the Lync system 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” Cisco VCS(s)
   - Lync Directors should route Video network SIP domain(s) (and the Lync Server SIP domain) to the “Lync Gateway” Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)
   - FEPs will route traffic that they don’t know how to route to Director, and Director will route the calls to the Cisco VCS
2. If the Lync system 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 Director should trust the “Lync Gateway” Cisco VCS(s)
   - Lync Director should route Video network SIP domain(s) (and the Lync SIP domain) to the “Lync Gateway” Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)
   - FEPs will route traffic that they don’t know how to route to Director, and Director will route the calls to the Cisco VCS
3. If the Lync system 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) to route calls for the video network directly to The “Lync Gateway” Cisco VCS(s) – configuring the pool ensures that the same configuration is applied to every FEP in the pool:
   - The FEP pools should trust the “Lync Gateway” Cisco VCS(s)
   - All FEP pools should route calls to the “Lync Gateway” Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)
4. If Lync Server is a single FEP then that FEP should be configured to route calls for the Video Network directly to the “Lync Gateway” Cisco VCS(s):
   - the single FEP should trust the “Lync Gateway” Cisco VCS(s)
   - the single FEP should route calls to the “Lync Gateway” Cisco VCS cluster FQDN (or if only a single Cisco VCS, the FQDN of that Cisco VCS)

Cisco VCS should be configured such that:

5. If the Lync system is fronted by a Hardware Load Balancer in front of Lync Directors then the “Lync Gateway” Cisco VCS(s) should be configured to route calls for Lync through the Hardware Load Balancer in front of the Lync Directors, and receive calls from either of the Lync Directors:
   - the “Lync Gateway” Cisco VCS(s) need to neighbor to the Hardware Load Balancer
   - the “Lync Gateway” Cisco VCS(s) also need to have another neighbor zones that contain the Peer addresses of both Lync Directors
   - the Hardware Load Balancer neighbor zone is pointed to by the Search rules that route calls to Lync
   - the neighbor zones to the other FEPs must also have their zone profile set to *Microsoft Office Communications Server 2007* but must not be referenced by any search rules
6. If the Lync system is fronted by a Lync Director then the “Lync Gateway” Cisco VCS(s) should be configured to route calls for Lync through the Lync Director, and receive calls from the Lync Director:
   - configure the Lync Director as the Peer address in the neighbor zone
7. If the Lync system has no Lync Director but a Hardware Load Balancer in front of Front End Processors then the “Lync Gateway” Cisco VCS(s) should be configured to route calls for the Video Network directly to the Hardware Load Balancer, and receive calls from any of the FEPs:

- the “Lync Gateway” Cisco VCS(s) need to neighbor to the Hardware Load Balancer
- the “Lync Gateway” Cisco VCS(s) also need to have 1 or more neighbor zones that contain the Peer addresses of all the Lync FEPs
- the Hardware Load Balancer neighbor zone is pointed to by the search rules that route calls to Lync Server
- the neighbor zones to the other FEPs must also have their Zone profile set to Microsoft Office Communications Server 2007 but must not be referenced by any search rules

8. If Lync Server is a single FEP then the “Lync Gateway” Cisco VCS(s) should be configured to route calls for Lync Server to the single FEP directly, and receive calls from the FEP:
   - configure the single FEP as the Peer address in the neighbor zone

For more details about Lync Director, see “Appendix 14 – Cisco VCS and Microsoft Lync Director’.

Prerequisites prior to configuring Cisco VCS and Lync Server to interoperate

Before configuring the Video Network and the Lync system to interwork, make sure that the following is operational:

- Lync Server is configured and operational and access is available to Active Directory for managing users.
- The FQDN of Lync Server (enterprisepool.test-customer.com in this example) is resolvable via the DNS server that Cisco VCS Control is configured to use. DNS servers should be the same for VCS Control and Lync Server.
- The FQDNs of each of the “Lync gateway” Cisco VCSs and the FQDN of the “Lync gateway” cluster must be resolvable via the DNS server.
- The video endpoints registered to the Video Network must support the H.263 video codec – this is the only video codec which is common to Lync clients and standard video endpoints.
- If TLS is to be used (recommended) ensure that the DNS server supports reverse DNS lookup (often supported using PTR records).
- Topology Validation of the Front End Servers on all Lync Directors and Lync Server FEPs must show no errors. (Topology Validation Tool can be found in the Resource Toolkit for Lync.)

Microsoft Lync Server 2010

Topology Validation Results

Topology	C:\Users\administrator.LYNC\AppData\Local\Temp\2\TopologyValidator\TV_SquidTopology.xml
Target Pool FQDN	lyncfe01.lync.lab
Test Users	sip:user3@lync.lab [Registrar Pool: lyncfe01.lync.lab] sip:user2@lync.lab [Registrar Pool: lyncfe01.lync.lab]
Overall Result	Total:17 Pass:13 Fail: Skip:2 Not Applicable:1
Logs	Click here

Test Case	Result	Start Time	Finish Time	Test Users
All Tests - lyncfe01.lync.lab	Success	17/05/2011 11:38:22	17/05/2011 11:39:49	
Service Installation Check	Success	17/05/2011 11:38:22	17/05/2011 11:38:22	
Register	Success	17/05/2011 11:38:22	17/05/2011 11:38:37	sip:user3@lync.lab
Peer to Peer IM	Success	17/05/2011 11:38:37	17/05/2011 11:38:44	sip:user3@lync.lab sip:user2@lync.lab
Group IM	Success	17/05/2011 11:38:44	17/05/2011 11:38:54	sip:user3@lync.lab sip:user2@lync.lab
Presence	Success	17/05/2011 11:38:54	17/05/2011 11:38:58	sip:user3@lync.lab sip:user2@lync.lab
Peer to Peer AV Conference	Success	17/05/2011 11:38:58	17/05/2011 11:39:10	sip:user3@lync.lab sip:user2@lync.lab
AV-Conference	Success	17/05/2011 11:39:10	17/05/2011 11:39:17	sip:user3@lync.lab sip:user2@lync.lab
Peer To Peer PSTN Call	Success	17/05/2011 11:39:17	17/05/2011 11:39:20	sip:user3@lync.lab sip:user2@lync.lab
PSTN Outbound Call	Skipped	17/05/2011 11:39:20	17/05/2011 11:39:20	
Address Book	Success	17/05/2011 11:39:20	17/05/2011 11:39:26	sip:user3@lync.lab
Location Policy	Success	17/05/2011 11:39:26	17/05/2011 11:39:29	sip:user3@lync.lab
Location Information Service Configuration	Success	17/05/2011 11:39:29	17/05/2011 11:39:33	sip:user3@lync.lab
Dial-In Conferencing	Success	17/05/2011 11:39:33	17/05/2011 11:39:36	sip:user3@lync.lab
Address Book Web-Query	Success	17/05/2011 11:39:36	17/05/2011 11:39:39	sip:user3@lync.lab sip:user2@lync.lab
ClientAuth	Success	17/05/2011 11:39:39	17/05/2011 11:39:49	sip:user3@lync.lab
Federation	Not Applicable			
Phone Bootstrap	Skipped	17/05/2011 11:39:49	17/05/2011 11:39:49	

Enabling calls between endpoints registered on Cisco VCS Controls in the video network

Video network Cisco VCS Control configuration summary

The configuration of the Cisco 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 2 items are configured:

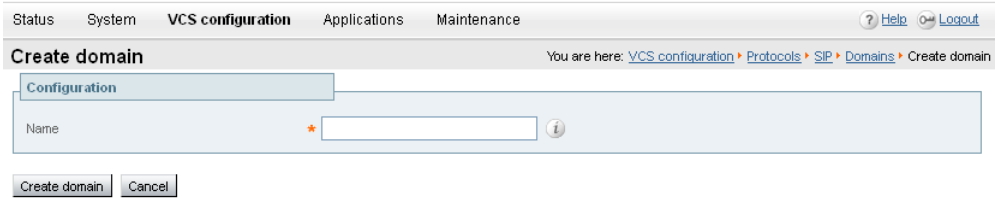
- SIP domain of the video network - needed for SIP registration and presence handling.
- Default links between the Cisco VCS Control's zones.

Note: In small test and demo networks this configuration is carried out on the same Cisco VCS that is the "Lync Gateway" Cisco VCS

Ensure that the SIP domain of Cisco VCS Control(s) in the video network are configured

SIP endpoints register with the Cisco VCS Control with a URI in the format **user-id@sip-domain**. The Cisco 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. Click **New**.
3. Set **Name** to, for example, *vcs.domain*.
4. Click **Create domain**.



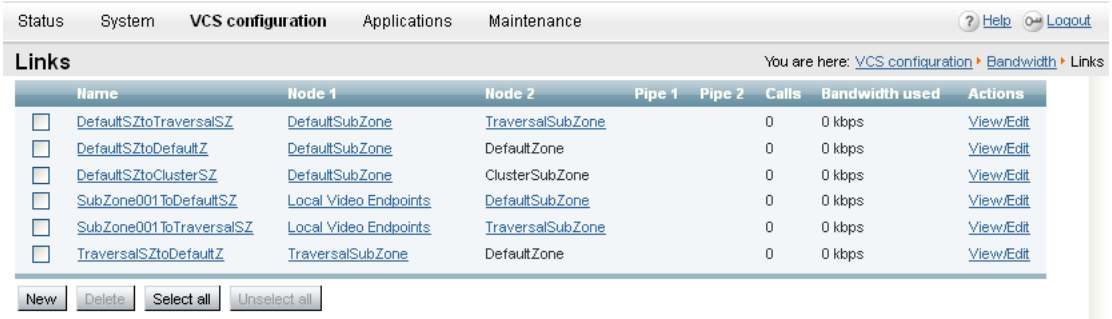
Ensure that default links between the Cisco VCS Control's zones are set up

For a call to succeed there must be appropriate links between Zones.

Links must exist from:

- Default Subzone to Traversal Subzone
- Default Subzone to Default Zone
- Default Subzone to Cluster Subzone (*this is required even if Cisco VCS is not part of a cluster)*
- Traversal Subzone to Default Zone

Check these on the **Links** page (**VCS configuration > Bandwidth > Links**).



If any links are missing, log onto the command line interface and execute the command:
`xcommand DefaultLinksAdd`

Lync Server configuration

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

Registering endpoints to the Video Network

Endpoint configuration.

For H.323, configure the endpoints as follows:

- H.323 ID (for example, user2@VCS.domain)
- H.323 Call Setup = Gatekeeper
- Gatekeeper IP address = IP address of Cisco VCS Control

For SIP, configure the endpoints as follows:

- SIP Address (URI) (for example, user1@VCS.domain)
- Server Address (Proxy address) = IP address of Cisco VCS Control

Confirming registrations

Registration status can be confirmed on the **Registrations** page (**Status > Registrations**).

By default the Cisco VCS Control accepts all registrations to SIP domains configured in the Cisco VCS Control. It is possible to limit registrations by explicitly allowing or denying individual registrations (see the Cisco VCS Configuration section of the Cisco 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 Cisco VCS Control (**Status > Calls > History**).

Enabling calls between Lync clients registered on Lync Server

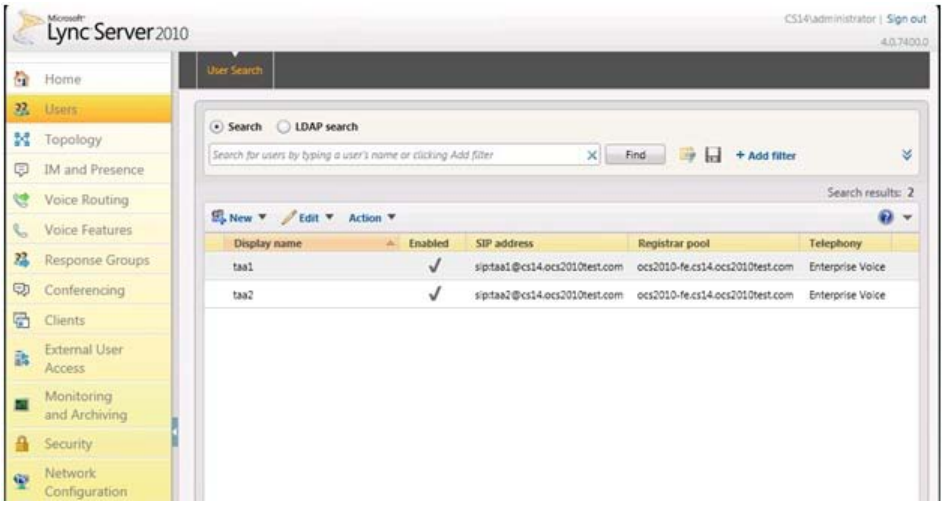
Cisco VCS Control configuration

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

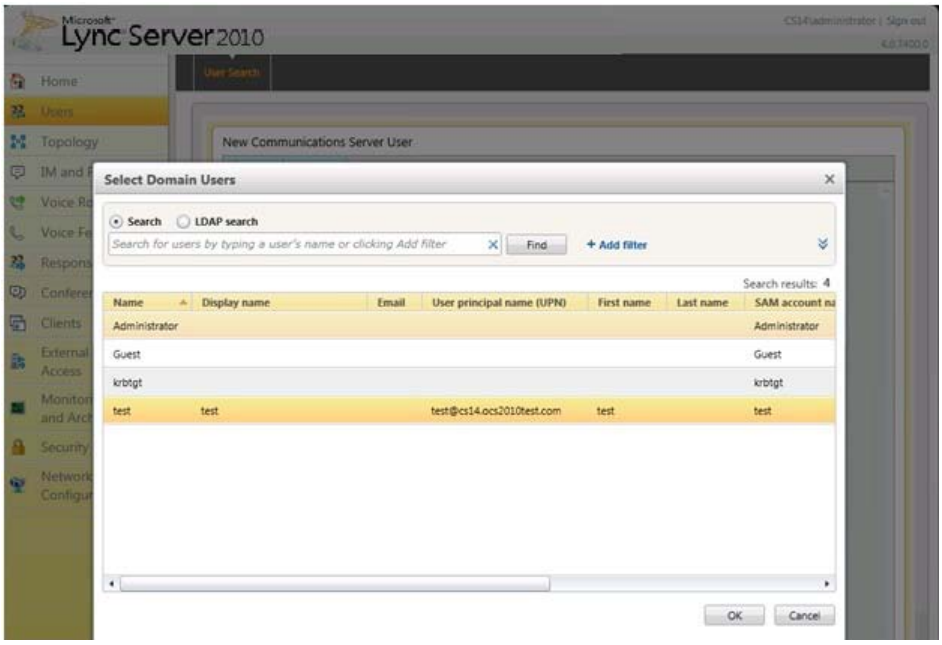
This can be done both by Communication Server Control Panel (CSCP) and Communication Server Power Shell (CSPS) commands.

On Communication Server control panel go to the **Users** menu: you can see users already enabled for communication server.

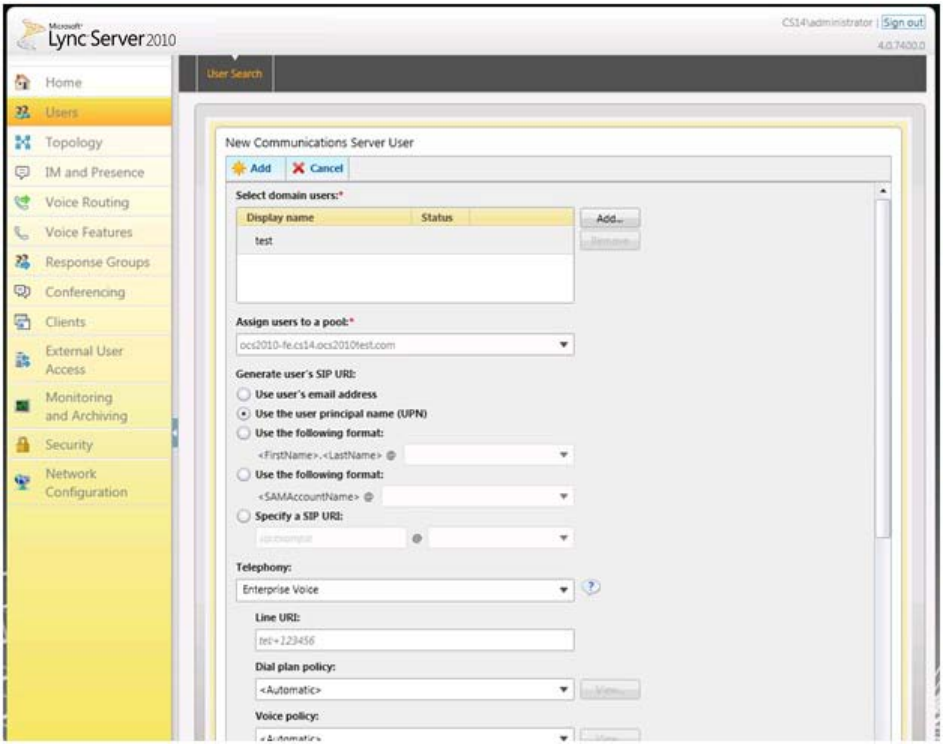


To add a new user:

1. Select **New > User**.
2. Select **Add**.
3. Find and select the user 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.



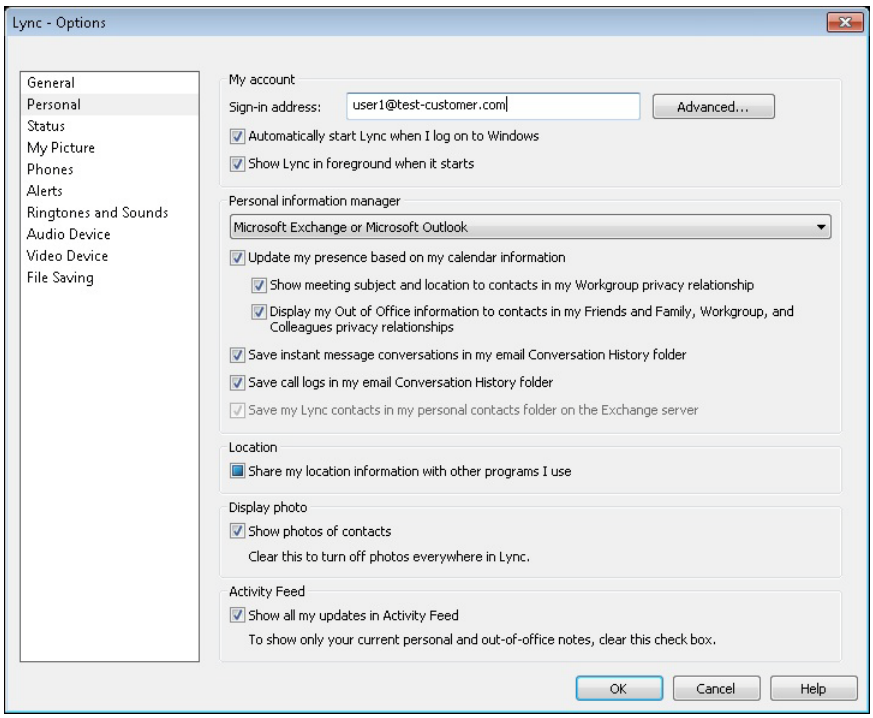
This can be done in single command by CSPS using the command “`enable-csuser`”. For example:

```
enable-csuser -identity "test1" -registrarpool "lyncpool01.test-
customer.com" -sipaddress sip:user1@test-customer.com
```

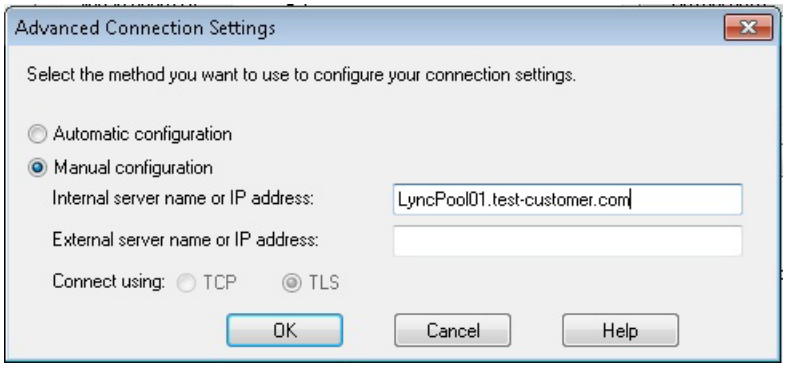
Registering Lync clients to the Lync Server

Lync client configuration

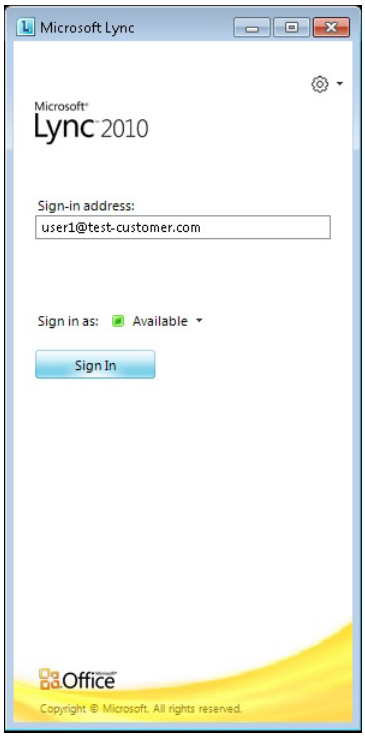
1. Install Lync client.
2. From the menu, click on the **icon > Personal > Sign-In address…**
3. Set up **Sign-in address** as required. This is the SIP URI of the Lync; if this user also has video endpoints on the Video network, this URI will be the same URI as that configured as the OCS Relay FindMe™ user ID (set up later), for example user1@test-customer.com.



4. Click **Advanced**.



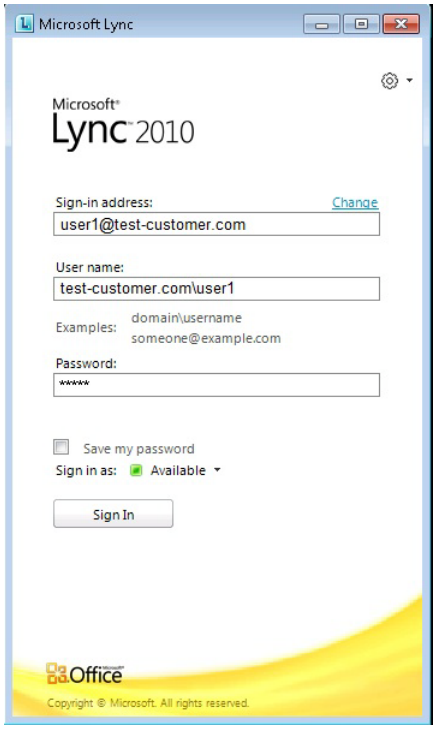
5. In a production environment ensure **Automatic configuration** is selected.
   If this proves not to work, select **Manual configuration** and set **Internal server name or IP address** to the FQDN of the Lync server.
6. Click **OK** to return to the **Options** dialog.
7. Click **OK** to return to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



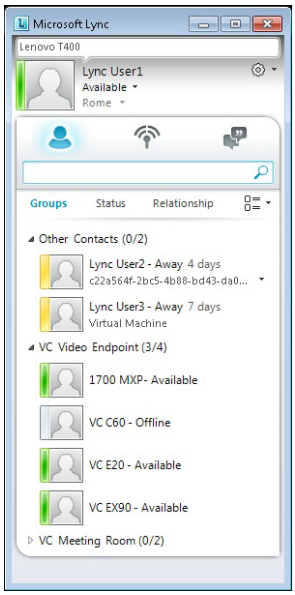
8. Click **Sign In**.
9. **User name** is the Active Directory name of the user. This may or may not be the same as the sign in address.

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 lync.lab\user1 instead of user1@lync.lab

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



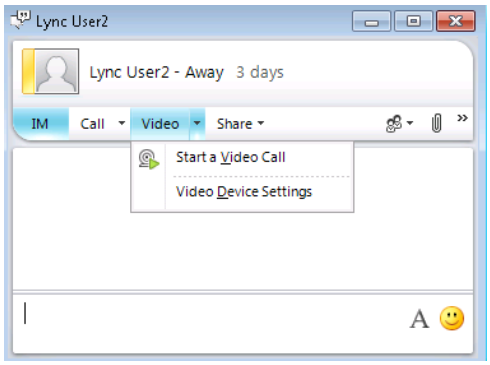
11. Click **Sign In**.



Testing the configuration

To make a video call between Lync endpoints:

1. Double-click on the buddy you want to call.



2. Click **Start a Video Call**.
3. Answer the call on the receiving Lync Client.

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

This is configured in 4 stages:

1. Video Network Cisco VCS Control Configuration
2. “Lync gateway” Cisco VCS Control configuration (1)
3. Lync Server Configuration
4. “Lync gateway” Cisco VCS Control configuration (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” Cisco VCS (cluster).
2. Set up a Search rule to route calls with the Lync Server domain to the “Lync gateway” Cisco VCS (cluster).

Note: In small test and demo networks this configuration is not necessary - the video network Cisco VCS is the “Lync Gateway” Cisco VCS. Go to ‘“Lync gateway” Cisco VCS Control configuration (1)’ on page 24.

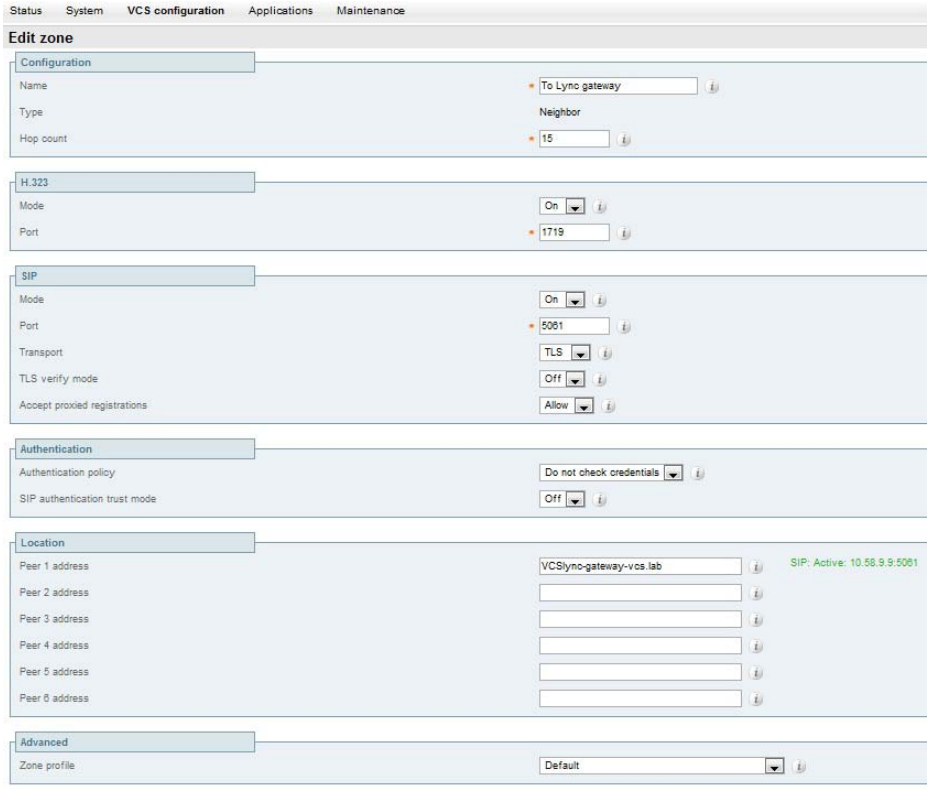
Set up a neighbor zone to the “Lync gateway” Cisco VCS (cluster)

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

Name	An appropriate name, for example “To Lync Gateway”
Type	*Neighbor*
SIP mode	*On*
SIP port	5061 (or the value that is the same as that configured on the “Lync gateway” Cisco VCS for TLS mode SIP)
SIP transport	*TLS*
H.323 mode	*On*
TLS verify mode	*Off*
Accept proxied registrations	*Deny*
Authentication Policy	*Do not check credentials*
SIP authentication trust mode	*On*
In the Location section: Peer 1 address	IP address or FQDN of the “Lync gateway” Cisco VCS (or the 1st Cisco VCS in the “Lync gateway” Cisco VCS cluster)
In the Location section: Peer 2 address to Peer 6 address	IP address or FQDN of the 2nd to 6th “Lync gateway” cluster peers (if any)
In the Advanced section: Zone profile	*Default*

It is recommended that the connection to the “Lync Gateway” Cisco VCS uses SIP over TLS to communicate so that encrypted calls can be handled. H.323 mode should also be enabled, so that any interworking that has to be done for calls with Lync Server is carried out on the “Lync gateway” Cisco VCS.

4. Click **Save**.



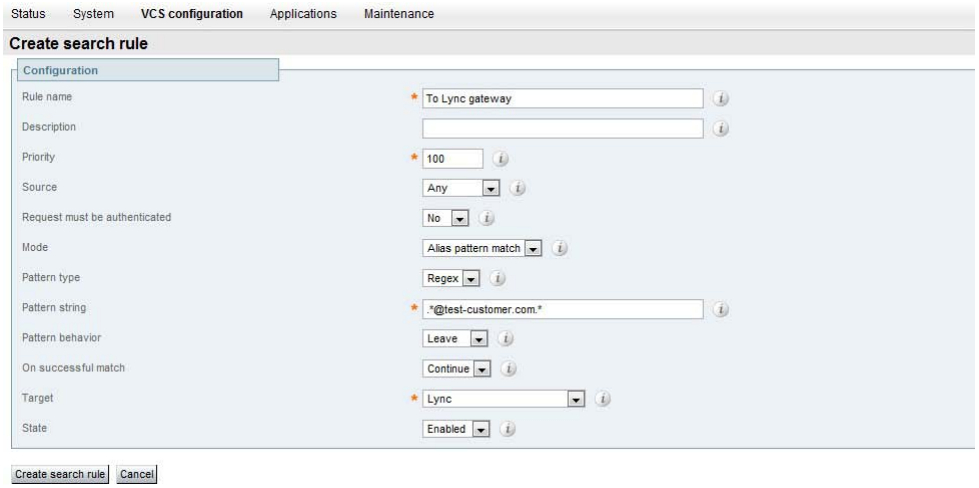
Note: Do not worry about the status section indicating Failed. This will change to Active after the zone’s IP address / FQDN has been saved.

Set up a search rule to route calls with the Lync Server domain to the “Lync gateway” Cisco 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 “To Lync Gateway”
Priority	Leave as default, for example 100
Source	*Any*
Request must be authenticated	*No*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	.*@test-customer.com.*
Pattern behavior	*Leave*
On successful match	*Continue*
Target zone	*Lync*
State	*Enabled*

4. Click **Create search rule**.



"Lync gateway" Cisco VCS Control configuration (1)

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

It is recommended to use TLS connectivity between Cisco VCS and Lync, Server but TCP connection is also explained. (TCP may not work for Lync Server configurations that include HLBs and / or Lync Director).

To configure a "Lync gateway" Cisco 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" Cisco VCS.
3. Ensure that the default links between the "Lync gateway" Cisco VCS Control's zones are set up.
4. Configure DNS.
5. Ensure that cluster name is configured.
6. Configure an NTP server.
7. Switch on TLS in SIP configuration.
8. Set **H.323 <--> SIP interworking** to *On*.
9. Set **Call routed mode** to *Always*.

Generate and load private key, root certificate, and server certificate onto "Lync gateway" Cisco VCS Control (not needed if TCP connection is used)

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

Note: 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 Cisco VCS then use the section "Server certificate for each Cisco VCS".

Details on how to create certificates for Cisco VCS are documented in "Cisco VCS Deployment Guide – Certificate creation and use with Cisco VCS".

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

The certificate must specify:

- **Subject name**: the Cisco VCS cluster's routable domain, e.g.vcslyncgateway.test-customer.com
- **Subject Alternate Name**: a comma separated list of the Cisco VCS peers' routable domains (DNS Local hostname concatenated with DNS Domain)
  e.g. vcslyncpeer1.test-customer.com,vcslyncpeer2.test-customer.com

Server certificate for each Cisco VCS:

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

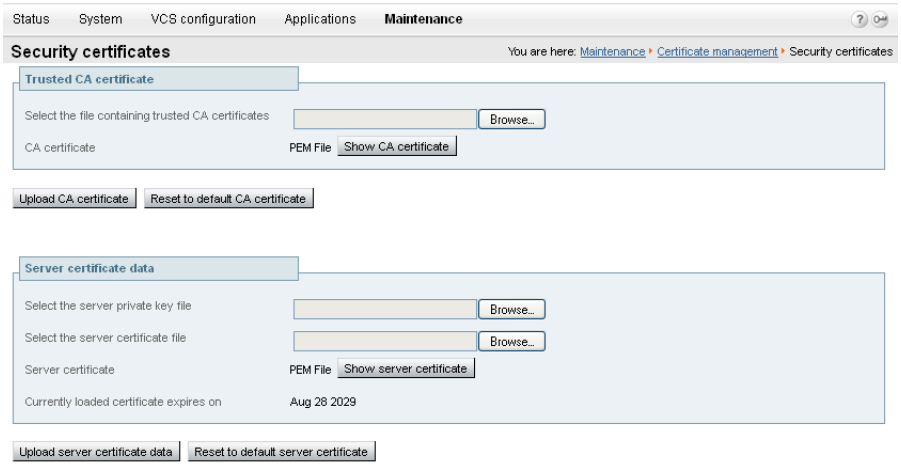
- **Subject name**: the Cisco VCS peer's routable domain (DNS Local hostname concatenated with DNS Domain) e.g. vcslyncpeer1.test-customer.com

and if it is part of a cluster:

- **Subject Alternate Name**: the Cisco VCS cluster's routable domain, e.g. vcslyncgateway.test-customer.com

Load the certificates:

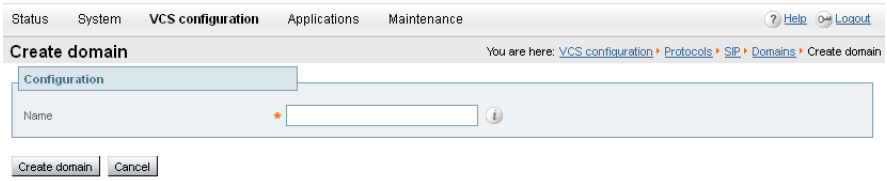
Load the certificates on the **Security certificates** page (**Maintenance > Certificate management > Security certificates**):



Set up the SIP domain of the "Lync Gateway" Cisco VCS

OCS Relay FindMe™ users need to have the "Lync gateway" Cisco VCS handle the Lync Server's domain.

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

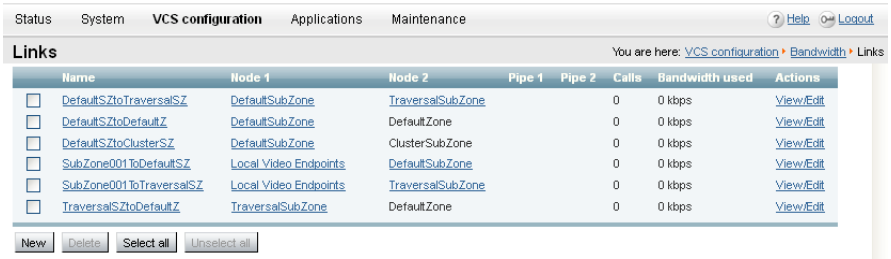


Ensure that default links between the "Lync gateway" Cisco VCS Control's zones are set up

For a call to succeed there must be appropriate links between Zones, links must exist from:

- Default Subzone to Traversal Subzone
- Default Subzone to Default Zone
- Default Subzone to Cluster Subzone (*this is required even if Cisco VCS is not part of a cluster)*
- Traversal Subzone to Default Zone

Check these on the **Links** page (**VCS configuration > Bandwidth > Links**):



If any links are missing, log onto the command line interface and run the command:

```
xcommand DefaultLinksAdd
```

Configure DNS details

Configure the DNS Server details

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

On the 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 servers.

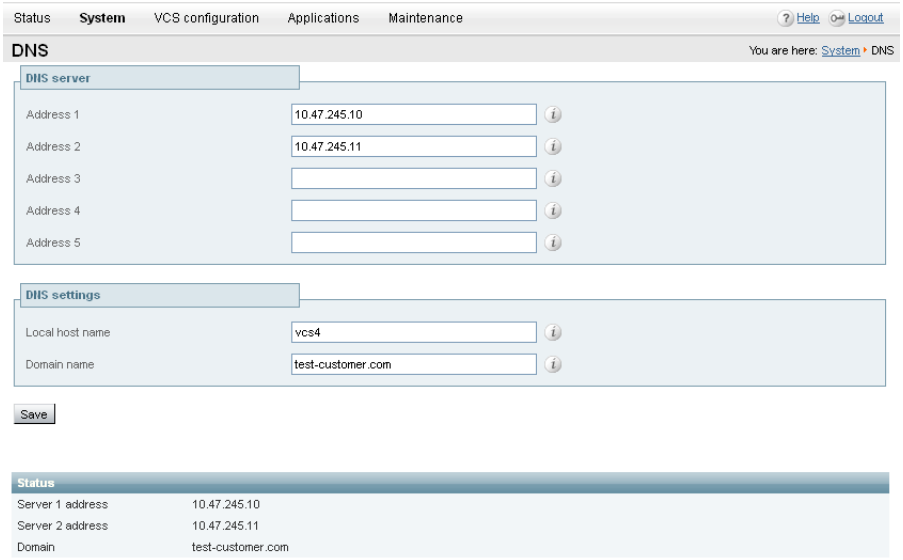
Note: If the DNS server IP address is 127.0.0.1 that means that Lync Server is using a DNS server on its own hardware. Instead of entering 127.0.0.1 on the Cisco VCS, use the IP address of the Lync Server platform instead.

On each "Lync gateway" Cisco VCS Control peer:

1. Go to the **DNS** page (**System > DNS**).
2. Set **DNS server Address 1** to the IP address of DNS server noted earlier.
3. If Lync Server has more than one DNS server defined, configure the remaining fields as follows:

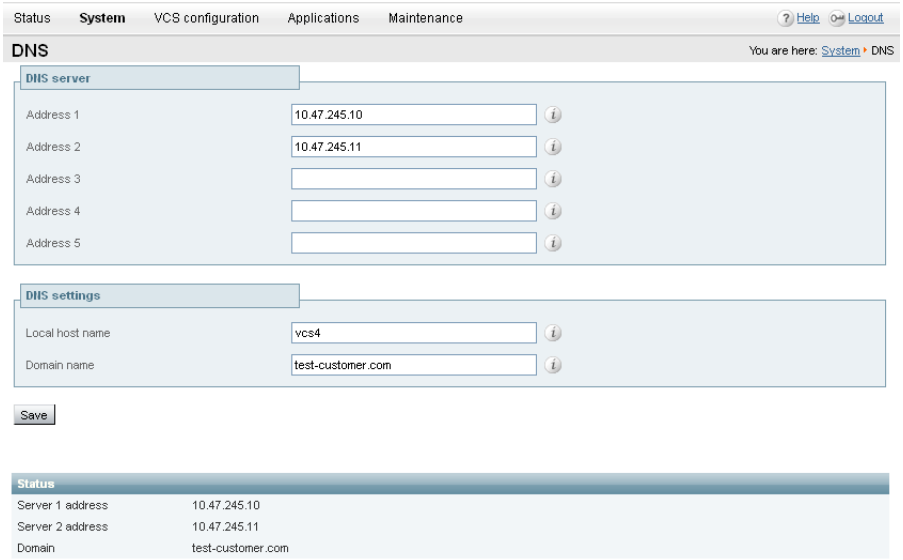
DNS Server Address 2	IP address of DNS server 2 (if there is a second DNS server)
DNS Server Address 3	IP address of DNS server 3 (if there is a third DNS server)
DNS Server Address 4	IP address of DNS server 4 (if there is a fourth DNS server)
DNS Server Address 5	IP address of DNS server 5 (if there is a fifth DNS server)

4. Click **Save**.



Ensure that Local hostname and DNS domain are configured

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



1. On the **DNS** page (**System > DNS**) set:
   a. **Local host name** to a unique hostname for this Cisco VCS.
   b. **Domain name** to the domain name for this Cisco VCS.
2. Click **Save**.

Note that the **Local host name** concatenated with **DNS domain** name is the routable FQDN of this Cisco VCS.

Note: If these are not configured and the connection between Lync Server and Cisco VCS is TLS, then although the neighbor zone goes active and Cisco VCS can send messaging to Lync Server, Lync Server will never open a TLS connection back to Cisco VCS, resulting in no calls Lync Server to Cisco VCS and other strange behavior.

Ensure that cluster name is configured

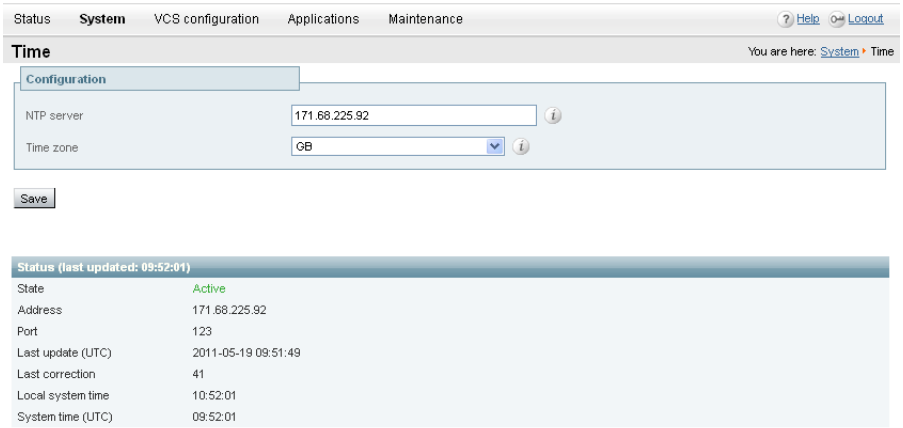
This should be configured whether the Cisco VCS is part of a cluster or not; this value is used with FindMe™ as well as clustering.

For each “Lync gateway” Cisco 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 VCS Cluster Creation and Maintenance Deployment Guide (X6.1) - D14367.08”. If the cluster name needs changing follow the procedure in that document.

Configure an NTP server

On each “Lync gateway” Cisco VCS Control peer:

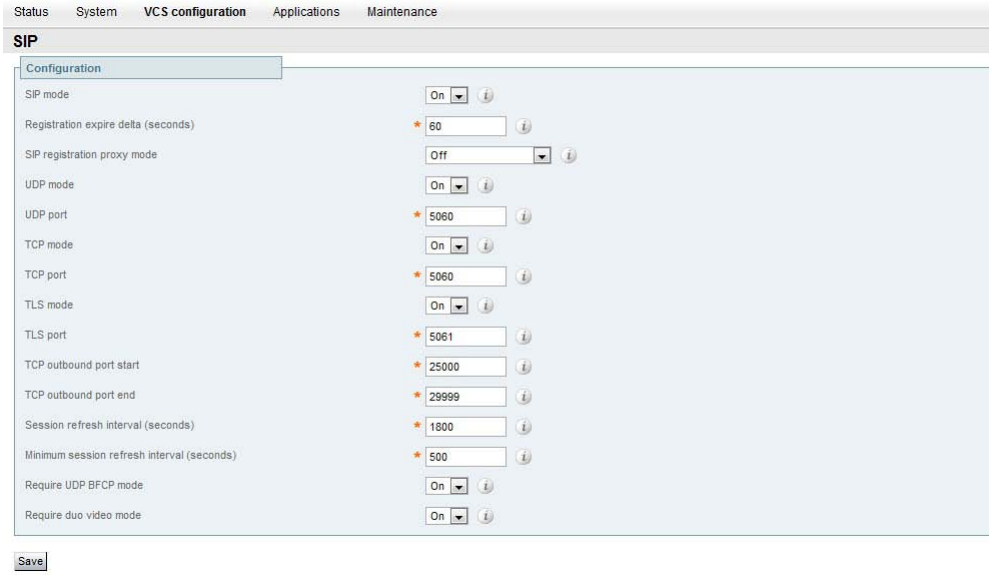
1. Go to the **Time** page (**System > Time**).
2. Set **NTP server** to the IP address of an NTP server
3. Set **Time zone** as appropriate to the location of the Cisco VCS.



Note: You can find out which time server that windows server is using by typing ‘net time /querysntp’ from a windows command line

Switch on TLS in SIP configuration (not needed if TCP connection is used)

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



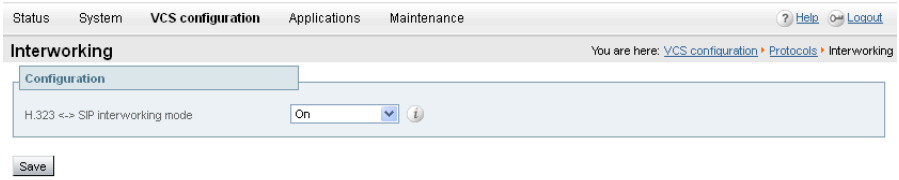
Set up H.323 ←→ SIP interworking

For H.323 endpoints to be able to communicate with Lync Server Cisco VCS must interwork the SIP signaling and H.323 signaling.

When H.323 endpoints are interworked to Lync Server SIP, the Cisco VCS carrying out the interworking needs to know that it is interworking to Lync Server (as the interworking functionality needs to specifically handle the requirements of Lync Server), therefore the interworking must be carried out on the "Lync gateway" Cisco VCS.

To ensure interworking is carried out on this "Lync gateway" Cisco VCS, set **H.323 ←→ SIP interworking mode** to *On* (rather than *Registered only*, as usually recommended).

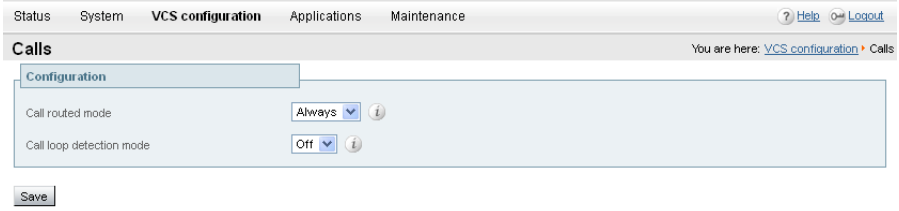
1. Go to the **Interworking** page (**VCS configuration > Protocols > Interworking**).
2. Set **H.323 ←→ SIP interworking mode** to *On*.
3. Click **Save**.



Set Call routed mode to Always

Even if the **"Lync gateway**" Cisco VCS is part of a cluster, and the cluster deployment guide says that **Call routed mode** should be set to *Optimal*, when connecting to Lync Server, **Call routed mode** must be set to *Always*, so that the signaling from Lync Server is always processed by the "Lync gateway" Cisco VCS.

1. Go to the **Calls** page (**VCS configuration > Calls**).
2. Set **Call routed mode** to *Always*.
3. Click **Save**.



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 will not know how to route them, so will pass the calls to the Director 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 Server

   For 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 Static Route(s) to route calls to the “Lync gateway” Cisco VCS(s).
4. Configure Lync Server to make media encryption optional.

Trust a Lync Gateway VCS and assign a static route on Lync Server

These steps have to be configured on each Lync Director, or Each FEP – whichever the Cisco VCS communicates directly with.

On Lync Server:

1. Select **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Management Shell**.
2. Set a Lync Gateway VCS 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 FQDN of the Lync Gateway VCS (or Lync Gateway VCS Cluster name if present). 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`: it 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.LYNC>New-CsTrustedApplicationPool -Identity
     vcs.test-customer.com -Registrar LyncPool01.test-customer.com -site 1
     -RequiresReplication $false -ThrottleAsServer $true -
     TreatAsAuthenticated $true
     ```
3. 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 TCP port to be used for neighboring (should be 5061, if TLS)

  For example:

  ```
  C:\Users\administrator.LYNC>New-CsTrustedApplication -ApplicationID
  VCSApplication1 -TrustedApplicationPoolFqdn vcs.test-customer.com -
  Port 5061
  ```

4. Allow encryption to be negotiated

   - Use the command "`set-CsMediaConfiguration`" with the following parameters:

     `-EncryptionLevel`: specifies that encryption is not mandatory

     For example:

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

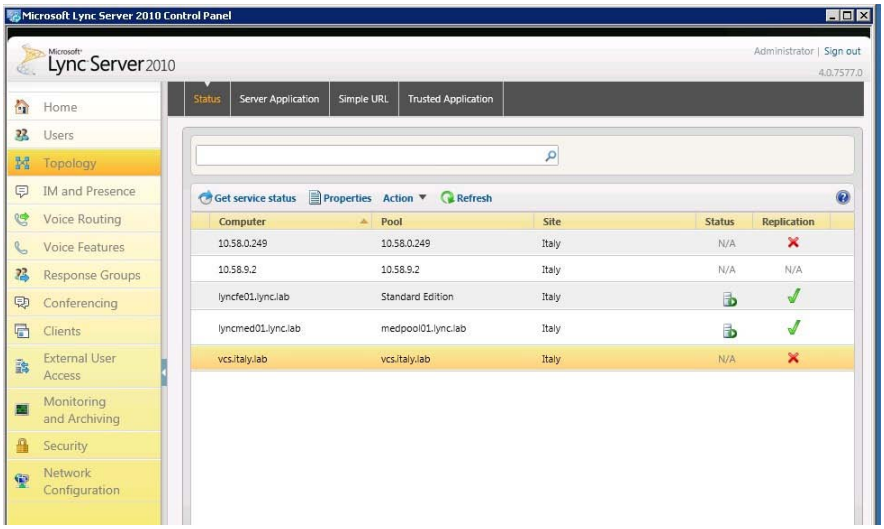
5. Apply the configuration

   - Use the command "`Enable-CsTopology`".

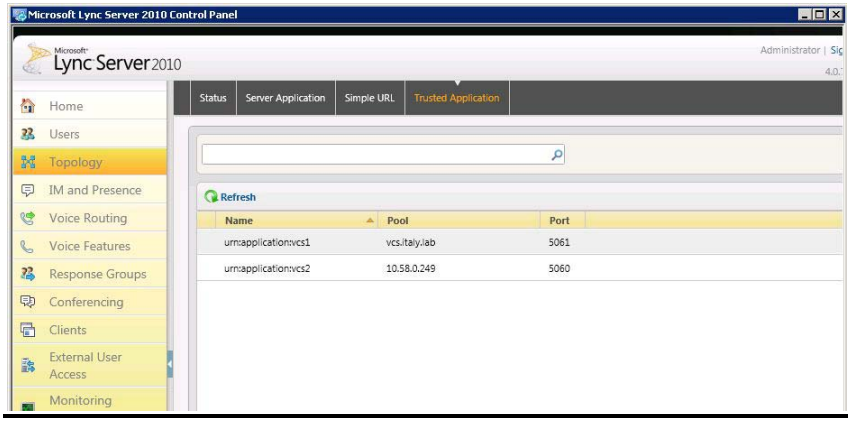
     For example:

     ```
     C:\Users\administrator.LYNC>Enable-Cs-Topology
     ```

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



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



6. Create a static route

   - Use the command "`New-CsStaticRoute`" with the following parameters:

     $=: the label referring to this specific new route.

     `-TLSRoute`: specifies that the route is TLS

     `-TCPRoute`: specifies that the route is TCP

     `-Destination`: "" specifies the Lync Gateway VCS FQDN (or Lync Gateway VCS Cluster name if present) 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 TCP port to be used for neighboring (should be 5061)

     `-UseDefaultCertificate`: specifies to use the default certificate assigned to the Front End (must be $true)

     For example:

     ```
     C:\Users\administrator.LYNC> $Route1=New-CsStaticRoute -TLSRoute -
     Destination "vcs.test-customer.com" -MatchUri "VCSsipdomain.lab" –
     Port 5061 -UseDefaultCertificate $true
     ```

7. 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 before to the specified Identity (note that brackets are curly)

     For example:

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

8. Verify static route assignment

   - In order to verify the correct assignment of the route use the command "`Get-CsStaticRoutingConfiguration`".

     For example:

     ```
     C:\Users\administrator.LYNC> Get-CsStaticRoutingConfiguration
     ```

     Identity: Global

     Route: {MatchUri=VCSsipdomain.lab;MatchOnlyPhoneUri=False;Enabled=True;ReplaceHostInRequestUri=False}

Note: Static routes should be set up for all domains handled by the Cisco VCS.

- If Lync Server tries to route a call to the domain shared between Lync Server and Cisco VCS:
  - Lync Server will first check all its registrations, both Lync Server registrations and OCS Relay FindMe™ registrations registered to Lync Server. If any registration is found that matches the called URI the call will be sent to that device, or if multiple registrations exist, the call will be forked to all registered devices that match the URI.
  - If there is no registration Lync Server will then check the static domain routes and if there is one for this domain Lync Server will route the call to the destination specified.

- If Lync Server tries to route a call to a domain that is not shared between Lync Server and Cisco VCS:
  - Lync Server will check the static domain routes and if there is one for this domain Lync Server will route the call to the destination specified.

Although the primary access to end users registered on Cisco VCS may be via a specific domain, providing static routes for other domains handled by Cisco VCS means that:

- Endpoints in different domains that may call Lync Server can be called back using their 'caller ID' which may have a domain other than the primary domain.

- When using OCS Relay and Lync Server and Cisco VCS have the same domain for registered devices, devices like MCUs and ISDN gateways which may register IDs in the same domain as Lync, Server but not have FindMe™ IDs associated with them (e.g. because they are ad hoc conferences) will be able to be called by Lync Server.

Configure Lync Server to make media encryption optional

By default Lync Server mandates the use of encrypted media. The headers used in Lync Server SRTP, however, are different from those used by video network devices. Calls between the video network and Lync Server must therefore use unencrypted media, unless you are using Cisco VCS version X6.1 with the **Enhanced OCS Collaboration** option key and the connection between the Cisco VCS and Lync Server is TLS.

If the Cisco VCS is not using the **Enhanced OCS Collaboration** option key or is not connected to Lync Server via TLS, then the Microsoft Lync Server 2010 zone configuration in the "Lync gateway" Cisco VCS(s) handles the signaling to ensure that media encryption is not negotiated. Lync Server needs to be configured to accept calls where media is not encrypted.

On Lync Server:

1. Select **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Management Shell**.
2. Allow encryption to be negotiated
   - Use the command "`set-CsMediaConfiguration –EncryptionLevel supportencryption`".

Note:

- This parameter is a value communicated to Lync clients to affect its operation. To activate this change on a Lync client, the Lync client must be logged off and logged back in again.
  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, any calls with video endpoints that do not support encryption will fail – in this case **SupportEncryption** should be used instead.

Lync gateway" Cisco VCS Control configuration (2)

1. Configure the "Lync gateway" Cisco VCS with a neighbor zone that contains Lync Server.
2. Set up a search rule to select what gets routed to the Lync Server zone.
3. If Hardware Load Balancers are used, set up neighbor zones to receive calls from Lync Server.

Configure the "Lync gateway" Cisco VCS with a neighbor zone that contains Lync Server

1. Go to the **Zones** page (**VCS configuration > Zones**).
2. Click **New**.
3. Configure the fields as follows:

   It is recommended that the "Lync gateway" Cisco VCS uses SIP over TLS to communicate with Lync Server.

   For SIP over TLS configure the following fields:

SIP mode	*On*
SIP port	5061 (or the value that is the same as that configured on Lync Server for Cisco VCS access over TLS)
SIP transport	*TLS*
TLS verify	*Off*

   Not recommended, but if SIP over TCP is required, configure the following fields:

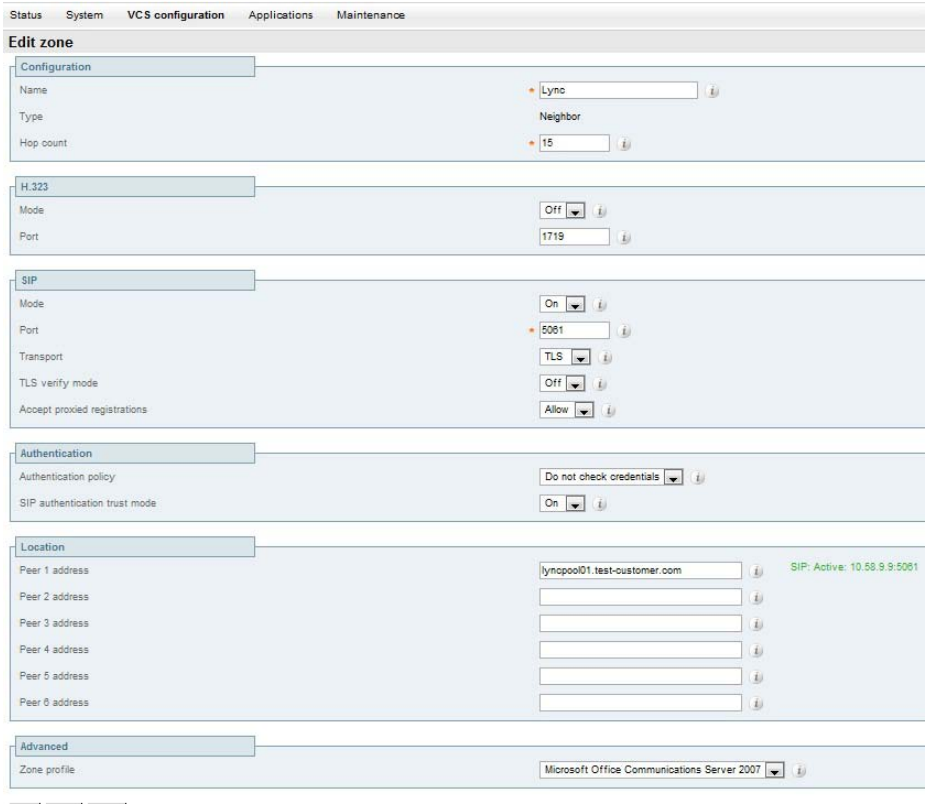
SIP mode	*On*
SIP port	5060 (or the value that is the same as that configured on Lync Server for Cisco VCS access over TCP)
SIP transport	*TCP*

4. For TLS and TCP configure the following fields:

H.323 mode	*Off* (H.323 access is not required for communication with Lync Server)
Authentication policy	*Do not check credentials*
SIP authentication trust mode	*On*
In the Location section: Peer 1 address	FQDN of Lync Server (Lync Director, Hardware Load Balancer or FEP as appropriate), for example: enterprisepool.test-customer.com
In the Advanced section: Zone profile	*Microsoft Office Communications Server 2007*

   Note: 'Appendix 5 – Advanced parameters set by selecting zone profile 'Microsoft Office Communications Server 2007' identifies the advanced configuration values that selecting Microsoft Office Communications Server 2007 selects.

5. Click **Save**.



Note:

- Do not worry about the status section indicating Failed. This will change to Active once the zone's IP address / FQDN has been saved.
- Lync Server does not accept INVITEs with no SDP; it requires the calling party to choose the audio and video codecs. When interworking an H.323 call to Microsoft Lync Server 2010, Cisco VCS offers a default set of codecs. By default Cisco VCS chooses a sensible audio and video codec for Lync Server but see *Appendix 6 – Setting default codecs for H.323 to SIP calls* if it is desired to modify the codecs offered in the initial INVITE of an interworked call.

Set up a search rule to select what gets routed to the Lync Server zone

Search rules are used to specify the URIs to be forwarded to this neighbor Lync Server (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 Server *calls*" for further information about user=phone).

For this scenario, anything with a domain test-customer.com will be matched (and passed to Lync Server); no transformation is required.

("*Appendix 7 – Presence with and without transforms*" provides additional details about using transforms and what needs to be done if presence is to be used when transforms are applied in the Search rule.)

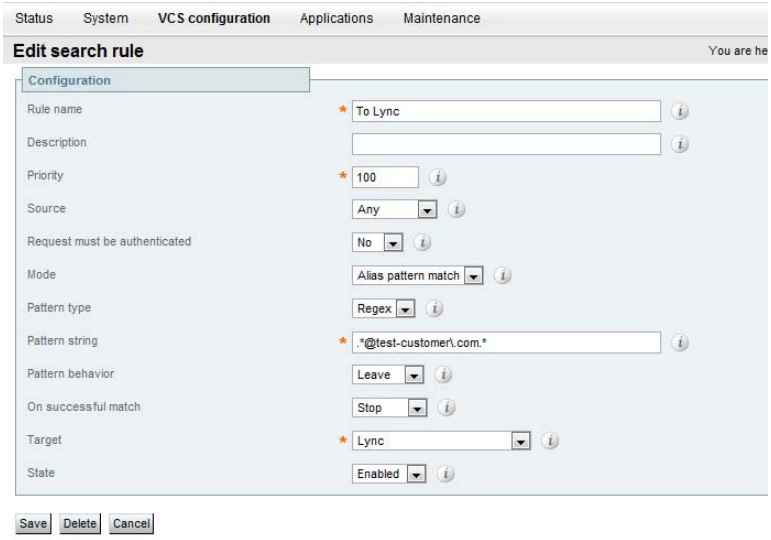
1. Go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**).
2. Click **New**.

   Configure the search rule so that all calls to URIs in the format .*@test-customer.com are forwarded to Lync Server. (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.)

3. Configure the following fields:

Rule name	To Lync
Zone name	Lync
Priority	100
Source	*Any*
Request must be authenticated	*No*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	.*@test-customer\.com.*
Pattern behavior	*Leave*
On successful match	*Stop*
Target zone	*Lync*

4. Click **Create search rule**.



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

Note: Never use a **Mode** of *Any alias* - always use a pattern string which matches the Lync Server registrations as closely as possible so that only calls, notifies and other messages that are handled by this zone get routed to this neighbor.

If *Any alias* were to be selected, then all calls and other messages would be routed to the Lync Server zone — subject to no higher priority Search rules matching — whether or not Lync Server supports that call or message.

If Hardware Load Balancers or Lync Directors are used, set up neighbor zones on the "Lync gateway" Cisco VCS(s) to receive calls from Lync FEPs

If Hardware Load Balancers are used then Lync Server will still send messages to Cisco VCS from the devices directly behind the main Hardware Load Balancer.

If the main Hardware Load Balancer is in front of Lync Directors, then neighbor zones need to be configured that reference the Lync Directors, so that Cisco VCS will treat calls received from these devices as Lync Server calls.

If the main Hardware Load Balancer is in front of FEPs, then neighbor zones need to be configured that reference all the FEPs, so that calls received from these devices are treated as Lync Server calls.

1. Go to the **Zones** page (**VCS configuration > Zones**).
2. Click **New**.
3. Configure the fields as follows:

Name	"Lync receive only 1"
Type	*Neighbor*

For SIP over TLS configure the following fields:

SIP mode	*On*
SIP port	5061 (or the value that is the same as that configured on Lync Server for Cisco VCS access over TLS)
SIP transport	*TLS*
TLS verify mode	*Off*
Accept proxied registrations	*Deny*

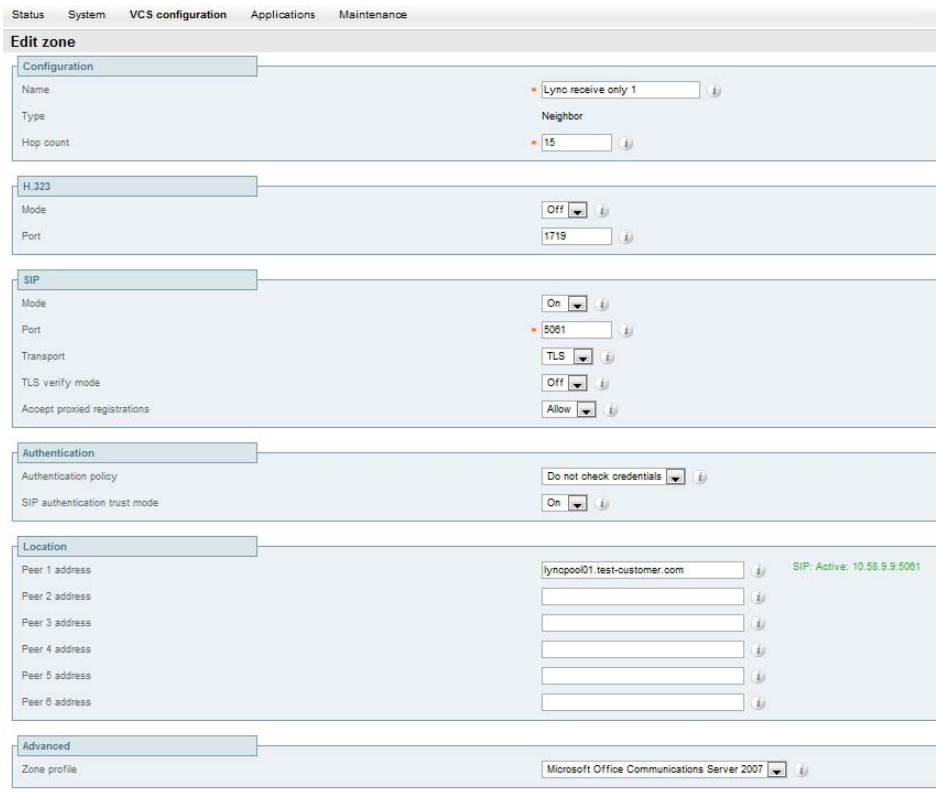
Not recommended, but if SIP over TCP is used, configure the following fields:

SIP mode	*On*
SIP port	5060 (or the value that is the same as that configured on Lync Server for Cisco VCS access over TCP)
SIP transport	*TCP*
Accept proxied registrations	*Deny*

For TLS and TCP configure the following fields:

H.323 mode	*Off* (H.323 access is not required for communication with Lync Server)
Authentication policy	*Do not check credentials*
Sip authentication trust mode	*On*
In the Location section: Peer 1 address	FQDN of an Lync Director or an FEP as appropriate
In the Location section: Peer 2 address	FQDN of an Lync Director or an FEP as appropriate
In the Location section: Peer 3 address	FQDN of an Lync Director or an FEP as appropriate – if any more than 2
In the Location section: Peer 4 address	FQDN of an Lync Director or an FEP as appropriate – if any more than 3
In the Location section: Peer 5 address	FQDN of an Lync Director or an FEP as appropriate – if any more than 4
In the Location section: Peer 6 address	FQDN of an Lync Director or an FEP as appropriate – if any more than 5
In the Advanced section: Zone profile	*Microsoft Office Communications Server 2007*

4. Click **Create Zone**.



Note: Do not worry about the status section indicating Failed. This will change to Active once the zone's IP address / FQDN has been saved.

If there are more than 6 FEPs behind the main Hardware load balancer, add further neighbor zones (each with unique names) until all FEPs are referenced as a Peer x Address.

Note: Do not configure any search rules to point to these zones - these zones are receive only.

Calls can now be made between SIP and 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 user1@test-customer.com or user2@test-customer.com from both SIP and H.323 endpoints registered on Cisco VCS Control.

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

"Lync gateway" Cisco VCS Control configuration

1. Configure the "Lync gateway" Cisco VCS with a neighbor zone that contains the video network.
2. Set up one or more Search rules to route calls with video network domains to the video network.

Note: In small test and demo networks this configuration is not necessary as the video network Cisco VCS is the "Lync Gateway" Cisco VCS. You can skip this section and go to "Lync configuration" on page 41.

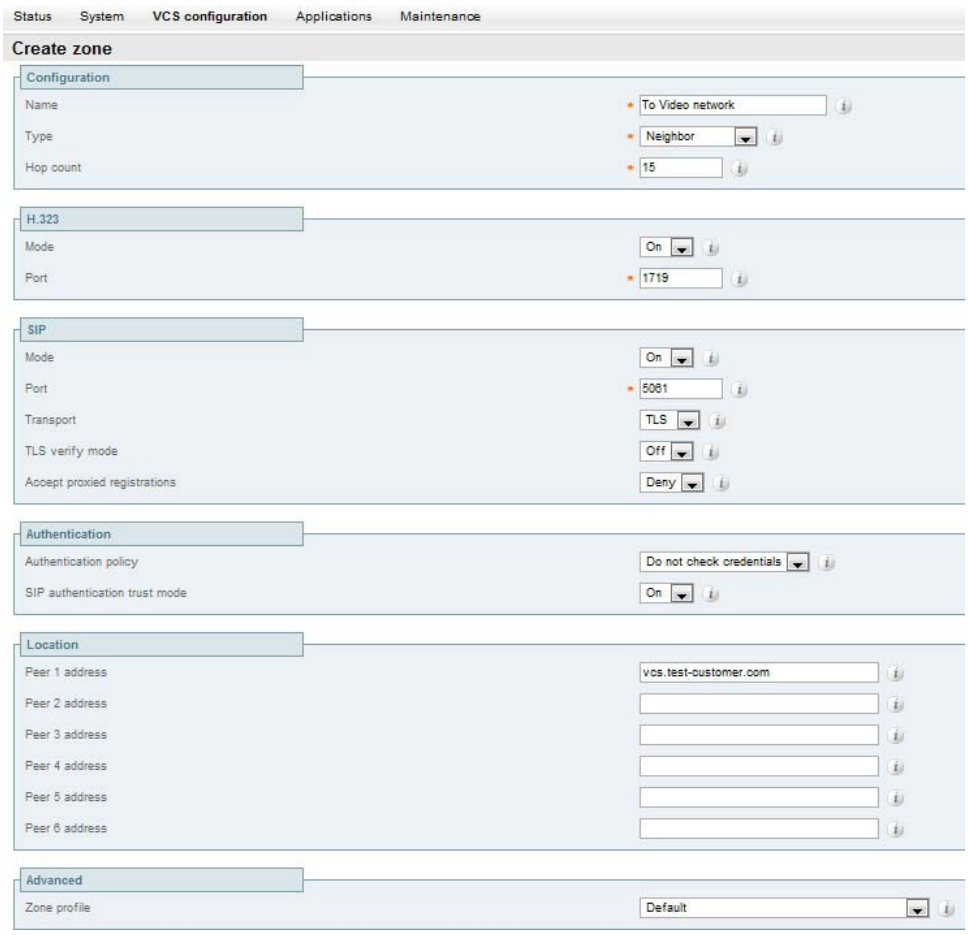
Configure the "Lync gateway" Cisco VCS with a neighbor zone that contains the video network

1. Go to the **Zones** page (**VCS configuration > Zones**).
2. Click **New**.

   It is recommended that the connection to the "Lync gateway" Cisco VCS uses SIP over TLS to communicate so that encrypted calls can be handled. H.323 mode should also be enabled, so that any interworking that has to be done for calls with Lync Server is carried out on the "Lync gateway" Cisco VCS.
3. Configure the fields as follows:

Name	"To Video network"
Type	*Neighbor*
SIP mode	*On*
SIP port	5061 (or the value that is the same as that configured on the "Lync gateway" Cisco VCS for TLS mode SIP)
SIP transport	*TLS*
TLS verify mode	*Off*
Accept proxied registrations	*Deny*
H.323 mode	*On*
In the Location section: Peer 1 address	IP address or FQDN of the video network Cisco VCS (or the 1st Cisco VCS in the Video network cluster)
In the Location section: Peer 2 address to Peer 6 address	IP address or FQDN of the 2nd to 6th video network cluster peers (if any)
In the Advanced section: Zone profile	*Default*

4. Click **Create zone**.



Note: Do not worry about the status section indicating Failed. This will change to Active once the zone's IP address / FQDN has been saved.

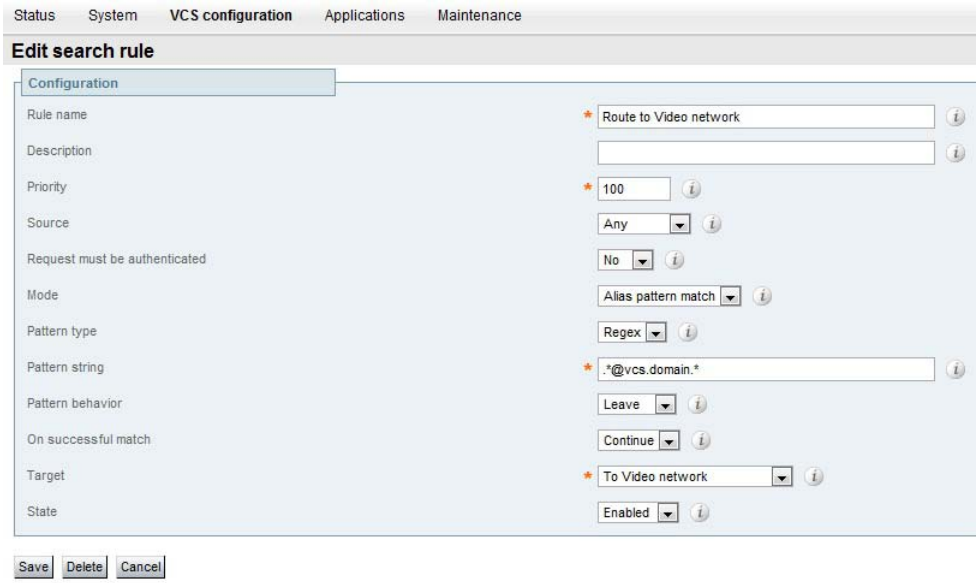
Set up one or more search rules to route calls with video network domains to the video network

1. Go to the **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 Video network"
Priority	Leave as default, for example 100
Source	*Any*
Request must be authenticated	*No*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	Anything in the Video network domain, for example .*@vcs.domain.*
Pattern behavior	*Leave*
On successful match	*Continue*
Target zone	Select the Video network zone, for example "To Video network"

4. Click **Save**.

5. Repeat until there is a rule for each video network domain.



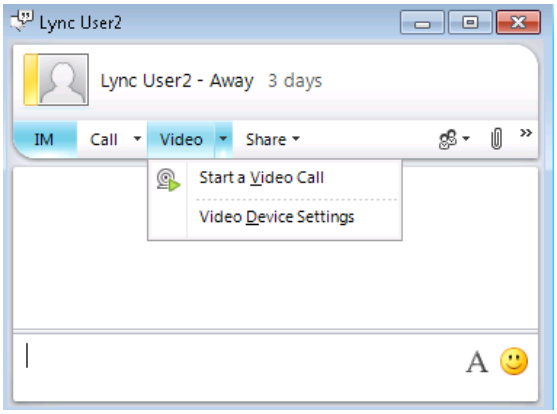
Lync Server configuration

No further configuration (beyond that carried out above) is required on Lync to allow calls from Lync clients to endpoints registered on Cisco VCS Control.

Testing the configuration

Test calls from Lync Clients registered on Lync Server to endpoints registered on Cisco VCS Control.

For example, call user2@vcs.domain or user1@vcs.domain 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):



Enabling Lync clients to see presence status of endpoints registered on Cisco 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 by 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 Cisco VCS Control can see the presence status of other endpoints registered to Cisco VCS Control.

In summary:

	… to Cisco VCS	**… to Lync**
Cisco VCS to … (no OCS Relay)	Full presence available	Presence = Available only
Cisco VCS to … (with OCS Relay)	Full presence available	Presence = Available and In-Call
Lync to …	No presence information available	Full presence available

Cisco VCS configuration

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

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

- Cisco VCS PUA generates Presence = available if endpoint is registered
- Cisco VCS PUA generates Presence = In-call if the endpoint is in a call

If an endpoint generates presence and the PUA is enabled, the Cisco VCS Presence Server will aggregate both results. If there are results from the PUA plus just one other Presence Publisher, the Presence Server deems the PUA to be monitoring the other publisher, so the other publisher’s status always wins; otherwise the Presence Server supplies the “highest interest” presence information available, for example “in-call” is reported in preference to “on-line”. The Presence Server also supports richer presence information – such as “Busy, in a meeting” – which may be supplied by the endpoint.

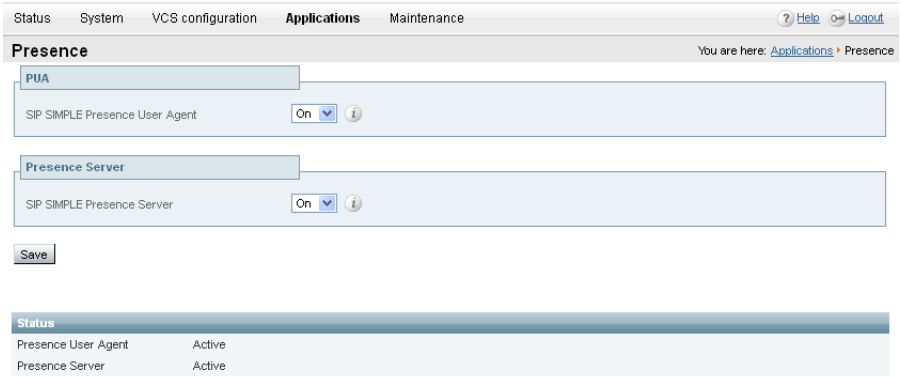
Note: For H.323 devices to supply presence (via the PUA) the registered H323 ID of that endpoint must resemble a SIP URI. The presence will be published for that URI.

To configure presence on the Cisco VCS Control:

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

SIP SIMPLE Presence User Agent	*On* (if Cisco VCS Control is to generate presence information for registered endpoints)

SIP SIMPLE Presence Server	*On*



Note: The Cisco VCS that connects to Lync Server should be the presence server for ALL sip domains that Lync Server might want to look at for presence; this limits the number of Cisco VCSs that Lync Server 's presence requests will travel through.

Presence requests use up SIP resources and with Lync Server 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 Cisco VCSs that already heavily used for taking calls.

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

Lync Server configuration

No further configuration (beyond that carried out above) is required on Lync Server to support presence.

Testing the configuration

Test calls from endpoints registered on Cisco VCS Control to Lync clients registered on Lync Server.

For example, call user1@test-customer.com or user2@test-customer.com from both SIP and H.323 endpoints registered on Cisco VCS Control.

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

- See the icon change from gray to green when an endpoint is registered on Cisco VCS Control.
- See the icon change from green to gray if the endpoint becomes de-registered from Cisco VCS Control.

OCS Relay configuration of “Lync Gateway” Cisco VCS(s)

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

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

What does OCS Relay do?

When enabled, OCS Relay registers FindMe™ users that are in the same domain as Lync Server to Lync Server so that they appear like Lync users to other Lync devices.

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

Without OCS Relay and FindMe™, Lync Server will not fork the call to Cisco VCS, but:

- If a Lync is registered with the called address then just that Lync will ring.
- If there is no Lync registered and there is no static domain route for this call then the call will just fail.

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

- OCS Relay also allows the presence of FindMe™ users registered to Lync Server to provide ‘in-call’ as well as ‘available’ and ‘off-line’ status to Lync users.
  - Endpoint devices and FindMe™ entries that are not registered to Lync Server can only communicate ‘available’ and ‘off-line’ status to Lync Server, even if OCS Relay is enabled.
  - Without OCS Relay and FindMe™, Cisco VCS can only communicate ‘available’ and ‘off-line’ status to Lync Server.

Note: The “Lync gateway” Cisco VCS(s) must host the presence server for the domain of the Lync Server network (test-customer.com) in order for presence to be provided to Lync Server.
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” Cisco VCS(s). The “Lync gateway” Cisco VCS(s) must therefore also host the presence server for the domain of the video network (vcs.domain).
If FindMe™ entries contain multiple devices in the active location, Cisco VCS will aggregate the presence of those devices whose presence is hosted on the “Lync gateway” Cisco VCS(s) 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 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 users registered with this ID all ringing simultaneously – rather than the return call being addressed directly back to the single endpoint that made the call.

OCS Relay and a cluster of Cisco VCSs

From Cisco VCS X5.0 OCS Relay can be enabled in a cluster of Cisco VCSs. When used in a cluster of Cisco VCSs, the OCS Relay FindMe™ users will be shared across cluster peers (using an algorithmic distribution scheme). Each cluster peer will register its own OCS Relay FindMe™ users to Lync Server. When calls are made from Lync Server to OCS Relay FindMe™ users Lync Server will send the call to the Cisco VCS peer that registered that user – hence the calls are statically load-shared across the Cisco VCS peers.

Note: Calls to Video endpoint IDs that are not OCS Relay FindMe™ user IDs will not match a registered user, and so will be routed by the static domain route configured in Lync Server. These calls to non-OCS Relay FindMe™ endpoints will therefore be delivered to a single Cisco VCS peer or a range of Cisco VCS peers (slowly rotating) if a round-robin DNS address is configured in Lync Server. (When using round-robin, Lync Server rotates peers approximately once per 5 seconds - this helps with resilience, but is not fast enough to provide effective load sharing.

Configure OCS Relay and FindMe™

It is best practice to keep the video endpoints in their own domain, and just have the FindMe™ users on the “Lync gateway” Cisco 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 user2@test-customer.com is called, the call will fork to the Lync client with the same name, and also to user2.office@vcs.domain and user2.external@vcs.domain (assuming that these two vcs.domain devices are listed as primary devices in User2’s FindMe™.

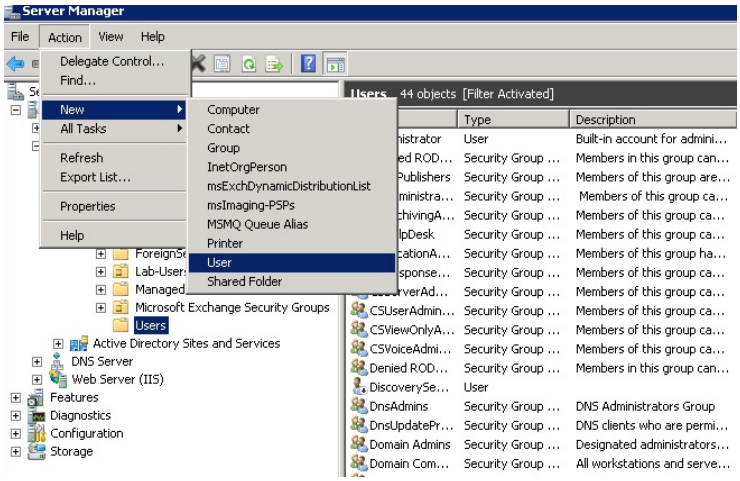
Note: It is strongly recommended that the user is created on Lync Server first and then FindMe™ accounts created on Cisco VCS 5 to 10 minutes later, when the user is fully available on Lync Server.

Active Directory configuration

Ensure that Active Directory user accounts exist for all FindMe™ accounts on the “Lync Gateway” Cisco VCS(s) that will register to Lync (FindMe™ accounts that have the same domain as Lync).

On the PC running the Active Directory for Lync users:

1. Select **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:

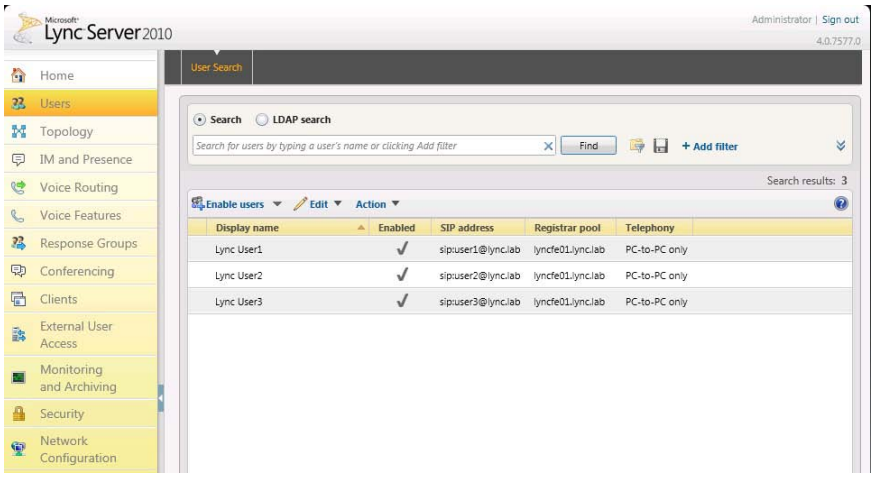
3. Click **Action > New > User**.
4. Configure the following fields:

First name	The user’s first name
Last name	The user’s last name
User logon name	The user’s logon name

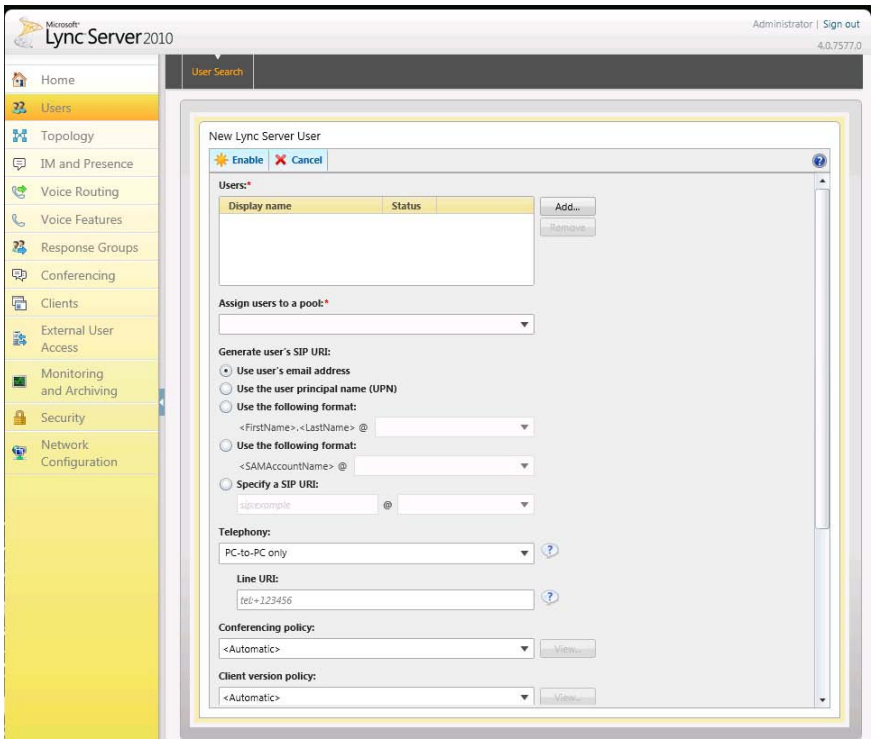
5. Click **Next**.
6. Configure the following fields:

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

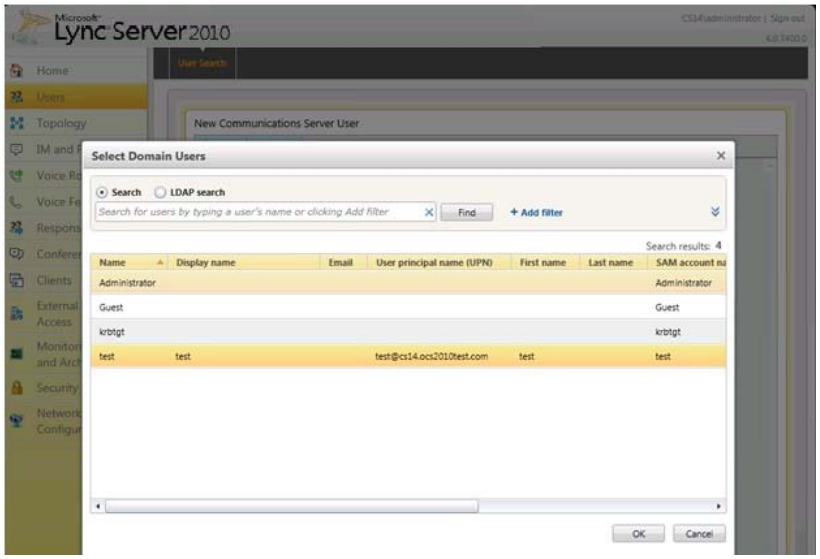
7. Click **Next**.
8. Click **Finish**.
9. Enable the user for Lync:
   - This can be done both by Communication Server Control Panel (CSCP) and Communication Server Power Shell (CSPS)commands.
     i. On Communication Server control panel go to the **Users** menu. You can see the users already enabled for communication server.



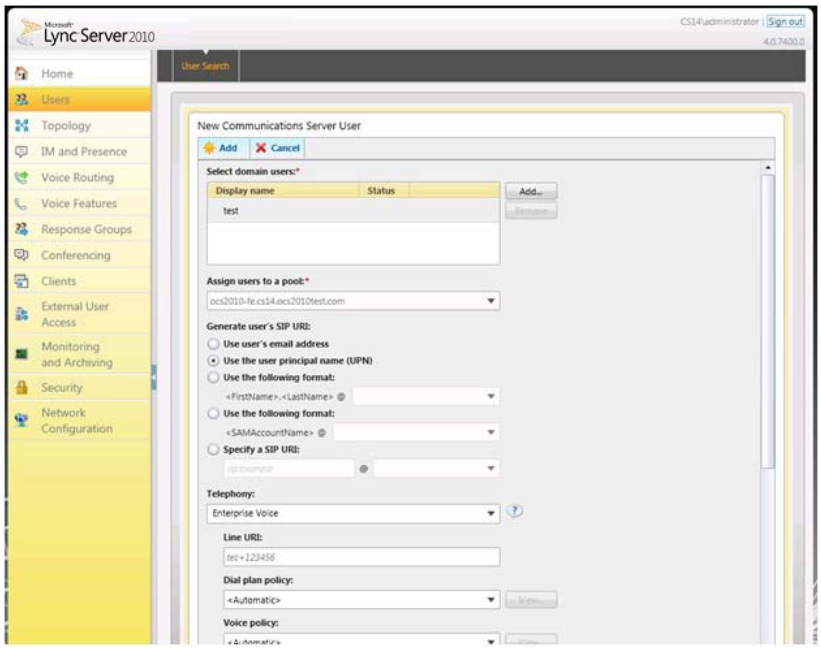
     ii. To add a new user, select **Enable users**.



iii. Click **Add**.



iv. Find and select the user in Active Directory.



v. Select the communication server pool to assign to the user.

vi. Select your preferred method to **Generate user’s SIP URI**.

vii. 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 "test1" -registrarpool "lyncpool01.test-customer.com" -sipaddress sip:user1@test-customer.com
  ```

“Lync gateway” Cisco VCS Configuration

The shared Cisco VCS / Lync Server domain **test-customer.com** is highlighted below so that it is easy to see which entries need to be changed to the shared domain used in your installation.

1. Go to the **Option keys** page (**Maintenance > Option keys**).
2. In the **Software option** section, in **Add option key**, enter the “User Policy” key (116341U00-1-xxxxxxxx).
3. Click **Add option**.
4. Go to the **FindMe configuration** page (**Applications > FindMe > Configuration**).
   a. Ensure **FindMe mode** is set to *On*.
   b. Set **Caller ID** to *FindMe ID*.
5. Click **Save**.
6. Configure Cisco VCS to be authoritative for the Lync Server domain so that FindMe™ users with that domain can be handled by this Cisco VCS and registered as Lync devices to Lync Server. Go to the **Domains** page (**VCS Configuration > Protocols > SIP > Domains**).
7. Click **New**.
8. In **Name** enter the domain shared with Lync Server (for example, **test-customer.com**).
9. Click **Create domain**.
10. Go to the **SIP** page (**VCS configuration > Protocols > SIP > Configuration**).
11. Set **SIP registration proxy mode** to *Proxy to known only*.
12. Click **Save**.

Note: If **SIP registration proxy mode** is already configured as *Proxy to any*, this is also suitable.

13. Ensure that presence is enabled (as described in *Enabling* Lync *clients to see the presence status of endpoints registered on Cisco VCS Control*).
14. Ensure that the Lync Server Neighbor zone is set up as described in”“ Lync gateway” Cisco VCS Control configuration (2)”.
    (If the Lync Server Neighbor zone is named anything other than “Lync”, then the CPL below must be updated to match the Lync Server Neighbor zone **Name**.)
15. Modify the “To Lync” Search rule set up in “Set up a Search rule to select what gets routed to the Lync Server zone”, replace the rule with:

Priority	40
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	(.*)lync\.(**test-customer\.com**.*)
Pattern behavior	*Replace*
Replace string	\1\2
On successful match	*Stop*
Target Zone	*Lync*

Note: If multiple domains are supported on Lync Server, only a single domain can be used with OCS Relay functionality (Cisco VCS registering as a Lync) – other domains should be handled using the search rules configured previously.

16. Click **Save**.

Note: The CPL below converts calls to test-customer.com destined for Lync Server to calls to lync.test-customer.com.
A second search rule, as defined in ‘Lync Server receiving Presence from non-OCS Relay FindMe™ entries, where there is a transform for Cisco VCS devices accessing Lync Server ’ (in *Appendix 7 – Presence with and without transforms*) is not necessary for Lync Server to see the presence of OCS Relay FindMe™ users. The OCS Relay communicates presence to Lync Server using Microsoft signaling.

17. Create a text file containing the following call policy (CPL), but replacing **test-customer.com** with the name of the sip domain shared between the Cisco VCS and Lync Server (and also the zone name if not “Lync”). Save it as a “.txt” file.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
   xmlns:taa="http://www.tandberg.net/cpl-extensions"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
      <taa:routed>
  <!-- VCS / LYNC CPL version 1.3 -->
         <taa:rule-switch>
            <!-- Don't fork calls from LYNC back to LYNC -->
            <taa:rule originating-zone="(LYNC|AMGW)" destination="(.+)@test-customer\.com">
               <proxy />
            </taa:rule>
            <!-- Only send to LYNC things sent to LYNC's contact details (e.g. presence Notify)--
   >
            <taa:rule origin="(.*)" destination="(.+)@test-customer\.com;opaque=user:epid.*">
               <taa:location clear="yes" regex="(.+)@(.+);.*" replace="\1@lync.\2">
                  <proxy />
               </taa:location>
            </taa:rule>
            <!-- Fork other calls to LYNC -->
            <taa:rule origin="(.*)" destination="(.+)@test-customer\.com">
               <taa:location clear="no" regex="(.+)@(.+)" replace="\1@lync.\2">
                  <proxy />
               </taa:location>
            </taa:rule>
         </taa:rule-switch>
      </taa:routed>
</cpl>
```

Note: Take care when copying CPL – non printing characters may cause CPL not to load, giving an error message such as:

18. Go to the **Call Policy configuration** page (**VCS configuration > Call Policy > Configuration**).
19. Set **Call Policy mode** to *Local CPL*.
20. Click **Save**.
21. Upload the new policy file:
    a. Click **Browse**.
    b. Select the text file (“.txt” created above) containing the CPL and click **Open**.
    c. Click **Upload file**.
22. Set FindMe™ to present the FindMe™ ID (rather than the endpoint ID) when any device in the primary list of FindMe™ devices makes a call – so that when a called party rings the caller ID back all FindMe™ endpoints ring, not just the endpoint that made the initial call will ring.
    a. Go to **Application > FindMe > Configuration**.
    b. Set **Caller ID** to *FindMe Id*.
23. For each Lync user that is to share Lync Client and Cisco VCS endpoints, create a FindMe™ user account on the Cisco VCS with the same URI as the Lync user.
    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 Server’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
Confirm password	As Initial password
FindMe type	*Individual*

24. Make sure the domain shared with the Lync Server is DNS resolvable, usually by adding the Lync server as a DNS server address on the Cisco VCS. See “Configure the DNS” above.
25. Configure the OCS Relay App on the Cisco VCS:
    a. Go to the **OCS Relay** page (**Applications >OCS Relay**).
    b. Configure the following fields:

OCS Relay mode	On
OCS Relay domain	**test-customer.com**
OCS Relay routing prefix	Lync

Note: OCS Relay can take up to 3 minutes to pick up a new OCS Relay FindMe™ entry and register it. If a number of entries are deleted and the same number are added, it can take OCS Relay up to 60 minutes to observe the change in identities and update the registrations.

Verify FindMe™ accounts are registered

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

1. Go to the **OCS Relay status** page (**Status > Applications > OCS Relay**).
2. Verify the following for each FindMe™:
    - Registrations state is Registered
    - Subscription state is Active
    - Presence state is Online

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

Testing the Configuration

- Test that calls to Lync Server 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 Server 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.
- Test that the presence of Cisco VCS endpoints is reflected in Lync presence – log out of the Lync client for a user and check that the Off-Line, Available and In-Call status of the Cisco VCS endpoint listed in the relevant FindMe™ is presented as the presence state in a Lync client watching presence for that user.

Appendix 1 - Troubleshooting

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 admin or user policy or cpl
   - 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

   it is likely that 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: 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**).

Real time detailed event log

To obtain a more detailed log of key events and errors, start up netlog level 1 logging and then try the call or initiate a presence action.

1. Log in to Cisco VCS Control as **admin** using an SSH or Telnet connection.
2. At the prompt type:
   `netlog 1`
3. To turn off tracing, at the prompt type:
   `netlog off`

Information displayed between typing netlog 1 and netlog off contains the key events and error messages that occurred between those two times.

Tracing calls

Tracing calls at SIP / H.323 level

1. Log in to Cisco VCS Control as **admin** using an SSH or Telnet connection.
2. At the prompt type:
   `netlog 2`
3. To turn off tracing, at the prompt type:
   `netlog off`

Information displayed between typing netlog 2 and netlog off contains the SIP and H.323 messaging received and sent out by the Cisco VCS.

Information displayed by netlog 2 includes the key event and error message information reported by netlog 1. Viewing netlog 1 and netlog 2 information separately can be useful so that netlog 1 messages are not lost within the detailed SIP / H.323 messaging.

Presence not observed as expected

Presence Server status

- To check who is providing presence information to the Cisco VCS Presence Server:
  - Go to **Status > Presence > Publishers**
- To check whose presence is being watched for (on domains handled by Cisco VCS Presence Server):
  - Go to **Status > 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 > 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 logged out and logged 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 syslog 1 log. If there are still problems, trace the SIP messaging using syslog 2.

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

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

Lync Server 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 netlog 2 trace, an indication that the device is in Microsoft mode is the presence of a “proxy=replace” field in the contact header of the OK from the device.)

Call connects but clears after about 25 seconds

If a call connects but almost immediately clears, this is likely to be because the ACK to the OK is not getting through.

Cisco VCS to Lync Server calls fail – DNS Server

Cisco VCS needs to have details about DNS names of Lync Server pools etc, and so needs to have one of its DNS entries set to point to the Lync Server ’s DNS server. (On Cisco VCS go to **System > DNS**, and check the **DNS server address**).

Cisco VCS to Lync Server calls fail - HLB

If the Lync Server 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 Cisco VCS will be with the FEP. Cisco 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 Server clears the call after the SIP timeout due to the FEP not seeing the ACK.

(Calls Lync – registered to the FEP – to Cisco VCS may still work.)

Calls between Lync and an endpoint that is not registered to the Lync Server gateway Cisco VCS clear shortly after connecting

Check that **Call routed mode** is set to *Always* on the **VCS configuration > Calls** page.

One way media: Lync → endpoint registered to Cisco VCS

When using Microsoft Edge Server

When Lync registers to Lync Server through a Microsoft Edge Server, the local IP address and port that the Lync declares are usually private and un-routable (assuming that Lync is behind a firewall and not registered on a public IP address). In order to identify alternate addresses to route media to, the Lync uses ICE candidates.

Handling Lync ICE candidates is not supported in Cisco VCS up to and including Cisco VCS X6.1.

Calls should connect OK, and media should flow from Lync to the video endpoint. Audio and video from the endpoint are unlikely to be received by Lync, because the destination information is encoded in the Lync ICE candidate lines.

When using a Hardware Load Balancer in front of Lync Server

Cisco VCS modifies the application part of INVITEs / OKs received from Lync to make them compatible with traditional SIP SDP messaging. Cisco VCS only does this when it knows that the call is with Lync Server. If there are problems with one-way media (media only going from Lync to the Cisco VCS registered endpoint), check the Search history and ensure that the call is seen coming from an Lync Server neighbor zone.

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 IPs.

Lync Server rejects Cisco 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 Server doesn’t trust the sender of the message.
- A response ‘401 Unauthorized’ response to OPTIONS is another indication that Lync Server doesn’t trust the sender of the OPTIONS message.

Ensure that the Cisco VCS sending these messages is included in the Lync Server’s topology > trusted application list.

Note, this can be seen if a load balancer is used in front of the Lync Server , and Lync Server is configured with the application trust authorizing the Cisco VCS – Lync Server sees calls coming from the hardware load balancer rather than from the Cisco VCS. See *Appendix 13 – Cisco VCS and hardware load* balancers.

Lync Server stays in ‘Connecting …’ state

MOC does not change into the connected state until it receives RTP (media) from the device it is connecting to.

No audio on audio call through an ISDN gateway

- Upgrade Cisco TelePresence ISDN GW to version 1.5.

Prior to version 1.5 the ISDN GW sent RTP traffic from SSRC = 0; Lync would not accept RTP traffic with SSRC = 0.

From version 1.5 the ISDN GW sends RTP traffic from a random, non zero, SSRC and Lync receives this correctly.

No video through an ISDN gateway

Some ISDN endpoints initiate a call using one set of codecs, then before media is sent, change the codecs to better codecs (for example an initial offering of H.261 is updated to H.263). Lync doesn't accept a change in codec before media is sent.

To work around this, "Meet me" on a conference, so that the ISDN endpoint sets up a call and connects to the MCU and Lync sets up a call and connects to the MCU independently.

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

In Some Lync Server configurations, especially where Lync Server PSTN gateways are used, calls are only allowed to be made if the calling party is authorized. This actually means that the calling party's domain must be the Lync Server 's 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 Server 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 Lync Server and in the FindMe™ configuration **Caller ID** is set to *FindMe ID* (instead of *Incoming ID*).

Lync endpoints try to register with Cisco 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 uses:

- _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 only supports TLS connection to the Edge Server. The _sip._tcp.<domain> DNS SRV record should be used for the Cisco VCS Expressway. Configure Lync to use encryption (set Lync Server to 'Supports encryption' – as specified in the configuration process).

OCS Relay problems

OCS Relay FindMe™ users take a long time to register.

OCS Relay can take up to 3 minutes to pick up a new OCS Relay FindMe™ entry and register it. If a number of entries get deleted and the same number get added, it can take OCS Relay up to 60 minutes to observe the change in identities and update the registrations.

OCS Relay FindMe™ users fail to register.

If OCS Relay 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.
3. The Cisco VCS **SIP registration proxy mode** is set to *Proxy to known only* (or *Proxy to any*).
4. That there is no transform that may be inadvertently corrupting the registration – e.g. appending an **@domain** to a name which contains no @ (as registrations proxied to Lync Server have a URI which is the **domain** only - no @).
5. Check CPL is as defined in the 'OCS Relay configuration of "Lync gateway" Cisco VCS(s)' section.
6. Check that the zone details have been updated as defined in 'OCS Relay configuration of "Lync gateway" Cisco VCS(s)'.

Troubleshooting OCS Relay

OCS Relay produces an event log file that contains useful information about its operation.

This is only available through root login to Cisco VCS. It is a big file and so it is usually best to 'tail' the file to look at the last few entries.

To view the last 300 entries of the OCS Relay log file:

1. Login as root on Cisco VCS
2. Type:
   ```
   tail -300 /mnt/harddisk/log/elbe.log
   ```

Lync Server 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 may be found at: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=030548df-0dc7-4f86-b8a9-2f5ec8de8ba5

Lync Server stops running after an upgrade

Ensure that Automatic upgrades are turned off. There are occasions when an upgrade comes through which will affect operation of Lync Server. Check the validity of the upgrade before installing.

Problems with certificates

When creating certificates to load onto Cisco VCS for use with Lync Server (e.g. purchased from a certification authority) it is vital that the Subject Name contains the Lync Gateway FQDN (Lync Gateway cluster FQDN if present), and the Subject Alternate Name contains the FQDN for all Lync Gateways if part of a cluster.

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.

Appendix 2 – 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 Server 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 up-speed to video.

Note that:

- Interworking a Lync client to an H.323 endpoint, the call will only up-speed from voice to video if the up-speed 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. See the "Cisco VCS Multiway™ deployment guide".

Cisco VCS Cluster and OCS Relay

The OCS Relay feature is able to run in a cluster of Cisco VCS peers from version X5.

Appendix 3 – Benefits of using Cisco VCS with Lync Server

Separate management of video systems and PC based systems

Video managers can manage the video endpoints in the Cisco VCS environment that they know, and IT managers can focus on managing the PCs without needing to learn about video.

Cisco VCS brings H.323 integration to Lync Server

Lync Server works with SIP. Cisco VCS Control works with SIP and H.323 and can interwork H.323 calls to SIP calls allowing H.323 endpoints to be used in the Lync Server environment.

Duo Video

Sharing presentations in a conference is not supported in Lync Server, but it is supported by Cisco VCS.

Bandwidth management

The Cisco VCS uses the concept of pipes which allow you to apply bandwidth restrictions to a link. This ensures that calls are not attempted if they would overload a link's bandwidth. If a link's bandwidth would be exceeded, the call may be diverted to a different zone (link), down-sped to a lower bandwidth or rejected – depending on configuration.

The Cisco VCS bandwidth management operates on calls where:

- media traverses the Cisco VCS (traversal subzone)
- the source or destination device is in the Cisco VCS's local zone (default subzone, and IP addresses specified by explicit subzones)

For other calls, e.g. neighbor zone to neighbor zone non-traversal calls, where Cisco VCS has no idea of where or how the media is routed, it cannot perform bandwidth management.

FindMe™

FindMe™ allows users to set up groups of video endpoints / phones to ring when a call arrives. So, for example, the video phone can ring at the office, in the home office and on the laptop soft video phone at the same time – giving the highest likelihood of the person being able to answer their video call.

FindMe™ also allows devices to be called if the primary set are not answered or are busy, for example, to route them through to a mobile phone or video mail so that the call can always be handled.

FindMe™ can be configured such that calls from any device in the FindMe™ active location will present the FindMe™ ID as the caller ID

Appendix 4 – Known interoperating limitations

Video codecs

If Lync client is used, then the video endpoints registered to the Cisco 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.)

Video codec selection

When the Cisco VCS Control receives an H.323 call destined for Lync Server , the Cisco VCS must interwork the call to SIP and generate a SIP INVITE to send to the Lync Server. Lync Server does not support INVITES with no SDP – in other words, without a list of codecs that can be used for the call, so the Cisco VCS Control must populate the SDP with a “pre-chosen” list of codecs from which the Lync Server can select.

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

Joining a MOC conference (AV MCU)

Using a Lync client to invite a third party to join the call does not work whether the third endpoint is the endpoint registered to the Cisco VCS Control or whether the endpoint registered to the Cisco 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 Cisco 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 the Cisco VCS Multiway™ deployment guide.

Up-speeding from a voice call to a video call

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

Lync clients accessing Lync Server through Microsoft Edge Server

When Lync client registers to Lync Server through a Microsoft Edge Server, the SDP from Lync contains Microsoft ICE candidates, and the non local candidate needs to be used.

This functionality is not supported in Cisco VCS X6.1. Calls made from an endpoint registered to Cisco VCS to Lync should work, but calls made from Lync to an endpoint registered to Cisco VCS are likely to result in audio and video on the endpoint registered to Cisco VCS, but no video or audio on Lync.

Microsoft Mediation Server

Using Lync Server

Calls to Microsoft Mediation Servers work from endpoints in the Cisco 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 Cisco 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 Cisco VCS: make a second zone to Lync Server, 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 select 'Searches are automatically responded 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 Microsoft Office Communications Server 2007 zone.

Cisco VCS Cluster without OCS Relay

Lync Server does not have a way of load balancing calls to a cluster of Cisco VCSs. There is no way to tell Lync Server that there are multiple peers to receive calls for the Cisco VCS domain, and Lync Server will not load balance on a DNS SRV record, and there is a limit in Lync Server (and Windows) that the min TTL on Round Robin DNS is 5 minutes.

Use of Cisco VCS clusters with Lync Server and without OCS Relay therefore provides resilience, not extra capacity.

No audio on audio call through an ISDN gateway

Prior to version 1.5 the Cisco TelePresence ISDN GW sent RTP traffic from SSRC = 0; Lync would not accept RTP traffic with SSRC = 0. From version 1.5 the ISDN GW sends RTP traffic from a random, non zero, SSRC and Lync receives this correctly.

Lync client receives no video if it holds and then resumes a call

Lync does not request fast picture updates and so unless full frames are automatically sent from time to time by endpoints this results in no video on the Lync.

Video will be seen by Lync when using:

- MXP F8.0 or later SIP - as this supports the auto-generation of full video frames
- Ex/C-Series TC3 or later – as this supports the auto-generation of full video frames
- Cisco VCS X4.2 or later for calls interworked with H.323 endpoints – as Cisco VCS interworking supports the auto-generation of full frame update requests

Even with these fixes, sometimes Lync complains that it has no audio device configured when selecting resume … follow Lync's instructions to update the audio device and resume will then work.

Microsoft Server

Microsoft Servers recommended are:

Operating Systems for Server Roles

- Microsoft Lync Server 2010 supports the 64-bit editions of the following operating systems:
  - Windows Server 2008 R2 Standard operating system
  - Windows Server 2008 R2 Enterprise operating system
  - Windows Server 2008 R2 Datacenter operating system
  - Windows Server 2008 Standard operating system with Service Pack 2 (SP2)
  - Windows Server 2008 Enterprise operating system with SP2
  - Windows Server 2008 Datacenter operating system with SP2

Note: Lync Server 2010 is available only in 64-bit, which requires 64-bit hardware and 64-bit editions of Windows Server. Lync Server 2010 is not available in a 32-bit version.

Call forward from Lync to a Cisco 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 Cisco VCS registered endpoint or a FindMe then Cisco VCS sees this as a looped call.

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

For scenarios where:

- 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 to a SIP destination

the call will fail because Lync Server does not like the caller ID (From: header) being modified.

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

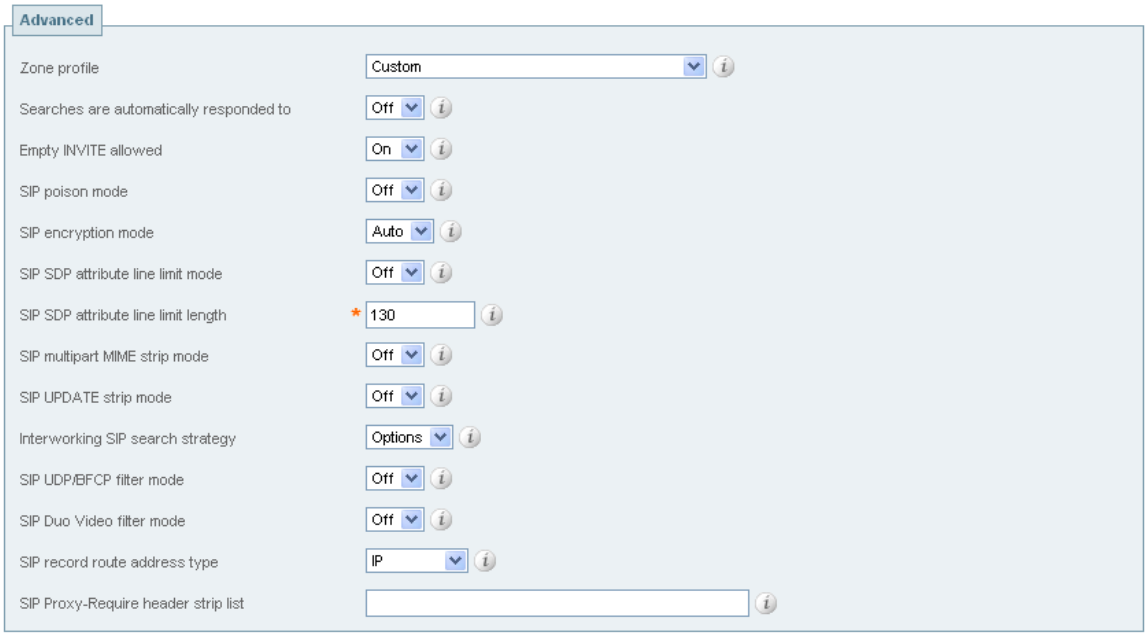
Best practice is that a Lync endpoint should never be included as a FindMe device. If MOC devices and video endpoints are to be related, OCS Relay should be used and a FindMe ID which is the same as the Lync URI should be created.

Appendix 5 – Advanced parameters set by selecting zone profile ‘Microsoft Office Communications Server 2007’

By setting the **Zone profile** to **Microsoft OCS 2007**, the following Advanced zone parameters are set:

Searches are automatically responded to	*Off*
Empty INVITE allowed	*Off* See “*Appendix 6 – Setting default codecs for H.323 to SIP calls”* to modify codecs offered in the initial INVITE.
SIP poison mode	*On*
SIP encryption mode	*Off*
SIP SDP attribute line limit mode	*On*
SIP SDP attribute line limit length	130
SIP multipart MIME strip mode	*On*
SIP UPDATE strip mode	*On*
Interworking SIP Search Strategy	*Info*
SIP UDP/BFCP filter mode	*Off*
SIP Duo Video filter mode	*On*
SIP record route address type	*Hostname*
SIP Proxy-Require header strip list	<Blank>

If these need to be modified, select custom zone and configure as required:



Appendix 6 – Setting default codecs for H.323 to SIP calls

Codecs to be offered

H.323 video calls typically do not provide codec information until after the call has connected. By contrast, in SIP, the codec information exchange is typically started in the original INVITE. By default, when interworking an H.323 call to a SIP call, Cisco VCS Control will start the SIP interworked call with an INVITE which has no SDP, requesting that the called party initiates the codec offering.

Microsoft Lync Server does not accept a SIP INVITE without an SDP.

Setting **Empty INVITE allowed** to **Off** in the Cisco VCS Control's **Edit Zone** page (**VCS Configuration > Zones >** Lync **Neighbor**) instructs Cisco VCS Control to put an SDP into the INVITE, and therefore to propose a set of codecs to use.

The default set of codecs to use are codecs supported by Lync Server ; if, however, a change is required the set of codecs proposed can be configured from the Command Line Interface.

The default audio codec to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Audio
   DefaultCodec:
   <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48
   /G723_1/G728/G729/AALCD_48/AALCD_56/AALCD_64/AMR>
```

… note only a single codec may be selected.

The default video codec to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Video
   DefaultCodec: <None/H261/H263/H263p/H263pp/H264>
```

… note only a single codec may be selected.

The default bit rate to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Video
   DefaultBitrate: <64..2048>
```

… note only a single bit rate may be selected.

The default resolution to offer is configured using:

```
xConfiguration Zones Zone [1..200] Neighbor Interworking SIP Video
   DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>
```

… note only a single resolution may be selected.

Appendix 7 – Presence with and without transforms

Presence SIP messages often have extra parameters in the URI header after the user-id@domain. In order to ensure that these extra parameters do not cause the search rules to fail to match, a '**.***' is appended to pattern strings.

Lync Server receiving Presence from non-OCS Relay FindMe™ entries, where there is no transform for Cisco VCS devices accessing Lync Server

For example, where to reach a Lync user1@test-customer.com the video endpoint calls user1@test-customer.com

The documentation above specifies the required configuration to allow calls and presence to be routed when the video network device calls the Lync endpoint's registered name to call it.

Lync Server receiving Presence from non-OCS Relay FindMe™ entries, where there is a transform for Cisco VCS devices accessing Lync Server

For example, where to reach a Lync user1@test-customer.com the video endpoint calls user1@lync.domain

If a search rule has been created with a domain name transform, for example to allow callers to dial user1@lync.domain as well / instead of user1@test-customer.com, an additional search rule with a pattern string for the raw domain (in this example .*@test-customer.com.*) must be added to allow presence messages through (Lync Server requests that the presence Notifies are sent to the Lync Server 's raw domain).

Allowing calls to the raw domain as well as the pre-transform domain is also useful for endpoints supporting dial back to caller. The calling party's caller identity will contain the raw domain information.

For example, if non OCS Relay set Search Rule 1 as follows:

Priority	100
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	(.*)@lync.domain
Pattern behavior	*Replace*
Replace string	\1@test-customer.com
On successful match	*Stop*
Target zone	*Lync*

Add a second search rule:

Priority	100
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*

Pattern string	.*@test-customer.com.*
Pattern behavior	*Leave*
On successful match	*Stop*
Target zone	*Lync*

Appendix 8 – TEL URI handling for Cisco VCS to Lync Server 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 Server to be able to look it up.

Lync Server 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 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.

For a non OCS Relay system this can be implemented as follows:

Priority	80 (match in preference to the no transform needed rule - 80 is higher priority than 100)
Source	*Any*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	(1…)(@vcs.domain)?(.*) (@vcs.domain will exist in SIP originated calls but not in H.323 originated calls)
Patter behavior	*Replace*
Replace string	+44134478\1;@test-customer.com;user=phone\3
On successful match	*Continue*
Target Zone	*Lync*

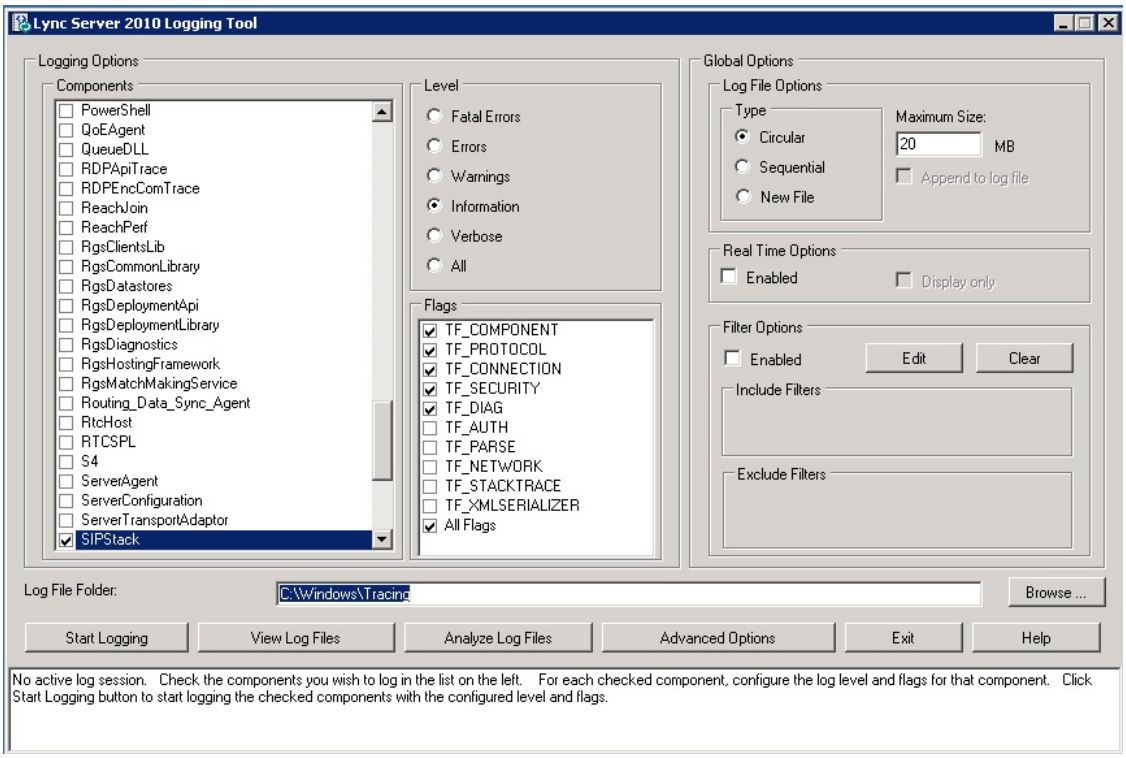
Appendix 9 – Debugging on Lync Server

Use of Lync Server Logging tool

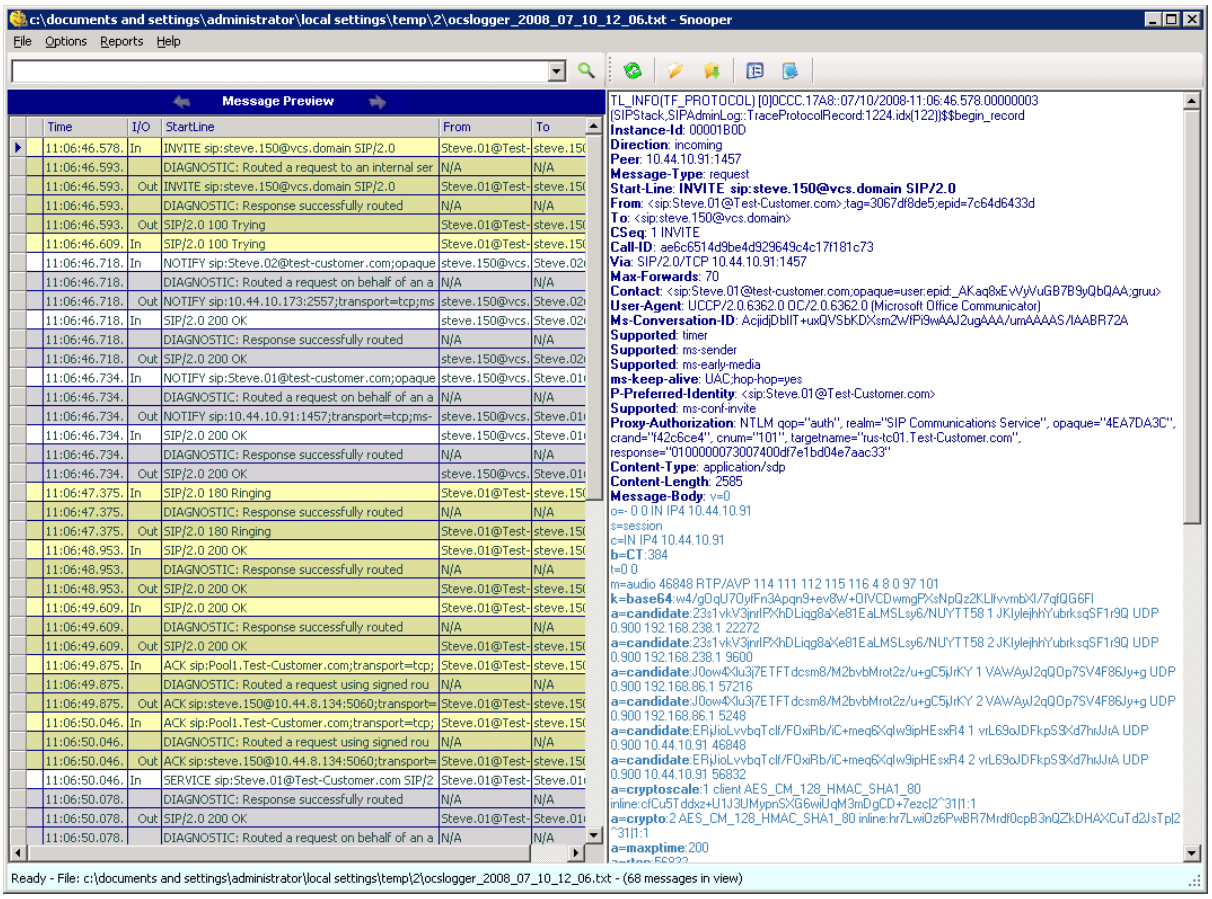
For debugging it is important to enable the logging on the appropriate Lync pool. If a Lync Director is in use, tracing here is a good starting point.

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

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



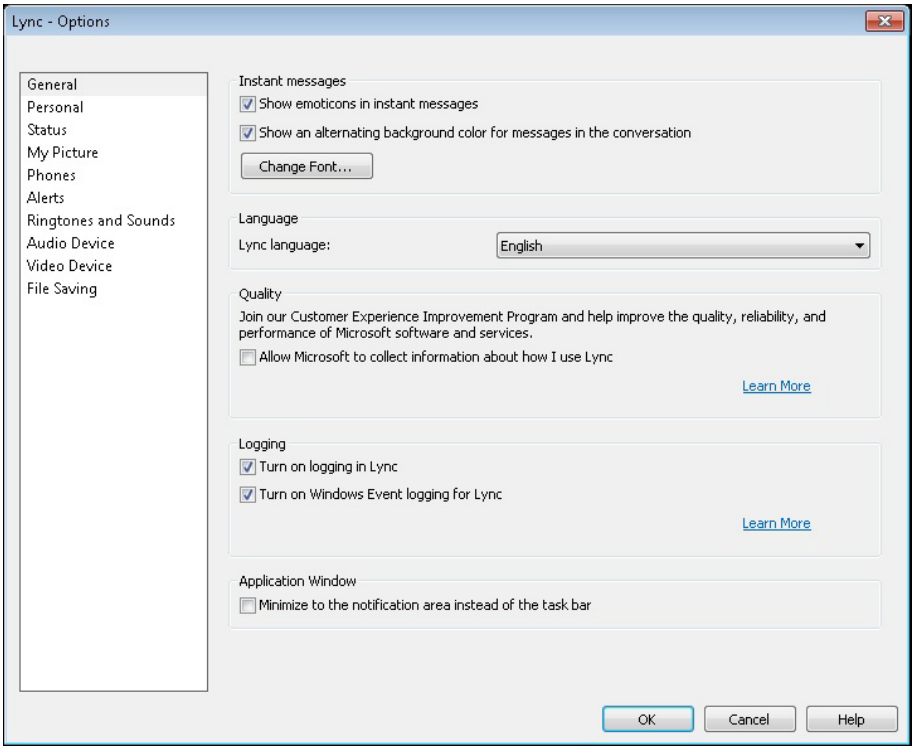
2. Select the logging option, for example SIPStack to look at SIP logs. (Details about all the logging options may be found at: http://technet.microsoft.com/en-us/library/bb936621.aspx)
3. Click **Start Logging**.
4. Make the call, or perform the function that needs to be debugged.
5. Click **Stop Logging**.
6. Click **Analyze Log Files** (install the Lync Server Resource Kit Tools if prompted to do so).
7. Review the trace:


c:\documents and settings\administrator\local settings\temp\2\ocslogger_2008_07_10_12_06.txt - Snooper
File Options Reports Help
Message Preview
Time I/O StartLine From To
11:06:46.578. In INVITE sip:steve.150@vcs.domain SIP/2.0 Steve.01@Test- steve.150
11:06:46.593. DIAGNOSTIC: Routed a request to an internal ser N/A N/A
11:06:46.593. Out INVITE sip:steve.150@vcs.domain SIP/2.0 Steve.01@Test- steve.150
11:06:46.593. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:46.593. Out SIP/2.0 100 Trying Steve.01@Test- steve.150
11:06:46.609. In SIP/2.0 100 Trying Steve.01@Test- steve.150
11:06:46.718. In NOTIFY sip:Steve.02@test-customer.com;opaque steve.150@vcs. Steve.02
11:06:46.718. DIAGNOSTIC: Routed a request on behalf of an a N/A N/A
11:06:46.718. Out NOTIFY sip:10.44.10.173:2557;transport=tcp;ms steve.150@vcs. Steve.02
11:06:46.718. In SIP/2.0 200 OK steve.150@vcs. Steve.02
11:06:46.718. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:46.718. Out SIP/2.0 200 OK steve.150@vcs. Steve.02
11:06:46.734. In NOTIFY sip:Steve.01@test-customer.com;opaque steve.150@vcs. Steve.01
11:06:46.734. DIAGNOSTIC: Routed a request on behalf of an a N/A N/A
11:06:46.734. Out NOTIFY sip:10.44.10.91:1457;transport=tcp;ms- steve.150@vcs. Steve.01
11:06:46.734. In SIP/2.0 200 OK steve.150@vcs. Steve.01
11:06:46.734. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:46.734. Out SIP/2.0 200 OK steve.150@vcs. Steve.01
11:06:47.375. In SIP/2.0 180 Ringing Steve.01@Test- steve.150
11:06:47.375. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:47.375. Out SIP/2.0 180 Ringing Steve.01@Test- steve.150
11:06:48.953. In SIP/2.0 200 OK Steve.01@Test- steve.150
11:06:48.953. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:48.953. Out SIP/2.0 200 OK Steve.01@Test- steve.150
11:06:49.609. In SIP/2.0 200 OK Steve.01@Test- steve.150
11:06:49.609. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:49.609. Out SIP/2.0 200 OK Steve.01@Test- steve.150
11:06:49.875. In ACK sip:Pool1.Test-Customer.com;transport=tcp; Steve.01@Test- steve.150
11:06:49.875. DIAGNOSTIC: Routed a request using signed rou N/A N/A
11:06:49.875. Out ACK sip:steve.150@10.44.8.134:5060;transport= Steve.01@Test- steve.150
11:06:50.046. In ACK sip:Pool1.Test-Customer.com;transport=tcp; Steve.01@Test- steve.150
11:06:50.046. DIAGNOSTIC: Routed a request using signed rou N/A N/A
11:06:50.046. Out ACK sip:steve.150@10.44.8.134:5060;transport= Steve.01@Test- steve.150
11:06:50.046. In SERVICE sip:Steve.01@Test-Customer.com SIP/2 Steve.01@Test- Steve.01
11:06:50.078. DIAGNOSTIC: Response successfully routed N/A N/A
11:06:50.078. Out SIP/2.0 200 OK Steve.01@Test- Steve.01
11:06:50.078. DIAGNOSTIC: Routed a request on behalf of an a N/A N/A
TL_INFO(TF_PROTOCOL) [0]0CCC.17A8::07/10/2008-11:06:46.578.00000003
(SIPStack,SIPAdminLog::TraceProtocolRecord:1224.idx(122))$$begin_record
Instance-Id: 00001B0D
Direction: incoming
Peer: 10.44.10.91:1457
Message-Type: request
Start-Line: INVITE sip:steve.150@vcs.domain SIP/2.0
From: <sip:Steve.01@Test-Customer.com>;tag=3067df8de5;epid=7c64d6433d
To: <sip:steve.150@vcs.domain>
CSeq: 1 INVITE
Call-ID: ae6c6514d9be4d929649c4c17f181c73
Via: SIP/2.0/TCP 10.44.10.91:1457
Max-Forwards: 70
Contact: <sip:Steve.01@test-customer.com;opaque=user:epid:_AKaq8xEvVyVuGB7B9yQbQAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office Communicator)
Ms-Conversation-ID: AcjidjDblIT+uxQVSbKDXsm2WfPi9wAAJ2ugAAA/umAAAAAS/IAABR72A
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
P-Preferred-Identity: <sip:Steve.01@Test-Customer.com>
Supported: ms-conf-invite
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service", opaque="4EA7DA3C",
crand="f42c6ce4", cnum="101", targetname="rus-tc01.Test-Customer.com",
response="0100000073007400df7e1bd04e7aac33"
Content-Type: application/sdp
Content-Length: 2585
Message-Body: v=0
o=- 0 0 IN IP4 10.44.10.91
s=session
c=IN IP4 10.44.10.91
b=CT:384
t=0 0
m=audio 46848 RTP/AVP 114 111 112 115 116 4 8 0 97 101
k=base64:w4/g0qU7OyfFn3Apqn9+ev8W+OIVCDwmgPXsNpQz2KLlfvvmbXl/7qfQG6Fl
a=candidate:23s1vkV3jnrlPXhDLiqg8aXe81EaLMSLsy6/NUYTT58 1 JKIylejhhYubrksqSF1r9Q UDP
0.900 192.168.238.1 22272
a=candidate:23s1vkV3jnrlPXhDLiqg8aXe81EaLMSLsy6/NUYTT58 2 JKIylejhhYubrksqSF1r9Q UDP
0.900 192.168.238.1 9600
a=candidate:J0ow4Xlu3j7ETFTdcsm8/M2bvbMrot2z/u+gC5jJrKY 1 VAWAyJ2qQOp7SV4F86Jy+g UDP
0.900 192.168.86.1 57216
a=candidate:J0ow4Xlu3j7ETFTdcsm8/M2bvbMrot2z/u+gC5jJrKY 2 VAWAyJ2qQOp7SV4F86Jy+g UDP
0.900 192.168.86.1 5248
a=candidate:ERjJioLvvbqTclf/FOxiRb/iC+meq6XqIw9ipHEsxR4 1 vrL69oJDFkpS9Xd7hrJJrA UDP
0.900 10.44.10.91 46848
a=candidate:ERjJioLvvbqTclf/FOxiRb/iC+meq6XqIw9ipHEsxR4 2 vrL69oJDFkpS9Xd7hrJJrA UDP
0.900 10.44.10.91 56832
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:cfCu5Tddxz+U1J3UMypnSXG6wiUqM3mDgCD+7ezcl2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:hr7LwiOz6PwBR7Mrdf0cpB3nQZkDHAXCuTd2JsTpl2
^31|1:1
a=maxptime:200
Ready - File: c:\documents and settings\administrator\local settings\temp\2\ocslogger_2008_07_10_12_06.txt - (68 messages in view)

Appendix 10 – Enable Debug on Lync

If Lync 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 11 – Endpoint specific configuration

T150

- Use code version L5.1 or greater.
- Set **Network > SIP Settings > Server Type** to **Auto** (not Microsoft).
- For versions prior to L6.0 set **Security > Encryption** to **Off.**

MXP 1000, MXP 1700, MXP 3000 and MXP 6000

- Use code version F7.0 or greater.
- Set **Network > LAN Settings > SIP Settings > SIP Server Settings > Server Type** to **Auto** (not Microsoft).

C20, C40, C60 and C90 (including T1 and T3 systems)

- Use code version TC2.0.0 or greater.
- Set **Advanced configuration > SIP > Profile 1 > Type** to **Standard** (not Microsoft).
- For versions up to and including 2.1.0 set Encryption = Off (not Best effort).

EX60 and EX90

- Use code version TC2.0.0 or greater.
- Set **Advanced configuration > SIP > Profile 1 > Type** to **Standard** (not Microsoft).
- For versions up to and including 2.1.0 set **Encryption** = *Off* (not *Best effort*).

E20

- Use code version TE2.0.0 or greater.
- Set **Advanced configuration > SIP > Profile 1 > Type** to **Standard** (not Microsoft).

Cisco TelePresence Movi

Movi 2

Movi 2 only supports H.264 video – MOC Clients do not support H.264; Movi can only make a video call to a MOC client if an IP gateway or an MCU is used to transcode between H.263 and H.264 media.

Movi 3 and Movi 4

Movi now supports H.263 – as supported by Lync Server. No special configuration is required.

Cisco TelePresence IP GW

- Use code version greater than 2.0(1.2).
- Set **SIP Registrar type** to **Standard SIP** (not Microsoft OCS/LCS).

Cisco TelePresence ISDN gateway

- Use code version 1.5 or greater.
- ISDN gateway is H.323 only and so calls between the gateway and Lync Server will be interworked by Cisco VCS.

Other endpoints

Other endpoints need to be tested for compatibility and required configuration. Although Cisco VCS does some manipulation of signaling data to make Microsoft SIP work with standard SIP and H.323 endpoints, Cisco VCS is not designed to fully insulate the Cisco VCS registered devices from Lync Server signaling nor Lync Server from the signaling of devices registered to the Cisco VCS.

The Polycom FX endpoint running version 6.0.5 code is known to generate H.263 video which is not compatible with Microsoft's Lync client. The Polycom FX v6.0.5 can only make a video call to a Lync client if an IP gateway (in transcoding mode) or an MCU is used to transcode the H.263 media.

Appendix 12 – Cisco TelePresence MCU configuration

MCU connectivity with Lync Server and Cisco VCS

MCUs must be registered to Cisco VCS in order for Lync callers to be able to join conferences.

OCS Relay

When OCS Relay is used, FindMe™ accounts can be set up for static conferences (for example if the In-Call presence status of the conference is wanted). For Ad hoc conferences (for example those created and used by Multiway™), a static route to the MCU's domain must be set up in order that calls can be routed to non FindMe™ destinations.

Configuration of Cisco VCS and MCUs registered to Cisco VCS

The configuration of both the Cisco VCS and the MCU documented in the 'Cisco VCS Multiway™ deployment guide' is the correct configuration for Cisco VCS and MCU when working with Lync Server Please see that document for further details.

Configuration of Lync Server to support Lync clients creating / joining ad hoc conferences

Ensure that Lync Server has a static domain route to the MCU's domain.

Appendix 13 – Cisco VCS and hardware load balancers in front of a bank of FEPs

Background

For Lync Server to scale to support large numbers of users, a pool of Front End Processors (FEPs) can be created for the Server system. Each FEP is then run on a separate piece of physical hardware so that the hardware resources of a single platform are no longer the limitation on call and IM processing.

So that endpoints (Lync clients, peer proxies etc) do not have to be individually configured to route their traffic to specific Front End Processors, a Hardware Load Balancer (HLB) is used to share out the traffic amongst the FEPs. The HLB provides a single virtual IP address for all of the FEPs.

When a HLB is sent data (like a SIP message), it uses an algorithm to decide where to route that message.

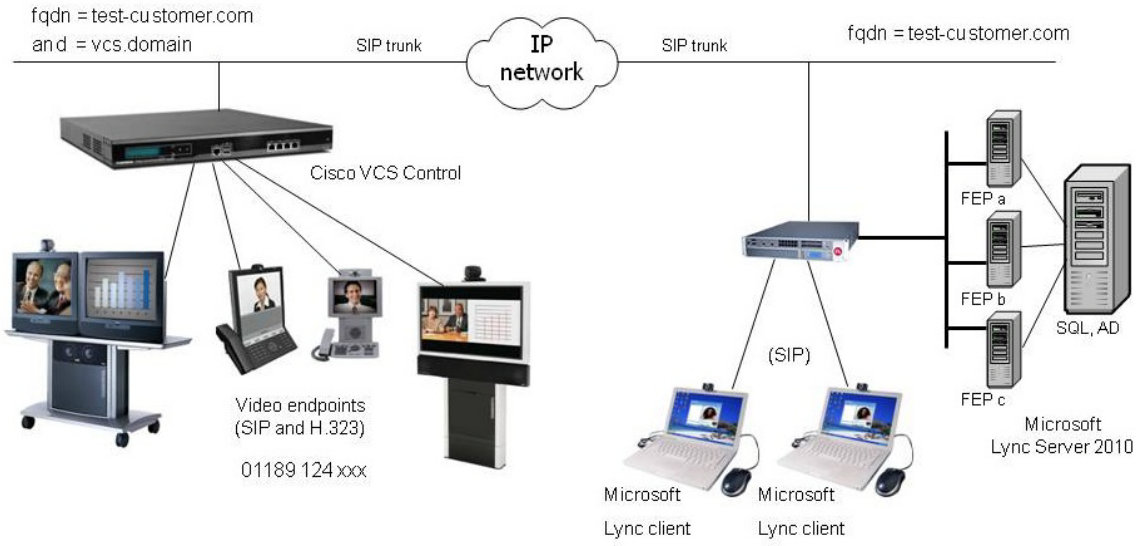
- Frequently source address routing is initially used, so that if a device has already communicated with an FEP (within the recent past) any further traffic from that device will also be routed to that same FEP.
- If source address routing does not define which FEP to send the message to, then either round-robin, or another more sophisticated algorithm that can tell the loading of the FEP will be used to find an appropriate FEP to route this new communication to.
- Some hardware load balancers have the ability to receive SIP traffic, and rather than routing it based on source address can route it based on the SIP device it relates to (allowing load balancing of SIP traffic from a proxy, like Cisco VCS).

The HLB will perform destination address NATing, meaning that messages addressed to the hardware load balancer's (virtual) IP address will be re-addressed to the required FEP.

Many load balancers also perform source address NATing by default in order to get replies for outside devices routed back via the load balancer, so that the outside device (Cisco VCS, for example) sees responses coming from the single IP address that it knows to be "Lync Server".

The content of any messaging is left unchanged.

Example infrastructure is shown below:



When connecting a Cisco VCS to a Lync system, Lync Server requires that a host peer proxy (like the Cisco VCS) is authorized to communicate with the Lync Server FEP. Peer proxies are treated as Applications.

On Lync Server:

1. Select **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Management Shell**.
2. Set a Lync Gateway VCS as a trusted application for Lync Server (VCS is treated as an application by Lync).
   - Use the command "`New-CsTrustedApplicationPool`" with the following parameters:

     `-Identity`: specifies the FQDN of the Lync Gateway VCS (or Lync Gateway VCS Cluster name if present). 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`: it 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.LYNC>New-CsTrustedApplicationPool -Identity
     vcs.test-customer.com -Registrar LyncPool01.test-customer.com -site 1
     -RequiresReplication $false -ThrottleAsServer $true -
     TreatAsAuthenticated $true
     ```
3. 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 TCP port to be used for neighboring (should be 5061, if TLS)

     For example:

     ```
     C:\Users\administrator.LYNC>New-CsTrustedApplication -ApplicationID
     VCSApplication1 -TrustedApplicationPoolFqdn vcs.test-customer.com -
     Port 5061
     ```
4. Allow encryption to be negotiated
   - Use the command "`set-CsMediaConfiguration`" with the following parameters:

     `-EncryptionLevel`: specifies that encryption is not mandatory

     For example:

     ```
     C:\Users\administrator.LYNC> set-CsMediaConfiguration -
     EncryptionLevel supportencryption
     ```
5. Apply the configuration
   - Use the command "`Enable-CsTopology`".

     For example:

     ```
     C:\Users\administrator.LYNC>Enable-Cs-Topology
     ```

For outbound messaging from Lync Server (to non registered devices) a static route needs to be set up.

6. Create a static route

   - Use the command "`New-CsStaticRoute`" with the following parameters:

     `$=`: the label referring to this specific new route.

     `-TLSRoute`: specifies that the route is TLS

     `-TCPRoute`: specifies that the route is TCP

     `-Destination`: "" specifies the Lync Gateway VCS FQDN (or Lync Gateway VCS Cluster name if present) 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 TCP port to be used for neighboring (should be 5061)

     `-UseDefaultCertificate`: specifies to use the default certificate assigned to the Front End (must be $true)

     For example:

     ```
     C:\Users\administrator.LYNC> $Route1=New-CsStaticRoute -TLSRoute -
     Destination "vcs.test-customer.com" -MatchUri "VCSsipdomain.lab" –
     Port 5061  -UseDefaultCertificate $true
     ```

7. 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 before to the specified Identity (note that brackets are curly)

     For example:

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

8. Verify static route assignment

   - In order to verify the correct assignment of the route use the command "`Get-CsStaticRoutingConfiguration`".

     For example:

     ```
     C:\Users\administrator.LYNC> Get-CsStaticRoutingConfiguration
     ```

     Identity: Global

     Route: {MatchUri=VCSsipdomain.lab;MatchOnlyPhoneUri=False;Enabled=True;ReplaceHostInRequestUri=False}

If a static route is set to TLS that link must have certificates that authenticate that the connection comes from the stated FQDN. The certificate must be created externally and loaded onto Cisco VCS – see "Cisco VCS deployment guide - Certificate creation and use with Cisco VCS").

In SIP signaling, the messaging from endpoints registered to Cisco VCS communicating with Lync Server contains route headers that direct responses to the Cisco VCS – bypassing the HLB. If the Cisco VCS is in the same subnet as the FEPs and the HLB, the FEPs route the SIP messages directly back to the Cisco VCS rather than through the HLB.

TLS connection

When a TLS connection is made through the load balancer, the load balancer routes the whole TLS stream through to the same destination device (FEP). If the FEP were to fail then the load balancer would route the TLS traffic to an alternative FEP. Having all traffic routed to the same FEP is not a disadvantage in that the majority of traffic into Lync Server is from Lync clients, and it is these that need to be balanced across FEPs. The HLB provides the resilience required for the Cisco VCS such that if an FEP fails, Cisco VCS will be routed to another FEP, and in fact all traffic going through a single FEP makes following the signaling path easier in case debugging is required.

Responses directly from devices behind a Hardware Load Balancer

If Source Address NATing is enabled on the HLB, responses to messages (like TRYING to an INVITE) will be routed back to the Cisco VCS via the HLB because the new transaction will be sent to the 'From' address, however, mid dialogue requests (like Re-INVITE and BYE) will be sent to the Cisco VCS directly because they will be sent to the device identified in the Record-route header.

Authentication with TCP

Trusting a VCS IP address (the alternative to communicating over TLS) is a security risk if the HLB is performing Source Address NATing, because in this case the FEPs will have to Trust the IP address of the HLB, and so any message sent via the HLB would be treated as trusted.

If Source Address NATing is not enabled on the HLB then the IP address of the Cisco VCS can be trusted.

Appendix 14 – Cisco VCS and Microsoft Lync Director

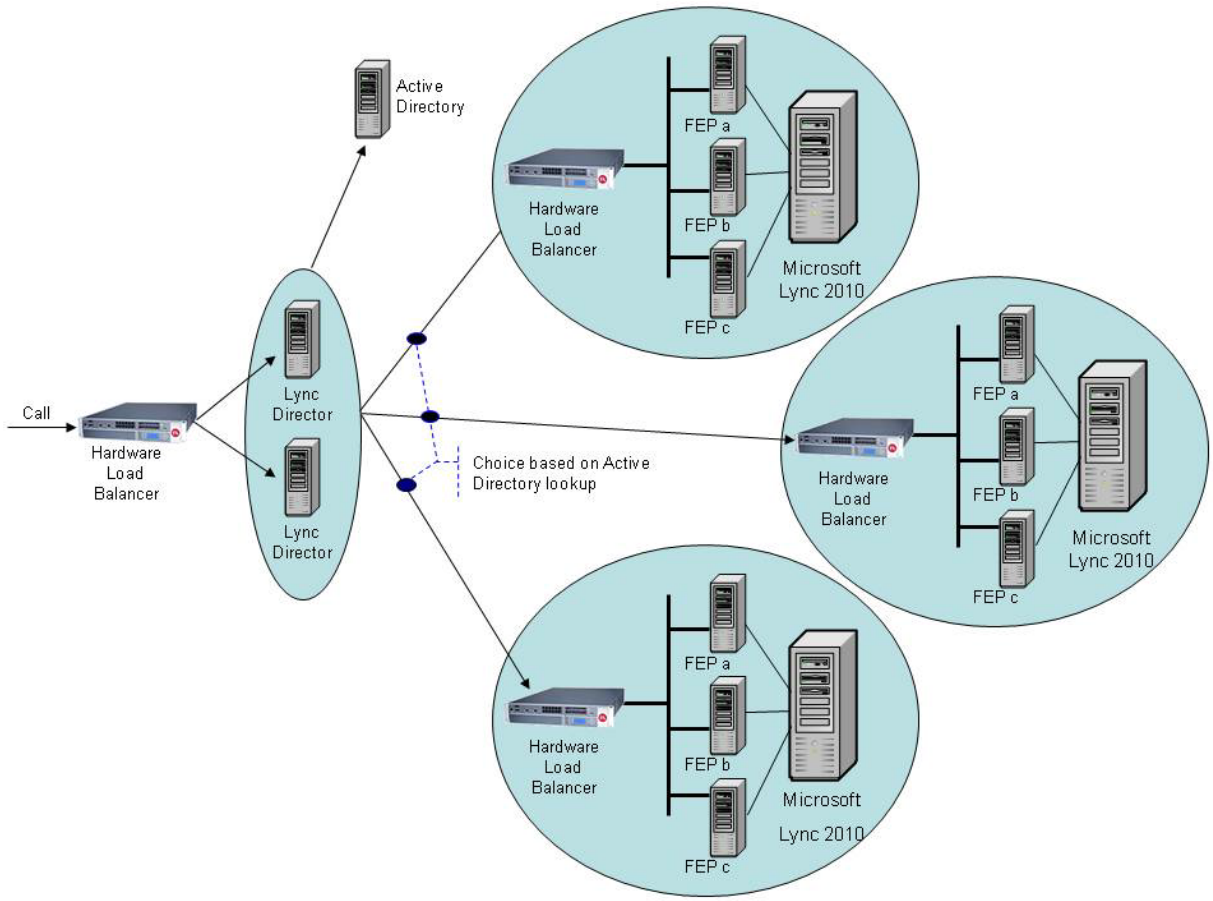
Background

Microsoft recommends that Lync Director is deployed when an organization hosts multiple Standard Edition Servers or Enterprise pools.

Microsoft Lync Director accesses the AD domain controllers for the whole network and can therefore both authenticate incoming requests, and also directs them to the appropriate enterprise pool or Standard edition server.

If a Director is not used, calls will use up resources on the Enterprise pool or Standard Edition Server that the call is initially received on, as that device will proxy the call to the correct home pool / server (remaining in-line). Not using Director thus uses resources on two devices rather than just the one and so affects the maximum capacity that the deployment can support.

Enterprise pools use Hardware Load Balancers (HLBs) to balance traffic across Front End Processors within that Enterprise Pool.



When handling a Register request, Director matches the source caller to their home Pool / standard edition server and uses a 301 response (permanently moved) to the initiator of the message to make them route this and future messages for this caller to the correct Pool / standard edition server.

When used with Cisco VCS the Lync Director should be configured to be the receiver of calls from the "Lync gateway" Cisco VCS and the source of calls from Lync Server to the "Lync gateway" Cisco VCS (see configuration sections in the main part of this document).

When used with a Microsoft Edge Server, Lync Director proxies messaging (not requesting a redirect) as endpoints outside the home network cannot be re-directed to communicate with another internal IP address which is not exposed to the public internet.

Configuration

Configure the "Lync Gateway" Cisco VCS(s)

Configuration of the "Lync Gateway" Cisco VCSs is described in the main body of this document.

Configure Lync Director

Configuration of the "Lync Director" is described in the main body of this document.

Appendix 15 – Cisco VCS and Lync Server voicemail

Video endpoints picking up voicemail from Lync Server

If you want to pick up voicemail from Lync Server using a SIP video network endpoint rather than using Lync, this can be achieved by calling the Lync URI with "`;opaque=app:voicemail`" appended, e.g. `user1@test-customer.com;opaque=app:voicemail`

If the user is a FindMe™ ID (e.g. an OCS Relay FindMe™) then this call request will be forked back to all FindMe™ devices for that ID as well as Lync Server. Lync Server voicemail will answer the call and other devices will display a missed call.

To avoid Cisco VCS forking calls that are aimed for the voicemail system to the FindMe™ ID devices, a transform should be added to the Cisco VCS: prepend the domain portion of the URI with "lync." if the call is for voicemail. This forces the Cisco VCS to route the calls to Lync Server only.
e.g. `(.+)@(test-customer.com;opaque=app:voicemail.*) --> \1@lync.\2`

The SIP calling device must support RFC2833 telephone events for presenting DTMF in order to communicate with the Lync Server voicemail server.

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.

© 2011 Cisco Systems, Inc. All rights reserved.