Cluster creation and maintenance

Cisco TelePresence Deployment Guide

Cisco VCS X7.0.n

Cisco TMS 12.6 or later

D14367.12

January 2012

Contents

Document revision history

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

Revision	Date	Description
1	Up to December 2009	Releases for earlier versions of Cisco VCS.
2	December 2009	Updated for VCS X5.
3	May 2010	Updated for VCS X5.1.1 and TMS 12.6.
4	August 2010	Updated for VCS X5.2. Replace previous Appendix 12 (Upgrading debian packages - only required for X5.1.1) with a new Appendix 12 - NAPTR records overview.
5	October 2010	New document styles applied.
6	December 2010	Updated for VCS X6.
7	February 2011	Clarify this document refers to VCS X6.0 only, and to TMS 12.6 or later.
8	May 2011	Updated for VCS X6.1.
9	August 2011	Updated for VCS X7.0.
10	September 2011	Updated Appendix 3 – IP port and protocol numbers.
11	October 2011	Updated for X7.0.n.
12	January 2012	Various minor revisions and clarifications applied.

Introduction

Cisco TelePresence Video Communication Server (Cisco VCS) clusters are designed to extend the resilience and capacity of a Cisco VCS installation. Cisco VCS peers in the cluster share bandwidth usage, routing, zone, FindMe™ and other configuration among themselves. Endpoints can register to any of the peers in the cluster; if they lose connection to their initial peer, they can re-register to another peer in the cluster.

Call licensing is carried out on a per-cluster basis. Any traversal or non-traversal call licenses that have been installed on a cluster peer are available for use by any peer in the cluster. If a cluster peer becomes unavailable, the call licenses installed on that peer will remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster — however, note that each peer is limited by its physical capacity (500 non-traversal calls and 100 traversal calls).

Every Cisco VCS peer in the cluster must have the same routing capabilities — if any Cisco VCS can route a call to a destination it is assumed that all Cisco VCS peers in that cluster can route the call to that destination. If the routing is different on different Cisco VCS peers, then separate VCSs / VCS clusters must be used.

This deployment guide describes how to create, modify and upgrade to X7.0.n VCS clusters. It provides information on how to:

- Upgrade VCS X1 / X2 Alternates to a VCS X7.0.n cluster
- Upgrade an X3 / X4 / X5.0 cluster to an X7.0.n cluster
- Upgrade an X5.1, X5.1.1 or X5.2 cluster to an X7.0.n cluster
- Upgrade an X6.0, X6.1, X7.0 or X7.0.n cluster to an X7.0.n cluster
- Create a new cluster of VCS X7.0.n peers
- Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)
- Remove a live Cisco VCS from a VCS X7.0.n cluster (permanently)
- Remove an out-of-service Cisco VCS from a VCS X7.0.n cluster (permanently)
- Disband a VCS X7.0.n cluster
- Change the master peer of a VCS X7.0.n cluster
- Change the IP address of a VCS X7.0.n peer

Note: In X3.x the use of Cisco TMS was essential to the correct operation of a VCS cluster because Cisco TMS was in control of copying configuration from the Master Cisco VCS to the non-master Cisco VCS peers.

In X4.1 the Cisco VCS performs the replication of configuration from Master Cisco VCS to non-master Cisco VCS peers and so use of Cisco TMS was optional for clustering. If provisioning was supported, Cisco TMS was needed.

In X5.x, X6.x and X7.0.n Cisco TMS is involved in initiating the environment for FindMe replication. Although not needed to replicate FindMe data throughout the cluster in a running environment, Cisco TMS is required to perform the initial distribution of the FindMe data throughout the cluster. Cisco TMS is also required if provisioning is to be supported on Cisco VCSs.

Note: Enabling provisioning and creating a cluster are two separate processes. If you intend to enable provisioning on your cluster, either:

- follow the instructions in this guide to create the cluster of Cisco VCSs (without provisioning enabled), and then follow the instructions in the Cisco TMS Provisioning Deployment Guide to enable provisioning across the cluster, or
- follow the instructions in the Cisco TMS Provisioning Deployment Guide to enable provisioning on what will be the Master Cisco VCS, and then follow the instructions in this guide to create the cluster of Cisco VCSs

For creating, modifying, and troubleshooting clusters that will remain X6.1 / X6.0 / X5 / X4.3 / X4.1 clusters, see:

- Cisco VCS Cluster Creation and Maintenance Deployment Guide (X6.1)
- Cisco VCS deployment guide - Cluster creation and maintenance (X6)
- Cisco VCS deployment guide - Cluster creation and maintenance (X5)
- TANDBERG VCS deployment guide - Cluster creation and maintenance (VCS X4.3)
- TANDBERG VCS deployment guide - Cluster creation and maintenance (VCS X4.1)

Prerequisites

Cisco VCS clusters peers must all run the same version of code, for example all X7.0.1, X7.0.2 or all X6.1. The only occasion where different peers should be allowed to run different versions of code is for the short period of time while a cluster is being upgraded from one version of code to another.

Before setting up a cluster of X7.0.n VCS peers or adding an X7.0.n VCS to a cluster, ensure that:

- a DNS SRV record is available for the cluster which contains A or AAA records for each peer of the cluster
- each and every Cisco VCS peer in a cluster is within a 15ms hop (30ms round trip delay) of each and every other Cisco VCS in or to be added to the cluster
- each and every Cisco VCS peer in a cluster must be directly routable to each and every other Cisco VCS in or to be added to the cluster. (There must be no NAT between cluster peers – if there is a firewall ensure that the required ports are opened.)
- all Cisco VCS peers have the same set of option keys installed
  - the number of call license keys may be different on different peers; all other license keys must be identical on each peer
  - the Cisco VCS must be restarted after installing some option keys in order to fully activate them
- the Cisco TMS version being run is TMS 12.6 or later (TMS 13.0 or later is recommended)
- each Cisco VCS has a different system name
- H.323 mode is enabled on each Cisco VCS (**VCS configuration > Protocols > H.323**, and for H.323 mode select On) – H.323 communications are used between cluster peers
- the Cisco VCS cluster has a DNS SRV record that defines all cluster peers
- the DNS servers used by the Cisco VCS peers must support both forward and reverse DNS lookups of Cisco TMS and all Cisco VCS peer addresses; the DNS servers must also provide address lookup for any other DNS functionality required (for example: system servers like NTP and the external manager that are configured using DNS names, Microsoft OCS/Lync Server FQDN lookup, LDAP server forward and reverse lookup); note that reverse lookups are frequently provided through PTR records
- If Cisco TMS is being used for replicating FindMe and/or Provisioning data, ensure that TMS Agent functionality has already been enabled on TMS (See the “TMS provisioning deployment guide” for details).

Upgrade VCS X1 / X2 Alternates to a VCS X7.0.n cluster

An upgrade from X1 / X2 alternates direct to an X7.0.n cluster is not possible, an upgrade from X1 / X2 to X5.2 must be performed first, then upgrade from X5.2 to X6.1, then upgrade to X7.0.n.

Follow the steps in “Upgrade VCS X1 / X2 Alternates to a VCS X5 cluster” in the “Cluster creation and maintenance guide (X5)”, upgrading the Cisco VCSs to X5.2, then follow the steps “Upgrade and X5.1, X5.1.1 or X5.2 cluster to an X6.1 cluster” in the “Cluster creation and maintenance deployment guide (X6.1)” and then return to this guide and follow the steps “Upgrade an X6.0, X6.1, X7.0 or X7.0.n cluster to an X7.0.n cluster”.

Upgrading VCS X1 / X2 Alternates to a VCS X7.0.n cluster is now complete.

Upgrade an X3 / X4 / X5.0 cluster to an X7.0.n cluster

An upgrade from an X3 / X4 / X5.0 cluster direct to an X7.0.n cluster is not possible, an upgrade from X3 / X4 /X5.0 to X5.2 must be performed first, then upgrade from X5.2 to X6.1, then upgrade to X7.0.n.

Follow the steps in “Upgrade a Cisco VCS X3 / X4 cluster to an X5 cluster (including Cisco TMS to 12.6)”, or the “Upgrade an X5.0 cluster to an X5.2 cluster” in the “Cluster creation and maintenance guide (X5)” to get to an X5.2 cluster, then follow the steps “Upgrade and X5.1, X5.1.1 or X5.2 cluster to an X6.1 cluster” in the “Cluster creation and maintenance deployment guide (X6.1)” and then return to this guide and follow the steps “Upgrade an X6.0, X6.1, X7.0 or X7.0.n cluster to an X7.0.n cluster”.

Upgrading a VCS X3 / X4 / X5.0 cluster to a VCS X7.0.n cluster is now complete.

Upgrade an X5.1, X5.1.1 or X5.2 cluster to an X7.0.n cluster

An upgrade from an X5.1 / X5.1.1 / X5.2 cluster direct to an X7.0.n cluster is not possible, an upgrade from X5.1 / X5.1.1 / X5.2 to X6.1 must be performed first, then upgrade from X5.2 to X7.0.n.

Follow the steps ""Upgrade and X5.1, X5.1.1 or X5.2 cluster to an X6.1 cluster"" in the "Cluster creation and maintenance deployment guide (X6.1)" and then return to this guide and follow the steps "Upgrade an X6.0, X6.1, X7.0 or X7.0.n cluster to an X7.0.n cluster".

Upgrading a VCS X5.1, X5.1.1 or X5.2 cluster to a VCS X7.0.n cluster is now complete.

Upgrade an X6.0, X6.1, X7.0 or X7.0.n cluster to an X7.0.n cluster

This procedure assumes that Cisco TMS, if used, is already running version 12.6 or later software and is operational with the X6.0, X6.1 or X7.0 cluster.

Note:

- Use of Cisco TMS is required if Device Provisioning or FindMe is to be used with this cluster.
- If the Cisco VCS is downgraded back to X6.0 or earlier from X6.1 or later, even after restoring the relevant backup, the VCSs will require re-clustering as the technique for sharing configuration data is different from X6.1.

Before the upgrade

For each Cisco VCS peer (including the Master):

1. Check the **Alarms** page (**Status > Alarms**) and ensure that all alarms are acted upon and cleared.

If Cisco TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each Cisco VCS peer:
   a. In the **TMS Agent Browser** panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the Cisco VCS peer.
   b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

Note: If authentication is intentionally enabled on the Cisco VCS, ignore the warning ‘verify that authentication is disabled on the VCS’

- If all tests are successful (all green check marks), proceed with the instructions below.
- If any errors are found (a red ‘X’ will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Upgrade Cisco VCS cluster peers to X7.0.n

Upgrade the Master peer

For the Master peer in the cluster:

1. Backup the Cisco VCS:
   a. If the VCS being backed up is version X6.1: log in as root on an SSH or other CLI interface. At the Cisco VCS command prompt, type:
   ```
   mkdir /tandberg/persistent/oti
   mkdir /tandberg/persistent/management
   ```
   b. Then perform a backup as described in “Appendix 1 – Backing up a Cisco VCS”.

Note: You should backup your system before upgrading. If at a later date you need to downgrade to an earlier version you will need to restore a backup made against that previous release.

2. Log in to the Master peer as admin on an SSH or other CLI interface. Enable maintenance mode; from the Cisco VCS command line type:

   ```
   xconfiguration SystemUnit Maintenance Mode: On
   ```

3. Log in to the Master peer as admin on the web interface.
4. Wait for all calls to clear and registrations to timeout on this master peer.
   If necessary, manually remove any calls on this peer that do not clear automatically (**Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
5. If necessary, manually remove any registrations from this peer that do not clear automatically (**Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).
   You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).
6. If TMS Agent Data Replication is enabled, enabling FindMe or Device Provisioning replication, on Cisco TMS:
   a. Select **Systems > Navigator** (and any required sub folders), then click on the Master Cisco VCS of the cluster.
   b. Select the **Clustering** tab.
   c. Ensure that all expected peers are shown in the **Cluster Peers** list.
   d. Clear the **Enable TMS Agent Data Replication on all Cluster Peers** check box.
   e. Click **Save Cluster Settings**.
   f. Review the status shown in **Administrative Tools > Activity Status** to ensure these tasks have completed successfully.

Note: This disables database replication from Cisco TMS to each cluster peer.

- Provisioning data will no longer be updated from Cisco TMS to the Cisco VCSs, however provisioning of endpoints from data cached on Cisco VCSs not in maintenance mode will continue.
- VCS cluster configuration replication will continue.
- VCS FindMe replication among Cisco VCS peers will STOP.

On the Master peer:

1. Upgrade and restart the Master Cisco VCS (**Maintenance > Upgrade**).
   For any further details see the "Upgrading Software" section of the Cisco VCS Administrator Guide.

Note: The web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if:

- Cisco VCS carries out a disk file system check – which it does approximately once every 30 restarts
- Provisioning is enabled, and database re-indexing is in progress

Upgrading of the software on the Master Cisco VCS is now complete.

Note: Do not worry about a “Cluster communication failure” alarm on the Master or any non-master peers – this is expected.

- The upgrade process disables the Cisco VCS’s provisioning functionality — provisioning will be restored later when **Enable TMS Agent Data Replication** is enabled.

If Cisco TMS is used, on TMS, ensure that TMS has all the correct settings for this upgraded Cisco by forcing a refresh of TMS:

1. Go to **Systems > Navigator** (and any required sub folders) and select the Master Cisco VCS.
2. Select the **Settings** tab.
3. Click **Force Refresh**.

If Cisco TMS is used and FindMe or Device Provisioning is required, enable replication on this upgraded master Cisco VCS peer.
On Cisco TMS:

4. Go to **Systems > Navigator** (and any required sub folders) then click on the master Cisco VCS.
5. Select the **TMS Agent** tab.
6. Select **Enable TMS Agent Data Replication**.
7. Ensure that **Authentication Scheme** is set to **Digest**.
8. Click **Save Settings**.

Note: This may take a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show the list of activities that are active, scheduled or in progress. Select the activity **Enable TMS Agent Data Replication for system(s) <name of system>**. This displays an activity log. Refresh this web page (button bottom left of this page) until the Activity Event completed successfully is reported.

- Do not worry about a message “Cluster replication error: cannot find master or this slave’s peer configuration file, manual synchronization of configuration is required” – this is expected while the cluster starts up. It should clear within 10 minutes.

- Similarly do not worry about TMS warnings and emails about cluster problems created during this upgrade.

On the Master Cisco VCS peer:

1. Check that the expected FindMe entries still exist on this master Cisco VCS (**Maintenance > Login accounts > User accounts**).
2. Check that other configuration (including Zone configuration, Transforms configuration and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.
3. Backup the master Cisco VCS (See “Appendix 1 – Backing up a Cisco VCS” for details).

Note: It is recommended that while Cisco VCS peers are running different versions of code, configuration changes to any Cisco VCS in the cluster are limited to the changes needed to complete the upgrade. Configuration changes will not be replicated across Cisco VCS peers that are not running the same version of software as the master Cisco VCS.

Upgrade non-master peers

Note: Do not worry about a “Cluster communication failure” alarm – this is expected.

For each non-master peer in the cluster:

1. Backup the Cisco VCS:
   a. If the VCS being backed up is version X6.1: log in as root on an SSH or other CLI interface. At the Cisco VCS command prompt, type:
      ```
      mkdir /tandberg/persistent/oti
      mkdir /tandberg/persistent/management
      ```
   b. Then perform backup as described in “Appendix 1 – Backing up a Cisco VCS”.

   Note: You should backup your system before upgrading. If at a later date you need to downgrade to an earlier version you will need to restore a backup made against that previous release.

2. Log in to the non-master peer as admin on an SSH or other CLI interface. Enable maintenance mode; from the Cisco VCS command line type:
   ```
   xconfiguration SystemUnit Maintenance Mode: On
   ```
3. Log in to the non-master peer as admin on the web interface.
4. Wait for all calls to clear and registrations to timeout on this non-master peer.
   If necessary, manually remove any calls on this peer that do not clear automatically (**Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
5. If necessary, manually remove any registrations from this peer that do not clear automatically (**Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).
   You can leave the registration for the conference factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own conference factory registration (if enabled).

On the non-master peer:

6. Upgrade and restart the Cisco VCS (**Maintenance > Upgrade**).
   If multiple peers need restarting, restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next.
   For any further details see the "Upgrading Software" section of the Cisco VCS Administrator Guide.

Note: The web browser interface may timeout during the restart process, after the progress bar has reached the end; this may happen if:

- Cisco VCS carries out a disk file system check – which it does approximately once every 30 restarts
- Provisioning is enabled, and database re-indexing is in progress

Upgrading the software on this non-master Cisco VCS peer is now complete.

Note:

- The upgrade process disables the Cisco VCS’s provisioning functionality — provisioning will be restored later when **Enable TMS Agent Data Replication** is enabled.

If Cisco TMS is used, on TMS, ensure that TMS has all the correct settings for this upgraded VCS by forcing a refresh of TMS:

1. Go to **Systems > Navigator** (and any required sub folders) and select the Master Cisco VCS.
2. Select the **Settings** tab.
3. Click **Force Refresh**.

If Cisco TMS is used and FindMe or Device Provisioning is required, enable replication on this upgraded non-master Cisco VCS peer.
On Cisco TMS:

4. Go to **Systems > Navigator** (and any required sub folders) then click on this non-master Cisco VCS.
5. Select the **TMS Agent** tab.
6. Select **Enable TMS Agent Data Replication**.
7. Ensure that **Authentication Scheme** is set to **Digest**.
8. Click **Save Settings**.

Note: This may take a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show the list of activities that are active, scheduled or in progress. Select the activity **Enable TMS Agent Data Replication for system(s) <name of system>**. This displays an activity log. Refresh this web page (button bottom left of this page) until the Activity Event completed successfully is reported.

- Do not worry about a message “Cluster replication error: cannot find master or this slave’s peer configuration file, manual synchronization of configuration is required” – this is expected while the cluster starts up. It should clear within 10 minutes.
- Similarly do not worry about TMS warnings and emails about cluster problems created during this upgrade.

On this non-master Cisco VCS peer:

1. Check the **Alarms** page (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.
2. Check that the expected FindMe entries exist on this Cisco VCS (**Maintenance > Login accounts > User accounts**).
3. Check that other configuration (including zone configuration, transforms configuration and other configuration for items from the System Configuration, VCS Configuration and Application menus) is as expected.
4. Repeat these steps for each non-master peer.

After all the cluster peers have been upgraded

After all cluster peers have been upgraded:

5. If TMS is used and FindMe or Device Provisioning is required, on Cisco TMS enable **TMS Agent Data Replication on all Cluster Peers**:
   a. Go to **Systems > Navigator** (and any required sub folders), then click on the Master Cisco VCS of the cluster.
   b. Select the **Clustering** tab.
   c. Select **Enable TMS Agent Data Replication on all Cluster Peers**.
   d. Click **Save Cluster Settings**.

Note: This may take a while to complete (approximately 5 minutes); select the **Activity Status** page (see link at the top of the screen) to show the list of activities that are active, scheduled or in progress. Select the activity **Enable TMS Agent Data Replication for system(s) <name of**

system>. This displays an activity log. Refresh this web page (button bottom left of this page) until the Activity Event completed successfully is reported.

After the upgrade

If Cisco TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each Cisco VCS peer:
   a. In the **TMS Agent Browser** panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the Cisco VCS peer.
   b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

Note: If authentication is intentionally enabled on the Cisco VCS, ignore the warning 'verify that authentication is disabled on the VCS'

- If all tests are successful (all green check marks), proceed with the instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Check cluster status

On each Cisco VCS (including the master):

1. Go to the **Clustering** page (**VCS Configuration > Clustering**).
   - Cluster database status should show **SUCCEEDED**.
   - VCS system configuration replication status should show **Last synchronization result SUCCEEDED**.
2. If replication with Cisco TMS is enabled:
   a. Select the link "**View TMS Agent replication status**".
   b. Check that the top line of the TMS Agent replication status report reports **Replication Enabled**.

Upgrading an X6.0, X6.1 or X7.0 cluster to an X7.0.n cluster is now complete.

Create a new cluster of VCS X7.0.n peers

Note: This procedure will require a period of downtime for the VCS service. Ensure that these instructions are followed in a scheduled maintenance window.

This section documents enabling clustering on a single Cisco VCS. This will be the Master peer of the cluster.

To complete the cluster by adding multiple Cisco VCSs, once this section is complete, follow the instructions in "Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)" to add the non-master peers to the cluster.

Do not use this section if the cluster already exists; instead, follow the instructions in "Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)".

Note: If Device Provisioning or FindMe is to be used with an X7.0.n VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

If Cisco TMS is to be used with this Cisco VCS cluster, ensure that it is running version 12.6 or later.

Prerequisites

- All Cisco VCSs to be included in the cluster must be running the same version of Cisco VCS software, and that version of software must be X7.0.n (n is the same value on all peers).
- If Device Provisioning and FindMe are configured, they must have already been proven to be operational on the master Cisco VCS after its upgrade to X7.0.n.
- If a firewall exists between cluster peers, it must be configured to permit the traffic documented in Appendix 3.

Set up the master peer of the cluster

This process sets up the first (Master) peer of this new cluster – additional peers are added afterwards using the "Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)" process.

Before proceeding, the Cisco VCS that will be the Master must be chosen.

Note:

- The Master Cisco VCS will be the source of the configuration information for all Cisco VCS peers in the cluster. Non-master Cisco VCS peers will have their configuration deleted and replaced by that from the Master.
- FindMe information can only be kept if the relevant Cisco VCS is already configured to operate with Cisco TMS and is configured with Enable TMS Agent Data Replication. (FindMe information for clusters is stored on Cisco TMS; it is deleted on VCS and overwritten by the information from Cisco TMS when **Enable TMS Agent Data Replication** is enabled.)

On neighbor Gatekeepers (GKs) and Border Controllers (BCs):

1. If the Master Cisco VCS has a traversal zone configured to connect with any GK or BC, upgrade these systems to N6.1 or Q6.1 or later code.

On other Cisco VCSs:

1. Check that no other Cisco VCS (anywhere) has this Cisco VCS's IP address in their Alternates or Clustering Peers list.

On this Master Cisco VCS:

1. Check that the Cisco VCS is running X7.0.n software.
2. Backup the Cisco VCS (See Appendix 1 for details).
3. On the web interface of this Master Cisco VCS, review the configuration to ensure that the Cisco VCS has:
   - A valid Ethernet speed (**System > Ethernet**).
   - Valid IP address and IP gateway (**System > IP**).
   - The same set of option keys installed as those that will be installed on all other peers of the cluster (**Maintenance > Option Keys**).

   Note: the number of call license keys may be different on different peers; all other license keys must be identical on each peer.

   - At least one valid DNS server configured, and that if unqualified DNS names are used elsewhere (e.g. for the NTP server), that the correct **Domain name** is also configured (**Domain name** is added as a suffix to an unqualified DNS name to make it into an FQDN) (**System > DNS**).

Note: <Local host name>.<DNS domain name> = FQDN of this Cisco VCS.

   - A valid and working NTP server configured (**System > Time**; in the Status section, the State should be "Synchronized").
   - No peers configured (**VCS configuration > Clustering** – all Peer x IP address fields on this page should be blank. If not, delete any entries and click **Save**).
4. Ensure that this Cisco VCS does not list any of the Cisco VCSs that are to be peers in this new cluster in any of its neighbor zones or traversal zones (**VCS configuration > Zones** then check each neighbor and traversal zone).
5. Set the H.323 **Time to live** to 60 (seconds) so that if a VCS becomes inaccessible to an endpoint, the endpoint will re-register quickly with another peer (**VCS configuration > Protocols > H.323**).
6. Go to **System > DNS** and ensure that the **Local host name** is the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System > System**, but excluding spaces, and unique for each Cisco VCS in the cluster); if not set it up appropriately and click **Save**.

Note: <Local host name>.<DNS domain name> = FQDN of this Cisco VCS.

7. Go to **VCS configuration > Calls** and set **Call routed mode** to *Optimal*.
8. Click **Save**.

Note: If Device Provisioning or FindMe is to be used with this X7.0.n VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

If Cisco TMS is to be used, on the Master Cisco VCS:

1. Ensure that the Cisco VCS can see Cisco TMS.
   To do this, select **System > External Manager** and in the Status section, ensure that the **State** is Active.
   (If not, follow the process on 'Appendix 2 – Adding a Cisco VCS to Cisco TMS').
2. Ensure that Cisco TMS can communicate with this Cisco VCS.
   To do this, on TMS select **Systems > Navigator** (and any required sub folders) then click on the name of the VCS and ensure that it says:
   "✓ System has no open or acknowledged tickets"
   (If not, follow the process on 'Appendix 2 – Adding a Cisco VCS to Cisco TMS').

On this Master Cisco VCS:

1. Check the **Alarms** page of the Cisco VCS to be added (**Status > Alarms**). If there is an alarm that the Cisco VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
   - Alarms about TMS Agent passwords being default will be cleared when TMS Replication is enabled.

If Cisco TMS is to be used:

1. Ensure that the Host Name of this Master Cisco VCS is set up in Cisco TMS:
   a. Select **Systems > Navigator** (and any required sub folders).
   b. Select this Cisco VCS.
   c. Select the **Connection** tab.
   d. Set **Host Name** to be the FQDN of this Cisco VCS, for example vcs3.uk.company.com.
   e. Click **Save/Try**.
   You can ignore any error messages like "`DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>`"
   f. Ensure that Cisco TMS updates its DNS.
      i. Select the **Settings** tab.
      ii. Click **Force Refresh**.
2. Ensure TMS Agent is enabled. Go to **Administrative Tools > Configuration > General Settings**, set **Enable Cisco TMS Agents** to **Yes**, and **Save Settings**.
   a. If this setting is changed, ensure it has completed by monitoring the status displayed on **Administrative Tools > Activity Status**, before moving on to the next steps.

For this Master Cisco VCS:

1. If Cisco TMS is configured to **Enable TMS Agent Data Replication** with this Cisco VCS, then any user accounts that existed on this Cisco VCS can be kept for use in the new cluster – if they are not wanted, they should be deleted.

   To check this status: on Cisco TMS go to **Systems > Navigator** (and any required sub folders) select this Cisco VCS and select the TMS Agent tab.

   If **Enable TMS Agent Data Replication** is not enabled, no FindMe data will be available for merging.

   If data is replicating with Cisco TMS:
   a. If the user accounts held on this Cisco VCS are not wanted, delete any that exist:
      i. Go to **Maintenance > Login accounts > User accounts**.
      ii. Select all of the accounts shown and click **Delete**.

2. Enable maintenance mode. Log in as admin on an SSH or other CLI interface. At the Cisco VCS command line type:
   ```
   xconfiguration SystemUnit Maintenance Mode: On
   ```
3. Wait for all calls to clear and registrations to timeout.
   If necessary, manually remove any calls that do not clear automatically (**Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
4. If necessary, manually remove any registrations that do not clear automatically (**Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).
   You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

5. Go to **VCS configuration > Clustering** and:
   a. Check that **Cluster name** is the routable Fully Qualified Domain Name used in SRV records that address this Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 9 – Cluster name and DNS SRV records).
   b. If it is not, the **Cluster name** needs changing; follow the procedure in “Appendix 8 – Changing the cluster name”.

Note: If the Cluster name is changed without following the procedure “Appendix 8 – Changing the cluster name” then any FindMe entries will be lost.

6. Click **Save**.
7. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

Configuration master	1
Cluster pre-shared key	Enter a password (any characters)
Peer 1 IP address	Set to the IP address of this (the master peer) Cisco VCS

Note: If the Cisco VCS has dual network interfaces, the Peer IP address MUST specify the LAN 1 interface address.

8. Click **Save**.
   To the right of the **Peer 1 IP address** field the words “*This VCS*” should appear (though this may require the page to be refreshed before they appear).
9. Restart the Cisco VCS (select **Maintenance > Restart**, then select **Restart system** and confirm **OK**.).

After the restart, on the Master Cisco VCS web interface:

1. Check that the configuration (including Zone configuration, Transforms configuration, CPL and other configuration for items from the System Configuration, VCS configuration and Application menus) is as expected.
2. Backup the Cisco VCS (See Appendix 1 for details).

On other devices:

- If you have any other Cisco VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this Master Cisco VCS peer, ensure that their zone configuration for this cluster is updated to only include the address of this Master Cisco VCS.

If Cisco TMS is used, on Cisco TMS:

1. Go to **Systems > Navigator** (and any required sub folders) and select this Master Cisco VCS
2. Select the **TMS Agent** tab:
   a. Ensure that **Enable TMS Agent Data Replication** is selected.
   b. Ensure that **Authentication Scheme** is set to **Digest**.
3. If any changes need to be made, click **Save Settings**.
4. Select **Activity Status** in the banner message to ensure the status reports success.

Note: If TMS Agent Data Replication reports Disabled then there is a problem. On Cisco TMS select **Administrative Tools > Activity Status** and look for the Description ‘Enable TMS Agent Data Replication for system(s): <VCS name(s)>’. Click on the description for a full listing of the Activity log associated with this action. Identify and fix any reported problems.

Note: Please refer to the Cisco TMS Provisioning Deployment Guide for more details on how to enable provisioning in TMS.

On this Master Cisco VCS peer:

1. Log in to the web browser of this Cisco VCS.
2. Check the Alarms page (**Status > Alarms**):
   a. If required, restart the Cisco VCS.
   b. If "Security Alert: the TMS agent database has the default LDAP password set" or "Security Alert: the TMS agent database has the default replication password set" appear, see the relevant section in 'Appendix 6 – Troubleshooting'.
3. If the Cisco VCS did not need to be restarted, ensure that maintenance mode is disabled. Log in as admin on an SSH or other CLI interface. At the Cisco VCS command line type:

```
xconfiguration SystemUnit Maintenance Mode: Off
```

After the master peer configuration

If Cisco TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For this master Cisco VCS peer:
   a. In the **TMS Agent Browser** panel on the left side of the page, expand the Un-clustered VCSs folder and the relevant sub folder and select the Cisco VCS peer.
   b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

Note: If authentication is intentionally enabled on the Cisco VCS, ignore the warning 'verify that authentication is disabled on the VCS'

- If all tests are successful (all green check marks), proceed with the "Additional cluster configuration" instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

No Cisco TMS

If Cisco TMS is not used to monitor / manage Cisco VCS then check the Alarms page on the Cisco VCS (**Status > Alarms**) and ensure that all Alarms are acted upon and cleared.

Note: Use of Cisco TMS is required if Device Provisioning or FindMe is to be used with this cluster.

Additional cluster configuration

- If Microsoft Office Communications Server 2007 (OCS) or Lync 2010 is to be connected to this cluster, see the "Cisco VCS deployment guide – Microsoft OCS 2007 (R2) and Lync 2010 and Cisco VCS Control (X7)".

Creation of the new cluster (of one Cisco VCS) is complete.

Adding another cluster peer

Add other Cisco VCSs to the cluster following the instructions in the next section: "Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)".

Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)

Follow this process if you have an existing X7.0.n cluster (of one or more peers) to which you want to add another Cisco VCS peer. If you do not have an existing cluster, following the instructions in the section “Create a new cluster of VCS X7.0.n peers”.

Note: You can have up to 6 Cisco VCSs, including the master Cisco VCS, in a cluster.

This process will add an X7.0.n VCS to the cluster and replicate the cluster Master’s configuration onto the Cisco VCS.

Note:

- Cisco VCS clusters peers must all run the same version of code as the master, for example all X7.0.n (x is the same value on all peers).
- Only one Cisco VCS must be added to the cluster at a time.

On the Master Cisco VCS:

1. Ensure that the Master Cisco VCS does not list this new Cisco VCS peer in any of its neighbor zones or traversal zones (**VCS configuration > Zones** then check each neighbor and traversal zone).

Note: The Master VCS will be the source of the configuration for this new VCS peer and all other VCS peers in the cluster. When a VCS is added to the cluster, its configuration will be deleted and replaced by that from the Master.

On the Cisco VCS to be added to the cluster:

1. Check that no other VCS (anywhere) has this VCS’s IP address in their Alternates or Clustering Peers list.
2. Check that the VCS software version is identical to the version running on the Master and any other cluster peers of the existing cluster (X7.0.n - x is the same value on all peers).
3. Backup the VCS (See Appendix 1 for details).

On the web interface of the Cisco VCS being added:

4. Review the configuration to ensure that the Cisco VCS has:
   - A valid Ethernet speed (**System > Ethernet**).
   - Valid IP address and IP gateway (**System > IP**).
   - The same set of Option keys as those installed on Master peer (**Maintenance > Option Keys**).

     Note: The number of traversal and non-traversal call license keys may be different on different peers; all other license keys must be identical on each peer.

   - At least one valid DNS server configured, and that if unqualified DNS names are used elsewhere (e.g. for the NTP server), that the correct **Domain name** is also configured (**Domain name** is added as a suffix to an unqualified DNS name to make it into an FQDN) (**System > DNS**).

Note: <Local host name>.<DNS domain name> = FQDN of this Cisco VCS.

- A valid and working NTP server configured (**System > Time**; in the Status section, the State should be 'Synchronized').
- No peers configured (**VCS configuration > Clustering** – all Peer x IP address fields on this page should be blank. If not, delete any entries and click **Save**).

If the cluster is managed by TMS, this VCS being added to the cluster must also be managed by TMS.

Note: If Device Provisioning or FindMe is to be used with an X7.0.n VCS cluster, then use of Cisco TMS is essential. If neither Device Provisioning nor FindMe is to be used, then use of Cisco TMS is optional but recommended.

If Cisco TMS is to be used, on the Cisco VCS to be added to the cluster:

1. Ensure that the Cisco VCS can see Cisco TMS.
   To do this, select **System > External Manager** and in the Status section, ensure that the State is Active.
   (If not, follow the process on 'Appendix 2 – Adding a Cisco VCS to Cisco TMS').
2. Ensure that Cisco TMS can communicate with this Cisco VCS. To do this, on TMS select **Systems > Navigator** (and any required sub folders) then click on the name of the VCS and ensure that it says:
   "✓ System has no open or acknowledged tickets"
   (If not, follow the process on 'Appendix 2 – Adding a Cisco VCS to Cisco TMS').

On the Cisco VCS being added to the cluster:

1. Check the **Alarms** page of the Cisco VCS to be added (**Status > Alarms**). If there is an alarm that the Cisco VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
   - Alarms about TMS Agent passwords being default can be ignored as they will be cleared when TMS Replication is enabled.
   - If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.

If Cisco TMS is to be used:

1. For the VCS to be added to the cluster, ensure that the Host Name of the VCS is set up in TMS:
   a. Select **Systems > Navigator** (and any required sub folders).
   b. Select this Cisco VCS
   c. Select the **Connection** tab.
   d. Set **Host Name** to be the FQDN of this non-master peer, for example vcs3.uk.company.com.
   e. Click **Save/Try**.
      You can ignore any error messages like "`DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>`"
   f. Ensure that Cisco TMS updates its DNS.
      i. Select the **Settings** tab.
      ii. Click **Force Refresh**.

For existing installations, if Cisco TMS is configured to **Enable TMS Agent Data Replication** with this Cisco VCS being added to the cluster, then any user accounts that existed on the Cisco VCS should be deleted.

To check this: on Cisco TMS go to **Systems > Navigator** - and any required sub folders - select this Cisco VCS and select the TMS Agent tab.

If **Enable TMS Agent Data Replication** is not enabled, no FindMe data will be stored on TMS.

If TMS Agent data is replicating with Cisco TMS:

a. Delete any user accounts that exist. On the Cisco VCS being added to the cluster:
   i. Go to **Maintenance > Login accounts > User accounts**.
   ii. Select all of the accounts shown and click **Delete**.

If Cisco TMS is used, for the master Cisco VCS in the cluster:

1. Select **Systems > Navigator** (and any required sub folders), then click on the Master Cisco VCS of the cluster.
2. Select the **Clustering** tab.
3. Clear the **Enable TMS Agent Data Replication on all Cluster Peers** check box (if it was set).
4. Click **Save Cluster Settings**.

Note: This disables database replication from Cisco TMS to each cluster peer.

- Provisioning data will no longer be updated from Cisco TMS to the Cisco VCSs, however provisioning of endpoints from data cached on Cisco VCSs will continue.
- VCS cluster configuration replication will continue.
- VCS FindMe replication among Cisco VCS peers will STOP.

If Cisco TMS is used, for each Cisco VCS in the cluster (including the Master and the Cisco VCS being added to the cluster), in Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders).
2. Select the Cisco VCS.
3. Select the **TMS Agent** tab.
4. Clear the **Enable TMS Agent Data Replication** check box (if it was set).
5. Click **Save Settings**.

On the Cisco VCS being added to the cluster:

1. Enable maintenance mode.
   From the Cisco VCS command line type:
   ```
   xconfiguration SystemUnit Maintenance Mode: On
   ```
2. Wait for all calls to clear and registrations to timeout.
   If necessary, manually remove any calls that do not clear automatically (**Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
3. If necessary, manually remove any registrations that do not clear automatically (**Status > Registrations > By device**, then select the check box next to the devices you want to remove and click **Unregister**).
   You can leave the registration for the Conference Factory – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

On the Master Cisco VCS:

1. On the Clustering page (**VCS configuration > Clustering**), one or more of the **Peer x IP address** fields should be empty.
   In the first empty field, enter the IP address of the new Cisco VCS peer.

Note:

- Only one Cisco VCS must be added to the cluster at a time (repeat the whole process if multiple Cisco VCS peers are being added).
- If the new Cisco VCS peer has dual network interfaces, the peer IP address MUST specify the LAN 1 interface address.

2. Click **Save**.

   Peer 1 should indicate 'This VCS'. The new peer may indicate 'Unknown' and then with a refresh should indicate 'Failed' as the Cisco VCS is not completely added to the cluster.

Note:

- A cluster communication failure alarm will be raised on the master and on other non-master peers already in the cluster advising that this new Cisco VCS peer is not communicating – this will clear later.
- Cluster configuration replication is suspended at this point until the new Cisco VCS has been completely added. Any changes made to the configuration of the cluster will not be replicated until this Cisco VCS has been completely added

On every other non-master Cisco VCS already in the cluster (not the Cisco VCS being added):

1. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows. This will typically involve adding the IP address of the additional peer.

   This list must be identical on every cluster peer, and is entered per-peer. It specifies which of the Peer IP addresses (1-6) is the configuration master (this configuration is replicated to all peers), and provides the encryption key with which the data is secured when shared across the network.

Cluster name	Identical to the **Cluster name** configured on the Master Cisco VCS
Cluster pre-shared key	Identical to that configured on the Master Cisco VCS
Configuration master	Identical to that configured on the Master Cisco VCS
Peer 1 IP address … Peer 6 IP address	Identical to those configured on the Master Cisco VCS (these must be in the same order)

2. Click **Save**.

On the additional non-master Cisco VCS being added to the cluster:

1. Log in as admin on an SSH or other CLI interface. At the Cisco VCS command prompt, type:

```
xcommand DefaultValuesSet Level: 2
xcommand DefaultLinksAdd
```

Note: This command will wipe any LDAP Authentication configuration – ensure that you have the web admin password before executing this command.

2. Go to the **Administrator accounts** page (**Maintenance > Login accounts > Administrator accounts**).
3. Delete all entries except the default admin account.
4. Go to **System > DNS** and ensure that **Local host name** is the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System > System**, but excluding spaces, and unique for each Cisco VCS in the cluster); if not set it up appropriately and click **Save**.

Note: <Local host name>.<DNS domain name> = FQDN of this Cisco VCS.

5. On the Clustering page (**VCS configuration > Clustering**) configure the fields as follows:

Cluster name	Identical to the **Cluster name** configured on the master Cisco VCS
Cluster pre-shared key	Identical to that configured on the Master Cisco VCS
Configuration master	Identical to that configured on the Master Cisco VCS
Peer 1 IP address … Peer 6 IP address	Identical to those configured on the Master Cisco VCS

6. Click **Save**.

Note: A cluster communication failure alarm will be raised on this Cisco VCS peer advising that this new Cisco VCS is not communicating – this will clear after the restart.

7. Restart the Cisco VCS:
   a. On the **Maintenance > Restart** page, click **Restart system**.
   b. Confirm the restart by clicking **OK**.

      If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.

8. After the restart, wait approximately 2 minutes – this is the frequency with which configuration is copied from the Master.
9. Check the **Alarms** page of the newly added Cisco VCS (**Status > Alarms**). If there is an alarm that the Cisco VCS must be restarted, select **Maintenance > Restart** and then click **Restart System**.
   - Alarms about TMS Agent passwords being default can be ignored; they will be cleared when TMS Replication is enabled.
   - If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
10. Check that the configuration (including zone configuration, transforms configuration, CPL and other configuration for items from the System Configuration, VCS configuration and Application menus) is as expected (not FindMe — this will be replicated later) as per the Master Cisco VCS.

On other devices:

- If you have any other Cisco VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of Cisco VCS peers, ensure that their zone configuration for this cluster is updated to include the address of this new peer.

If Cisco TMS is used, and if Device Provisioning or FindMe are to be used in this cluster, on TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.
2. Select the **Clustering** tab

   a. Ensure that **Enable TMS Agent Data Replication on all Cluster Peers** is selected.
      - If it is not selected, select it and click **Save Cluster Settings** or **Create Cluster** as appropriate.
3. Go to **Systems > Navigator** (and any required sub folders) then select the new Cisco VCS to be added to this cluster.
4. Select the **TMS Agent** tab
   a. Ensure that **Enable TMS Agent Data Replication** is selected.
   b. Ensure that **Authentication Scheme** is set to **Digest**.
5. If any changes need to be made, click **Save Settings**.

Note: If TMS Agent Data Replication reports Disabled then there is a problem. On Cisco TMS select **Administrative Tools > Activity Status** and look for the Description 'Enable TMS Agent Data Replication for system(s): <VCS name(s)>'. Click on the description for a full listing of the Activity log associated with this action. Identify and fix any reported problems.

On each Cisco VCS peer (including the master and this new VCS peer):

1. Log in to the web browser of the new Cisco VCS peer.
2. Check the **Alarms** page (**Status > Alarms**):
   a. If required, restart the Cisco VCS.
   b. If "Security Alert: the TMS agent database has the default LDAP password set" or "Security Alert: the TMS agent database has the default replication password set" appear, see the relevant section in 'Appendix 6 – Troubleshooting'.

      If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
3. Check that the expected FindMe entries (from the Master Cisco VCS) exist on this Cisco VCS **(Maintenance > Login accounts > User accounts**).

Check replication status:

Note: It can take 5 or so minutes before Cisco VCS reports the successful status. If problems are seen, refresh the screen after waiting 5 minutes.

On Cisco VCS:

1. Go to the **Clustering** page (**VCS configuration > Clustering**):
   - Clustering status should show Status Enabled.
   - VCS system configuration replication status should show Last synchronization result SUCCEEDED.
2. If replication with Cisco TMS is enabled:
   a. Select the link "View TMS Agent replication status".
   b. Check that the top line of the TMS Agent replication status report reports Replication Enabled.

If TMS is being used, ensure that it has all the correct settings for this upgraded VCS by forcing a refresh of TMS.

1. For every Cisco VCS in the cluster (including the Master Cisco VCS):
   a. Select **Systems > Navigator** (and any required sub folders) and click on the name of the Cisco VCS.
   b. Select the **Settings** tab.
   c. Click **Force Refresh**.

2. Repeat for all Cisco VCS peers in the cluster.

After adding the Cisco VCS peer to the cluster

If Cisco TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each Cisco VCS peer:
   a. In the **TMS Agent Browser** panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the Cisco VCS peer.
   b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

Note: If authentication is intentionally enabled on the Cisco VCS, ignore the warning 'verify that authentication is disabled on the VCS'.

- If all tests are successful (all green check marks), proceed with the "Additional cluster configuration" instructions below.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Additional cluster configuration

- If Conference Factory (Multiway™) is to be used, see the section "Conference Factory (Multiway™)" in "Appendix 4 – Impact of clustering on other Cisco VCS applications".
- If the cluster has non-default Trusted CA certificate and / or non default Server certificate ensure that the added peer is configured with the required Trusted CA certificate and an appropriate Server certificate.

Add an X7.0.n VCS to a VCS X7.0.n cluster is now complete.

Remove a live Cisco VCS from a VCS X7.0.n cluster (permanently)

This process will remove one Cisco VCS peer from an existing cluster. FindMe and configuration replication to this Cisco VCS will be stopped and the Cisco VCS will no longer be included in the list of peers in the cluster. Provisioning will also be disabled on the removed Cisco VCS.

- If the whole cluster is to be disbanded then use the procedure defined in “Disband a VCS X7.0.n cluster”.
- If the cluster peer to be removed is not accessible, use the procedure defined in “Remove an out-of-service Cisco VCS from a VCS X7.0.n cluster (permanently)”.

Before starting:

1. Ensure that the Cisco VCS to be removed from the cluster is not indicated as the Master peer. If it is the Master, see the section “Change the master peer of a VCS X7.0.n cluster” for instructions on how to make a different peer the master.

If Cisco TMS is used, on Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Cisco VCS to be removed.
2. Select the **TMS Agent** tab.
3. Clear the **Enable TMS Agent Data Replication** check box.
4. Click **Save Settings**.

On the Cisco VCS that is being removed:

1. Log into the web interface.
2. Go to the **Clustering** page (**VCS configuration > Clustering**):
   a. Change the **Cluster name** to a unique ID for this Cisco VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual Cisco VCS, for example "vcs1.example.com". (See Appendix 9 – Cluster name and DNS SRV records.)) Note: Do NOT use the process “Appendix 8 – Changing the cluster name (and keeping FindMe accounts)” because FindMe accounts are to be left with the cluster that this Cisco VCS is being removed from.
   b. Delete the **Cluster pre-shared key**.
   c. Delete all entries in the **Peer x IP address** fields.
3. Click **Save**.

Note:

- FindMe users will not be available on this removed Cisco VCS (they will be left available on the cluster).
- An alarm similar to that shown below may appear on the web interface and CLI of the Cisco VCS being removed. This is not a problem, the alarm will be cleared when the Cisco VCS is restarted:

4. Go to the OCS Relay page (**Applications > OCS Relay**).
   - If Mode = *On* change it to Mode = *Off* and click **Save**.
5. Restart the Cisco VCS (**Maintenance > Restart** and then click **Restart System**).

On the Master Cisco VCS:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) delete the IP address of the Cisco VCS that has been removed.
3. If the Cisco VCS being removed is not the last field in the list, move any other IP addresses up the list so that there are no empty fields between entries.
4. If the master Cisco VCS peer's IP address has been moved up the list in the previous step, alter the **Configuration master** value to match its new location.
5. Click **Save**.

On all the remaining non-master Cisco VCS peers:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) edit the **Peer x IP address** and **Configuration master** fields so that they are identical to those configured on the Master Cisco VCS.
3. Click **Save**.
4. Repeat for all remaining non-master Cisco VCS peers until they all have identical clustering configuration.

On other devices:

1. If you have any other Cisco VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of Cisco VCS peers, ensure their zone configuration for this cluster is updated to exclude the address of the removed peer.
2. If you have any endpoints registering to the Cisco VCS that has now been removed, change the configuration of the endpoint (or the configuration of the DNS server entry that points to the cluster peers) so that they register to one of the remaining clustered Cisco VCS peers instead.

Caution: The removed Cisco VCS will retain its configuration at the time it is removed from the cluster, and will continue to function as a non-clustered Cisco VCS. It is recommended that after it has been removed from the cluster it is taken out of service (e.g. perform `xcommand DefaultValuesSet Level: 2` and `xcommand DefaultLinksAdd`) or the Cisco VCS is reconfigured with an alternative configuration, so that other devices no longer try to use it as a cluster peer.

Reconfigure Cisco TMS

If Cisco TMS is used, on Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.
2. Select the **Clustering** tab.
3. Click **Update Cluster in TMS**.

After the removal

If Cisco TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.

4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each Cisco VCS peer:
   a. In the TMS Agent Browser panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the Cisco VCS peer.
   b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

Note: If authentication is intentionally enabled on the Cisco VCS, ignore the warning 'verify that authentication is disabled on the VCS'

- If all tests are successful (all green check marks), Removing a live Cisco VCS from a cluster is now complete.
- If any errors are found (a red 'X' will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Removing a live Cisco VCS from a cluster is now complete.

Remove an out-of-service Cisco VCS from a VCS X7.0.n cluster (permanently)

Use the following procedure if:

- the Cisco VCS is dead and needs to be RMAd, or
- the Cisco VCS cannot be accessed for some other reason

If the whole cluster is to be disbanded then use the procedure defined in “Disband a VCS X7.0.n cluster”.

If the cluster peer to be removed is accessible, use the procedure defined in “Remove a live Cisco VCS from a VCS X7.0.n cluster (permanently)” which clears up the removed Cisco VCS as well as its previous peers.

Note: This procedure does not delete clustering configuration from the removed Cisco VCS. Once removed, you must not reconnect the out-of-service Cisco VCS without first deleting all of its peers and stopping FindMe and configuration replication (see the section below ”Before you reconnect the out-of-service Cisco VCS back to the network”).

Before starting:

1. Ensure that the Cisco VCS to be removed from the cluster is not indicated as the Master Cisco VCS on Cisco TMS.
   If it is the Master Cisco VCS, see the section “Change the master peer of a VCS X7.0.n cluster” for instructions on how to make a different peer the master.

If Cisco TMS is used, on Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Cisco VCS to be removed.
2. Select the **TMS Agent** tab.
3. Clear the **Enable TMS Agent Data Replication** check box.
4. Click **Save Settings**.

On the Master Cisco VCS:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) delete the IP address of the Cisco VCS that has been removed.
3. If the Cisco VCS being removed was not the last in the list, move any other IP addresses up the list so that there are no empty fields between entries
   - If this results in the master Cisco VCS peer’s IP address moving up the list, alter the **Configuration master** value to match its new location.
4. Click **Save**.

On all the remaining non-master Cisco VCS peers:

1. Log into the web interface.
2. On the Clustering page (**VCS configuration > Clustering**) edit the **Peer x IP address** and **Configuration master** fields so that they are identical to that set on the Master Cisco VCS.
3. Click **Save**.
4. Repeat for all remaining non-master Cisco VCS peers.

On other devices:

1. If you have any other Cisco VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of Cisco VCS peers, ensure their zone configuration for this cluster is updated to exclude the address of the removed peer.

2. If you have any endpoints registering to the Cisco VCS that has now been removed, change the configuration of the endpoint (or the configuration of the DNS server entry that points to the cluster peers) so that they register to one of the remaining clustered Cisco VCS peers instead.

Reconfigure Cisco TMS

If Cisco TMS is used, on Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.
2. Select the **Clustering** tab.
3. Click **Update Cluster in TMS**.

After the removal

If Cisco TMS is being used, verify the correct operation of TMS Agent by running TMS agent diagnostics:

1. Log into Cisco TMS.
2. Go to **Administrative Tools > TMS Agent Diagnostics**.
3. In the **TMS Agent Browser** panel on the left side of the page, select **Local TMS Agent**.
4. Click **Run All Diagnoses** to run the diagnostic tests on the Local TMS Agent.
5. For each Cisco VCS peer:
   a. In the TMS Agent Browser panel on the left side of the page, expand the Clustered VCSs folder and cluster folder and select the Cisco VCS peer.
   b. Click **Run All Diagnoses** to run the diagnostic tests on the VCS peer.

Note: If authentication is intentionally enabled on the Cisco VCS, ignore the warning ‘verify that authentication is disabled on the VCS’.

- If all tests are successful (all green check marks), removing an out-of-service Cisco VCS from a cluster is now complete.
- If any errors are found (a red ‘X’ will appear against failing tests), do not proceed further with this upgrade, but contact your Cisco Authorized Service Provider for further assistance to resolve the issues identified.

Removing an out-of-service Cisco VCS from a cluster is now complete.

Before you reconnect the out-of-service Cisco VCS back to the network

If the removed Cisco VCS is ever recovered, before you reconnect it you must clear out its configuration. This is most easily implemented as follows:

1. Log into the VCS as root (over serial or SSH – serial connection will show more details as the factory reset progresses).
2. Type:
   `factory-reset`

   then press **enter**
   a. Keep option Keys = YES
   b. Keep IP configuration = YES or NO … depends on whether the VCS has been replaced with another at the same IP address
   c. Keep SSH keys = NO
   d. Keep root and admin passwords = YES or NO … as desired

   e. Save log files = NO … unless specifically requested for analysis purposes
   f. Replace hard disk = NO
   g. Are you sure you want to continue = YES

   Some messages will be displayed, then connection over serial / SSH will be lost.
   It may take some 20 or more minutes before VCS is available to access again.

3. Log into the VCS as Admin
4. Type:
   `xcommand DefaultLinksAdd`

This ensures that the configuration of the recovered Cisco VCS is returned to default and it will not interact with its ex-peers.

Disband a VCS X7.0.n cluster

This process will remove all Cisco VCS peers from an existing cluster. FindMe and configuration replication will be stopped, as will provisioning, and the cluster will be deleted from Cisco TMS.

Each Cisco VCS will retain its configuration at the time the cluster was disbanded, and will function as a stand-alone Cisco VCS.

Caution: If any of the Cisco VCSs are left in operation after being removed from the cluster, calls between endpoints registered to different Cisco VCSs that were once part of the same cluster will not succeed. This is because after the cluster has been disbanded, the Cluster Subzone will no longer exist and there will not be any link between the two Cisco VCSs over which calls can be routed. To overcome this, you must create neighbor relationships between the Cisco VCSs so that there are links between them.

- If any Cisco VCS is not accessible, firstly remove it using the procedure “Remove an out-of-service Cisco VCS from a VCS X7.0.n cluster (permanently)”.

If Cisco TMS is used, on Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.
2. Select the **Clustering** tab.
3. Clear the **Enable TMS Agent Data Replication on all Cluster Peers**.
4. Click **Save Cluster Settings**.
5. Select the **TMS Agent** tab.
6. Ensure that **Enable TMS Agent Data Replication** is not selected; if this needs changing, change it and click **Save Settings**.

If Cisco TMS is used, on Cisco TMS, for every non-master Cisco VCS peer:

1. Select **Systems > Navigator** (and any required sub folders) then click on the non-master Cisco VCS.
2. Select the **TMS Agent** tab.
3. Ensure that **Enable TMS Agent Data Replication** is not selected; if this needs changing, change it and click **Save Settings**.
4. Repeat for all non-master Cisco VCS peers – Cisco TMS may require you to pause between disabling each peer.

On each non-master Cisco VCS peer:

1. Log into the web interface.
2. From the Clustering page (**VCS configuration > Clustering**):
   a. Change the **Cluster name** to a unique ID for this Cisco VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual Cisco VCS, for example "vcs1.example.com", "vcs2.example.com". etc. (See Appendix 9 – Cluster name and DNS SRV records.))
   Note: Do NOT use the process “Appendix 8 – Changing the cluster name (and keeping FindMe accounts)” because FindMe accounts are to be left with the master peer of the cluster that this Cisco VCS is being removed from.
   b. Delete the **Cluster pre-shared key**.
   c. Delete all entries in the **Peer x IP address** fields.
3. Click **Save**.

Note:

- FindMe users will not be available on non-master Cisco VCSs (they will only be left available on the master).
- An alarm similar to that shown below may appear on the web interface and CLI of the Cisco VCS being removed. This is not a problem, the alarm will be cleared when the Cisco VCS is restarted:

4. Go to the OCS Relay page (**Applications > OCS Relay**).
   - If Mode = *On* change it to Mode = *Off* and click **Save.**
5. Restart the Cisco VCS (**Maintenance > Restart** and then click **Restart System**).
   If multiple peers need restarting, restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next.
6. Repeat for each non-master Cisco VCS.

On the Master Cisco VCS:

1. Log into the web interface.
2. If the **Cluster name** is to be changed on this Master Cisco VCS, FindMe information should be deleted, so that the database is not left with unused user accounts.
   a. Delete all FindMe entries:
      i. Go to **Maintenance > Login accounts > User accounts**.
      ii. Select each account and click **Delete**.
3. Go to the Clustering page (**VCS configuration > Clustering**).
   a. Optionally change the **Cluster name** to a unique ID for this Cisco VCS (ideally to the routable Fully Qualified Domain Name used in SRV records that address this individual Cisco VCS, for example "vcs1.example.com". (See Appendix 9 – Cluster name and DNS SRV records.))
      Use the process “Appendix 8 – Changing the cluster name (and keeping FindMe accounts)” if FindMe accounts are to be kept with this Cisco VCS.
   b. Delete the **Cluster pre-shared key**.
   c. Delete all entries in the **Peer x IP address** fields.
4. Click **Save**.

Note: An alarm similar to that shown below may appear on the web interface and CLI of the Cisco VCS being removed. This is not a problem; the alarm will be cleared when the Cisco VCS is restarted:

5. Restart the Cisco VCS (**Maintenance > Restart** and then click **Restart System**).

On other devices:

1. If you have any other Cisco VCSs, Gatekeepers or Border Controllers neighbored (or connected via a traversal zone) to this cluster of Cisco VCS peers, ensure that they have those zones removed, or modified appropriately.
2. If you have any endpoints registering to this Cisco VCS cluster, change the configuration of the endpoints (or the configuration of the DNS server entry that points to the cluster peers) so that they now register with an appropriate Cisco VCS.

Reconfigure Cisco TMS

If Cisco TMS is used, on Cisco TMS:

1. Select **Systems > Navigator** (and any required sub folders) then select the Master Cisco VCS.
2. Select the **Clustering** tab.
3. In the Cluster Settings section click **Delete Cluster**.
4. Confirm that you really want to delete the cluster by clicking **Delete**.
   Cisco TMS will report “Cluster successfully deleted”.

Disband a cluster of Cisco VCSs is now complete.

Change the master peer of a VCS X7.0.n cluster

Changing the master peer where the old master is or is not accessible

Note: The operations in this process should be performed in one go so that the cluster is not left in a state where there are multiple Cisco VCSs which think they are cluster Master.

On the "new" Master Cisco VCS:

1. Go to the **Clustering** page (**VCS configuration > Clustering**) and from the **Configuration master** drop-down menu select the ID number of the Peer entry that says 'This VCS'.
2. Click **Save**.

   While performing this change of master peer, ignore any alarms on VCS that report 'Cluster master mismatch' or 'Cluster replication error' – they will be rectified as part of this procedure.

If the "old" Master Cisco VCS is accessible, on the "old" Master Cisco VCS:

1. On the **Clustering** page (**VCS configuration > Clustering**) from the **Configuration master** drop-down menu select the ID number of the "new" Master Cisco VCS.
2. Click **Save**.

For all other non-master Cisco VCS peers, on that Cisco VCS:

1. Go to the **Clustering** page (**VCS configuration > Clustering**) and from the **Configuration master** drop-down menu select the ID number of the "new" Master Cisco VCS.
2. Click **Save**.

On each Cisco VCS in the cluster (including the master):

1. Confirm that the change to the **Configuration master** has been accepted by going to **VCS configuration > Clustering** and refreshing the page.
2. If any Cisco VCSs have not accepted the change, repeat the steps above.
3. Check the Status section:
   - Clustering status should show Status Enabled
   - VCS system configuration replication status should show Last synchronization result SUCCEEDED

Note: After approximately 2 minutes any alarms raised on the Cisco VCS peers that relate to 'Cluster master mismatch' and 'Cluster replication error' should automatically clear.

Reconfigure Cisco TMS

No changes are required; TMS will see the master change on the VCS cluster and report this appropriately.

If the old master is not available

If you are changing the Master because the "old" Master is not accessible, remove the "old" Master using the "Remove an out-of-service Cisco VCS from a VCS X7.0.n cluster (permanently)" procedure.

If the "old" Master was not accessible when changing the master peer of the Cisco VCS cluster, but later becomes available, you must bring it back into the cluster using the "Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)" procedure.

Changing the master peer of a Cisco VCS cluster is now complete.

Change the IP address of a VCS X7.0.n peer

To change the IP address of a Cisco VCS peer you must remove the Cisco VCS from the cluster, change its IP address, and then add the Cisco VCS back into the cluster.

The process is as follows:

1. Ensure that the Cisco VCS whose IP address is to be changed is not the Master Cisco VCS. If it is the Master Cisco VCS, follow the steps in the section “Change the master peer of a VCS X7.0.n cluster” to make a different peer the Master.
2. Carry out the process documented in “Remove a live Cisco VCS from a VCS X7.0.n cluster (permanently)”.
3. Change the IP address of the Cisco VCS.
4. Carry out the process documented in “Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)”.

Changing the IP address of a Cisco VCS peer is now complete.

Appendix 1 – Backing up a Cisco VCS

Backing up an X5.0 or later Cisco VCS

To backup the data:

1. On the Cisco VCS web interface go to **Maintenance > Backup and restore**.
2. Click **Create System Backup File** and save the file.
3. If Cisco TMS is used and the Cisco VCS is X5 or later:
   a. Click **Create TMS Agent backup file** and save the file (this backs up FindMe entries that are in X5 FindMe database format).

Note:

- If the TMS Agent backup is restored (uploaded) to Cisco VCS then:
  from a root login run “tmsagent_reindex_database” to ensure the uploaded data is linked into the database correctly.
- A TMS Agent backup contains the whole of the Cisco TMS’s provisioning and FindMe database (for all clusters and non-clustered Cisco VCSs with which Cisco TMS is replicating). It is saved for emergency use only – if restored to a cluster it will only get overwritten by the Cisco TMS data. It can be restored to a non-clustered Cisco VCS that is not replicating with Cisco TMS.

For Cisco VCS prior to X6.1, to save the VCS certificates:

4. Use SCP (log in as root) to copy the following files from the VCS:
   a. persistent/policy/policy.xml
   b. persistent/certs/*.*

Appendix 2 – Adding a Cisco VCS to Cisco TMS

On the Cisco VCS:

1. Go to the SNMP page (**System > SNMP**) and ensure that:
   a. **SNMP mode** is set to *v3 plus TMS support* or *v2c*.
   b. **Community name** is set to *public*.

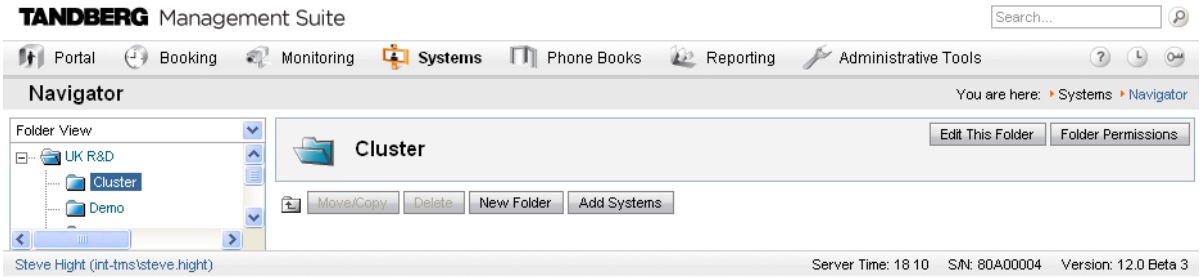
   (If SNMP was previously disabled, an alarm may appear indicating the need for a restart. If a restart is required, go to **Maintenance > Restart** and click **Restart System**.)

   If multiple peers need restarting: restart each peer in turn, waiting for the peer to be accessible through the web interface before restarting the next peer.
2. Go to the External Manager page (**System > External Manager**) and ensure that:
   a. **Address** is set to the IP Address or FQDN of Cisco TMS.
   b. **Path** is set to *tms/public/external/management/SystemManagementService.asmx*.
   c. If the **Protocol** is *HTTPS* and **Certificate verification mode** is *On* then you must load the relevant certificates before the connection can become 'Active'. See document "D50520 Implementing Secure Management" for details.
   d. If the **Protocol** is *HTTP* or **Certificate verification mode** is *Off*, no certificates need to be loaded.
3. Click **Save**.

The **Status** section of the **External Manager** page should show a **State** 'Active' or 'Initializing'.[1]

On Cisco TMS:

1. Select **Systems > Navigator**.
2. Select (or create) an appropriate folder in which to put the Cisco VCS (in the example below the folder has been called "Cluster"):



3. Click **Add Systems**.
4. In section "1. Specify Systems by IP addresses or DNS names", enter the IP address or DNS name of the Cisco VCS.
5. Click **Next**.

[1] TMS may force protocol to be HTTPS. The configuration for this is found in TMS **Administrative Tools > Configuration > Network settings.** The protocol will be forced to HTTPS if, in the **TMS Services** section **Enforce Management Settings on Systems** is set to **On** and in the **Secure-Only Device Communication** section **Secure-Only Device Communication** is set to **On**.

6. Look for ✓ System added.

   If an error occurs, e.g. "✗ Wrong Password", click on the **Edit System** link and correct the problem (enter the root password of the Cisco VCS).
7. Click **Finish Adding Systems**, **Add System despite warnings** or **Add More Systems** as appropriate.
8. If 'Could not connect to system. Details: No SNMP response' is reported, go to the **Connection** tab and type 'public' into the SNMP Get Community Name and select **Save/Try**.
9. If the Cisco VCS password is not default, set this up in the Connection tab or in **Settings > Edit Settings**.

- If the Cisco VCS was already configured in Cisco TMS, ensure that it has the correct IP address (in Cisco TMS, go to **Systems > Navigator** (and any required sub folders), select the Cisco VCS, and from the **Connection** tab check the **IP Address** field).

On Cisco VCS:

1. Go to the **External Manager** page (**System > External Manager**). The State should now show State Active.

Appendix 3 – IP port and protocol numbers

It is unusual to have any sort of firewall between cluster peers, but if there is, the following lists document the IP protocols and ports that must be open between each and every Cisco VCS peer in the cluster.

For cluster communications between Cisco VCS peers:

- UDP port 500 (ISAKMP) for PKI (Public Key Infrastructure) key exchange
- Standard SIP and H.323 ports are used for calls
- UDP port 1719 is used for bandwidth updates between Cisco VCS peers
- IP protocol 51 (IPSec AH) is used for database synchronization

For cluster communications between Cisco VCS peers and a Cisco TMS:

- TCP port 389 (LDAP) is used for directory lookup services
- TCP port 636 is reserved, currently not used
- TCP port 8989 is used for FindMe and provisioning data synchronization replication
- TCP port 4444 is used for FindMe and provisioning data synchronization administration from Cisco TMS to Cisco VCS

Appendix 4 – Impact of clustering on other Cisco VCS applications

Conference Factory (Multiway™)

- The Conference Factory application configuration is NOT replicated across a cluster.
- The Conference Factory template MUST be DIFFERENT on each of the Cisco VCS peers.

When configuring a cluster to support Multiway:

1. Set up the **same** Conference Factory alias (the alias called by the endpoint to initiate a Multiway conference) on each peer.
2. Set up a **different** Conference Factory template on each peer (so that each peer generates unique Multiway conference IDs).

For example, if the MCU service prefix for ad hoc conferences is **775** then the Master Cisco VCS may have a template of **775001%%@domain**, peer 2 a template of **775002%%@domain**, and peer 3 a template of **775003%%@domain**. In this way whichever Cisco VCS serves the conference ID, it cannot serve a conference ID that any other Cisco VCS could have served.

The same applies across a network. If there is more than one Cisco VCS or Cisco VCS cluster that provides Conference Factory functionality in a network, each and every Cisco VCS must provide values in a unique range, so that no two Cisco VCSs can serve the same conference ID.

Microsoft Office Communications Server 2007 (OCS) and Lync Server 2010

If OCS/Lync Server is to be configured to operate with an X7.0.n VCS cluster, see the “Cisco VCS deployment guide – Microsoft OCS 2007 (R2) and Lync 2010 and Cisco VCS Control (X7)”.

Note: If the Microsoft OCS/Lync B2BUA is turned off, some parameters on Cisco VCS, such as:

- Call routed mode
- H.323 ←→ SIP interworking mode

need setting according to that guide rather than this clustering guide.

Appendix 5 – Configuring endpoints to work with a Cisco VCS cluster

When configuring endpoints it is desirable for them to know about all the Cisco VCS peers in a cluster, so that at initial registration or later, if they lose connection to their Cisco VCS peer, they have the ability to register with and use another peer in the Cisco VCS cluster.

SIP and H.323 endpoints behave differently – the following sections show the methods that can be used, and order them in preferred order.

For additional details about DNS SRV and round-robin DNS see the URI dialling section in the Cisco VCS Administrator Guide.

Also see “Appendix 9 – Cluster name and DNS SRV records”.

H.323 endpoints

The options below are listed in preference order for providing resilience of connectivity of endpoints to a cluster of Cisco VCSs where 1 or more Cisco VCS cluster peers become inaccessible. The choice of option will depend on what functionality the endpoint you are using supports.

Option 1 – DNS SRV (preferred)

To use this option, there must be a DNS SRV record available for the DNS name of the Cisco VCS cluster that defines an equal weighting and priority for each cluster peer.

On each H.323 endpoint, configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = DNS name of the Cisco VCS cluster

If the endpoint supports DNS SRV, on startup the endpoint issues a DNS SRV request and receives a DNS SRV record back defining an equal weighting and priority for each cluster peer. It may also receive a list of lower priority entries pointing at a fallback cluster.

The endpoint then tries to register with a relevant cluster peer (having taken into account the priority / weightings). If that peer is not available, the endpoint will try and register to another listed peer at the same priority, or if all peers at that priority have been tried, a peer at the next lower (higher numbered) priority.

This will be repeated until the endpoint can register with a Cisco VCS. On registering with the Cisco VCS, the Cisco VCS will respond with the H.323 “Alternate Gatekeepers” list containing the list of Cisco VCS Cluster peer members.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection to its Cisco VCS then it will select an “Alternate Gatekeeper” from the list it was supplied with.

DNS SRV cache timeout should be set to a fairly long time (e.g. 24 hours) to minimize DNS traffic.

Option 2 – DNS Round-Robin (2nd choice)

To use this option, there must be a DNS A-record available for the DNS name of the Cisco VCS cluster that supplies a round-robin list of IP addresses.

On each H.323 endpoint configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = DNS name of the Cisco VCS cluster

If the endpoint does not support DNS SRV, on startup the endpoint will perform a DNS A-record lookup. The DNS server will have been configured to support round-robin DNS, with each of the

cluster peer members defined in the round-robin list. The DNS server will respond with one or more A-records, each time with a different IP address first.

The endpoint will take the address given by the DNS lookup and will then try and register with the relevant cluster peer. If that peer is not available, then the endpoint will perform another DNS lookup and will try to connect to the new Cisco VCS peer that it is given. (The DNS server will have supplied the next cluster peer's IP address.)

This will be repeated until the endpoint can register with a Cisco VCS. On registering with the Cisco VCS, the Cisco VCS will respond with the H.323 'Alternate Gatekeepers' list containing the list of Cisco VCS Cluster peer members.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection then it will select an "Alternate Gatekeeper" from the list it was supplied with.

DNS cache timeout should be set to a fairly short time (e.g. 1 minute or less) so that on failure to reach a Cisco VCS at startup, the endpoint is quickly pointed at a different Cisco VCS.

Option 3 – Static IP (least preferred)

Use this option if the Cisco VCS cluster does not have a DNS name.

On each H.323 endpoint configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = IP address of a Cisco VCS peer

On startup the endpoint will try and register with the VCS at the specified IP address. If that is not available, then the endpoint will continue trying at regular intervals.

This will be repeated until the endpoint can register with the Cisco VCS. On registering with the Cisco VCS, the Cisco VCS will respond with the H.323 "Alternate Gatekeepers" list containing the list of Cisco VCS Cluster peer members.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection then it will select an "Alternate Gatekeeper" from the list it was supplied with.

SIP endpoints

The options below are listed in preference order for providing resilience of connectivity of endpoints to a cluster of Cisco VCSs where 1 or more Cisco VCS cluster peers become inaccessible. The choice of option will depend on what functionality the endpoint you are using supports.

Option 1 – SIP Outbound (preferred)

SIP outbound allows an endpoint to be configured to register to 2 or more Cisco VCS peers simultaneously. The benefit of this is that if the connection between one peer and the endpoint gets broken, then a connection from the endpoint to the other peer remains. With the endpoint registering to both peers simultaneously, there is no break in service while the endpoint realizes that its registration has failed, before it registers to a different peer. Thus, at no time is the endpoint unreachable.

Configuration of SIP outbound is endpoint specific, but typically will be:

- Proxy 1
  - Server discovery = Manual
  - Server Address =
    DNS name of the Cisco VCS cluster (if DNSSRV name is available) or
    DNS name of cluster peer or
    IP address of cluster peer

- Proxy 2
  - Server discovery = Manual
  - Server Address =
    DNS name of the Cisco VCS cluster (if DNSSRV name is available) or
    DNS name of a different cluster peer or
    IP address of a different cluster peer
- Outbound = On

Option 2 – DNS SRV (2nd choice)

To use this option, there must be a DNS SRV record available for the DNS name of the Cisco VCS cluster that defines an equal weighting and priority for each cluster peer.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = DNS name of the Cisco VCS cluster

If the endpoint supports DNS SRV, on startup the endpoint issues a DNS SRV request and receives a DNS SRV record back defining an equal weighting and priority for each cluster peer. It may also receive a list of lower priority entries pointing at a fallback cluster.

The endpoint then tries to register with a relevant cluster peer (having taken into account the priority / weightings). If that peer is not available, the endpoint will try and register to another listed peer at the same priority, or if all peers at that priority have been tried, a peer at the next lower priority.

This will be repeated until the endpoint can register with a Cisco VCS.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection to its Cisco VCS, it will use the DNS SRV entry to find a new Cisco VCS to register to, starting at the highest priority.

DNS SRV cache timeout should be set to a fairly long time (e.g. 24 hours) to minimize DNS traffic.

Option 3 – DNS Round-Robin (3rd choice)

To use this option, there must be a DNS A-record available for the DNS name of the Cisco VCS cluster that supplies a round-robin list of IP addresses.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = DNS name of the Cisco VCS cluster

If the endpoint does not support DNS SRV, on startup the endpoint will perform a DNS A-record lookup. The DNS server will have been configured to support round-robin DNS, with each of the cluster peer members defined in the round-robin list. The DNS server will respond with one or more A-records, each time with a different IP address first.

The endpoint will take the address given by the DNS lookup and will then try and register with the relevant cluster peer. If that is not available, then the endpoint will perform another DNS lookup and will try to connect to the new Cisco VCS peer that it is given. (The DNS server will have supplied the next cluster peer's IP address.)

This will be repeated until the endpoint can register with a Cisco VCS.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection to its Cisco VCS it will perform another DNS lookup to find a new Cisco VCS to register to (the DNS server providing a Cisco VCS in the round-robin sequence).

DNS cache timeout should be set to a fairly short time (e.g. 1 minute or less) so that if a Cisco VCS is not accessible the endpoint is quickly pointed at a different Cisco VCS.

Option 4 – Static IP (least preferred)

Use this option if the Cisco VCS cluster does not have a DNS name.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = IP address of a Cisco VCS peer

On startup the endpoint will try and register with the Cisco VCS at the specified IP address. If that is not available, then the endpoint will continue trying at regular intervals.

This will be repeated until the endpoint can register with the Cisco VCS.

The endpoint will continue to use the first Cisco VCS that it registered to for re-registrations and for calls. If it ever loses connection then it will keep on trying to register to that Cisco VCS until it is accessible again.

Appendix 6 – Troubleshooting

Cisco VCS alarms and warnings

“Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined; see the Clustering section of the Cisco VCS Administrator Guide for more information”

Ensure that the same cluster name is configured on each VCS in the cluster.

The **Cluster name** should be the routable Fully Qualified Domain Name used in SRV records that address this Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 9 – Cluster name and DNS SRV records).

“Cluster replication error: <details> manual synchronization of configuration is required”

This may be:

- “Cluster replication error: manual synchronization of configuration is required”
- "Cluster replication error: cannot find master or this slave's peer configuration file, manual synchronization of configuration is required"
- "Cluster replication error: configuration master ID is inconsistent, manual synchronization of configuration is required"
- "Cluster replication error: this peer's configuration conflicts with the master's configuration, manual synchronization of configuration is required"

If a non-master Cisco VCS reports an alarm: “Cluster replication error – <details> synchronization of configuration”

On that non-master Cisco VCS:

- Log in as admin on an SSH or other CLI interface. At the command prompt type:
  `xcommand ForceConfigUpdate`

This will delete the non-master Cisco VCS configuration and then force it to update its configuration from the master Cisco VCS.

Caution: Only use this command if the configuration on the Master Cisco VCS is known to be in a good state.

"Cluster replication error: the NTP server is unreachable"

Configure an accessible NTP server on the Cisco VCS web page **System > Time**.

"Cluster replication error: the local VCS does not appear in the list of peers"

Check and correct the list of peers for this Cisco VCS on the Master Cisco VCS, and copy to all other Cisco VCS peers (**VCS configuration > Clustering**).

"Cluster replication error: automatic replication of configuration has been temporarily disabled because an upgrade is in progress"

Wait until the upgrade has completed.

"Invalid clustering configuration: H.323 mode must be turned On - clustering uses H.323 communications between peers"

Ensure that H.323 mode is on (see **VCS configuration > Protocols > H.323**).

“Security alert: the TMS Agent database has the default LDAP password set”

If the Cisco VCS is being managed by Cisco TMS, on Cisco TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**. In the Global (applied to all agents) section:
   a. Set up the **TMS Agent LDAP Configuration Password**.
   b. Click **Save**.

Note: This will configure the LDAP Configuration password on the Cisco TMS and all Cisco VCSs and their TMS Agents managed by that Cisco TMS.

If the Cisco VCS is a non-clustered Cisco VCS, follow the instructions in the Action link associated with the alarm.

“Security alert: the TMS Agent database has the default replication password set”

If the Cisco VCS is being managed by Cisco TMS, on Cisco TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**. In the Global (applied to all agents) section.
   a. Set up the **TMS Agent LDAP Replication Password**.
2. Click **Save**.

Note: This will configure the LDAP Configuration password on the Cisco TMS and all Cisco VCSs and their TMS Agents managed by that Cisco TMS.

If the Cisco VCS is a non-clustered Cisco VCS, follow the instructions in the Action link associated with the alarm.

“VCS database failure: Please contact your Cisco support representative”

They will help you work through the following steps:

1. Take a system snapshot and provide to TAC.
2. Remove the Cisco VCS from the cluster using: “Remove a live Cisco VCS from a VCS X7.0.n cluster (permanently)”.
3. Restore that Cisco VCS’s database by restoring a Cisco VCS backup taken on that Cisco VCS previously.
4. Add the Cisco VCS back to the cluster using “Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)”.

A second method is possible if the database does not recover:

1. Take a system snapshot and provide to TAC.
2. Remove the Cisco VCS from the cluster using: “Remove a live Cisco VCS from a VCS X7.0.n cluster (permanently)”.
3. Log in as root and run “clusterdb_destroy_and_purge_data.sh”.
4. Restore that Cisco VCS’s database by restoring a Cisco VCS backup taken on that Cisco VCS previously.

5. Add the Cisco VCS back to the cluster using "Add an X7.0.n VCS to a VCS X7.0.n cluster (n is the same value on all peers)".

Note: clusterdb_destroy_and_purge_data.sh is as dangerous as it sounds – only use this command in conjunction with instructions from TAC.

Cisco TMS

No TMS Agent tabs

If there are no TMS Agent tabs, TMS Agent has to be enabled in TMS. See the "TMS Provisioning deployment guide" for details about how to do this.

Cisco TMS warnings

TMS Cluster Diagnostics

If TMS cluster diagnostics reports a difference in configuration on Cisco VCS peers, it is comparing the output of `https://<ip address>/alternatesconfiguration.xml` for each Cisco VCS.

To manually check the differences, on a Unix / Linux system, run:

```
wget --user=admin --password=<password> --no-check-certificate https://<IP
     or FQDN of VCS>/alternatesconfiguration.xml
```

for each of the Cisco VCS peers, then use `diff` to check for differences.

Conference Factory template does not replicate

This is by design; the Conference Factory **%%** value is NOT shared between cluster peers and the Conference Factory application configuration is NOT replicated across a cluster.

See the section "Conference Factory (Multiway™)" above.

VCS's External manager protocol keeps getting set to HTTPS

Cisco TMS can be configured to force specific management settings on connected systems. This includes ensuring that a Cisco VCS uses HTTPS for feedback. If enabled, Cisco TMS will (on a time period defined by Cisco TMS) re-configure the Cisco VCS's **System > External manager** Protocol to HTTPS.

If HTTPS must be used for Cisco VCS to supply feedback to Cisco TMS, see details in "Appendix 2 – Adding a Cisco VCS to Cisco TMS" to see how to set up certificates etc.

Cisco TMS will force HTTPS on Cisco VCS if:

- **Administrative Tools > Configuration > Network Settings**, TMS Services > Enforce Management Settings on Systems = *On*
  and
- **Administrative Tools > Configuration > Network Settings**, Secure-Only Device Communication > Secure-Only Device Communication = *On*

Set **Enforce Management Settings on Systems** to *Off* if Cisco TMS does not need to force the management settings.

Set **Secure-Only Device Communication** to *Off* if it is unnecessary for Cisco VCS to provide feedback to Cisco TMS using HTTPS (if HTTP is sufficient).

My cluster of Cisco VCS Expressways with dual network interfaces is not replicating correctly

Cisco VCS Expressways with Dual Network interfaces are only designed to replicate through their LAN 1 interface. Ensure that the Peer x IP Address entries specified in **VCS configuration > Clustering** all refer to LAN 1 interfaces.

My cluster of Cisco VCS Expressways with static NAT is not replicating correctly

When using Cisco VCS Expressways with static NAT the cluster replication must occur on the LAN interface which is not behind the NAT device. Therefore LAN interface 1 must be the non NAT interface and the Peer x IP Address entries specified in **VCS configuration > Clustering** must all refer to LAN 1 interfaces. LAN interface 2 must be configured for static NAT.

Appendix 7 – Upgrading Cisco TMS to 12.6

To upgrade Cisco TMS from 12.2 to 12.6, follow the procedures documented in “Upgrade a VCS X3 / X4 cluster to an X5 cluster” in the Cluster creation and maintenance (X5) guide.

Appendix 8 – Changing the cluster name (and keeping FindMe accounts)

The cluster name specifies which data is to be used in the replicated database.

Follow this process to change the cluster name in order to retain the data associated with the previous cluster name. e.g. when a new VCS cluster is being created and the FindMe accounts are to be carried across from the Master Cisco VCS to the new cluster.

1. In the **root login**, at a command prompt, type:

   ```
   transferfindmeaccounts <current Cluster name of this VCS> <Cluster name of the cluster being created>
   ```

2. Go to **VCS configuration > Clustering** and:

   - Set **Cluster name** to be <Cluster name of the cluster being created>, where <Cluster name of the cluster being created> is the routable fully qualified domain name used in SRV records that address this Cisco VCS cluster, for example "cluster1.example.com". (See Appendix 9 – Cluster name and DNS SRV records).

Note:

- If transferfindmeaccounts is executed on multiple Cisco VCSs with different <current Cluster name of this VCS> to the same <Cluster name of the cluster being created>, the FindMe accounts from each of the Cisco VCSs will be merged into the new <Cluster name of the cluster being created> database.
- If a whole cluster is having its cluster name changed, the transferfindmeaccounts only needs to be run on the master Cisco VCS.
- If a Cisco VCS cluster has its name changed, go to Cisco TMS and select the Master Cisco VCS, select the clustering tab and ‘Cluster name has changed’ should be reported. Select ‘Update Cluster in TMS’.

Appendix 9 – Cluster name and DNS SRV records

Using DNS SRV to convert a domain to an IP address has a number of benefits:

- The structure of the lookup includes service type and protocol as well as the domain, so that a common domain can be used to reference multiple different services which are hosted on different machines (e.g. html, sip, h.323).
- The DNS SRV response includes priority and weighting values which allow the specification of primary, secondary, tertiary etc groups of servers, and within each priority group, the weighting defines the proportion of accesses that should use each server.
- Because the DNS SRV response contains details about priorities and weights of multiple servers, the receiving device can use a single lookup to search for an in-service server (where some servers are in-accessible) without the need to repeatedly query the DNS server (this is in contrast to using round robin DNS which does require repeated lookups into the DNS server if initial servers are found to be in-accessible).

The generic format of a DNS SRV query is:

- _service._protocol.<fully.qualified.domain>

The format of DNS SRV queries for sip (RFC 3263) and h.323 used by Cisco VCS are:

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>
- _sip._udp.<fully.qualified.domain> - not recommended for video calls, only use for audio-only calls
- _h323ls._udp.<fully.qualified.domain> - for udp RAS messaging, e.g LRQ
- _h323cs._tcp.<fully.qualified.domain> - for H.323 call signaling

The format of DNS SRV queries for sip (RFC 3263) and h.323 typically used by an endpoint are:

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>
- _sip._udp.<fully.qualified.domain> - not recommended for video calls, only use for audio-only calls
- _h323ls._udp.<fully.qualified.domain> - for udp RAS messaging, e.g LRQ
- _h323cs._tcp.<fully.qualified.domain> - for H.323 call signaling
- _h323rs._udp.<fully.qualified.domain> - for H.323 registrations

The DNS SRV response is a set of records in the format:

- _ service. _ protocol.<fully.qualified.domain>. TTL Class SRV Priority Weight Port Target

where Target is an A-record defining the destination.

Note: UDP is not a good transport medium for video – SIP messaging for video systems is too large to be carried on a packet based (rather than stream based) transport. UDP is often used for audio only devices.

Further details on DNS SRV can be found in the Cisco VCS Administrator Guide and RFC 2782.

The Cisco VCS **Cluster name** (configured on the **VCS configuration > Clustering** page) should be the <fully.qualified.domain> specified in the DNS SRV records that point to the Cisco VCS cluster.

Example: DNS SRV records for 2 peers of a VCS Expressway cluster for company.com

Where:

- FQDN of VCS Expressway peer 1: vcse1.company.com
- FQDN of VCS Expressway peer 2: vcse2.company.com
- FQDN of VCS Expressway cluster: company.com

```
_sips._tcp.company.com. 86400 IN SRV 1 1 5061 vcse1.company.com.
_sips._tcp.company.com. 86400 IN SRV 1 1 5061 vcse2.company.com.

_sip._tcp.company.com. 86400 IN SRV 1 1 5060 vcse1.company.com.
_sip._tcp.company.com. 86400 IN SRV 1 1 5060 vcse2.company.com.

_h323ls._udp.company.com. 86400 IN SRV 1 1 1719 vcse1.company.com.
_h323ls._udp.company.com. 86400 IN SRV 1 1 1719 vcse2.company.com.

_h323cs._tcp.company.com. 86400 IN SRV 1 1 1720 vcse1.company.com.
_h323cs._tcp.company.com. 86400 IN SRV 1 1 1720 vcse2.company.com.

_h323rs._udp.company.com. 86400 IN SRV 1 1 1719 vcse1.company.com.
_h323rs._udp.company.com. 86400 IN SRV 1 1 1719 vcse2.company.com.
```

Note:

- Priorities are all the same – only use different priorities if you have different clusters allowing failover from one primary cluster to another (secondary) cluster
  - in that case the primary cluster's peers should have one value and the other (secondary) cluster's peers a (larger) value
- Weights should be the same – so that there is equal use of each peer

Endpoints supporting SIP DNS SRV

Movi versions prior to 4.0 supports:

- _sip._tls.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

Movi version 4.0 and later supports:

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

E20 version TE2.1 and later supports:

- _sips._tls.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

MXP version F8.2 and later supports:

- _sip._tls.<fully.qualified.domain>

- _sip._tcp.<fully.qualified.domain>

T150 version L6.0 supports:

- _sip._tls.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

C-Series versions prior to TC4.0 supports:

- _sip._tls.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

C-Series from version TC4.0 supports:

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

Cisco TelePresence MCU supports:

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

SIP DNS SRV records required:

- _sips._tcp.<fully.qualified.domain> Movi (4.0 and later), C-Series (TC4.0 and later), Cisco VCS, MCU
- _sips._tls.<fully.qualified.domain> E20 to TE2.1
- _sip._tls.<fully.qualified.domain> MXP to F8.2, T150 to L6.0, Movi prior to 4.0, C-Series prior to TC4.0
- _sip._tcp.<fully.qualified.domain> All products for TCP

Note:

- UDP is not a good transport medium for video signaling – SIP messaging for video systems is too large to be carried on a packet based (rather than stream based) transport. UDP is often used for audio only devices.
- _sip._tls,<fully.qualified.domain> is an SRV record also used by Microsoft OCS Edge servers.

Looking up .SRV records

Nslookup

```
nslookup -query=SRV _sip._tcp.example.com
```

Dig

```
dig _sip._tcp.example.com SRV
```

```
; <<>> DiG 9.4.1 <<>> _sip._tcp.example.com SRV
;; global options:  printcmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44952
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;_sip._tcp.example.com.         IN      SRV

;; ANSWER SECTION:
_sip._tcp.example.com. 1183     IN   SRV     1 0 5060 sbc1.example.com.
_sip._tcp.example.com. 1183     IN   SRV     1 0 5060 sbc2.example.com.

;; AUTHORITY SECTION:
example.com.           87450    IN      NS      ns1.mydyndns.org.
example.com.           87450    IN      NS      ns2.mydyndns.org.

;; ADDITIONAL SECTION:
sbc1.example.com.      1536     IN      A       194.73.59.53
sbc2.example.com.      1376     IN      A       194.73.59.54
ns1.mydyndns.org.        75     IN      A       204.13.248.76
ns2.mydyndns.org.     10037     IN      A       204.13.249.76

;; Query time: 0 msec
;; SERVER: 10.44.8.11#53(10.44.8.11)
;; WHEN: Mon Jul 26 11:09:59 2010
;; MSG SIZE  rcvd: 243

~ #
```

Appendix 10 – NAPTR records

NAPTR records are typically used to specify various methods to connect to a destination URI, for example by email, by SIP, by H.323. They can also be used to specify the priority to use for those connection types, for example to use SIP tls in preference over using SIP tcp or SIP udp.

NAPTR records are also used in ENUM, when converting a telephone number into a dialable URI.

(For further details on ENUM see “Cisco VCS Deployment Guide - ENUM dialing on VCS”, document reference D14465).

E20 video endpoints use NAPTR records to identify whether they are inside a private network (and so should request provisioning data for the internal network) or are outside in the public internet (where they should request provisioning data for devices in the public network). The flag “s” is extended to “se” to indicate to the E20 that it is “external”.

(For further details see the “Cisco TMS Provisioning Deployment Guide”, document reference D14368).

NAPTR record format

Example: SIP access to example.com, and for enum lookups for 557120, 557121, and 557122.

$ORIGIN example.com.

```
IN      NAPTR   10   100   "s"   "SIPS+D2T"    ""                    _sips._tcp.example.com.
IN      NAPTR   12   100   "s"   "SIP+D2T"     ""                    _sip._tcp.example.com.
IN      NAPTR   14   100   "s"   "SIP+D2U"     ""                    _sip._udp.example.com.
```

$ORIGIN www.example.com.

```
IN      NAPTR   10   100   "s"   "http+I2R"    ""                    _http._tcp.example.com.
IN      NAPTR   10   100   "s"   "ftp+I2R"     ""                    _ftp._tcp.example.com.
```

$ORIGIN 0.2.1.7.5.5.enum.lookup.com.

```
IN      NAPTR   10   100   "u"   "E2U+sip"     "!^.*$!john.smith@tandberg.com!"      .
IN      NAPTR   12   100   "u"   "E2U+h323"    "!^.*$!john.smith@tandberg.com!"      .
IN      NAPTR   10   100   "u"   "mailto+E2U"  "!^.*$!mailto:john.smith@tandberg.com!"      .
```

$ORIGIN 1.2.1.7.5.5.enum.lookup.com.

```
IN      NAPTR   10   100   "u"   "E2U+sip"     "!^.*$!mary.jones@tandberg.com!"      .
```

$ORIGIN 2.2.1.7.5.5.enum.lookup.com.

```
IN      NAPTR   10   100   "u"   "E2U+h323"    "!^.*$!peter.archibald@myco.com!"     .
```

```
IN = Internet routing
         NAPTR = record type
                  10 = order value (use lowest order value first)
                        100 = preference value if multiple entries have the same order value
                               "u" = the result is a routable URI
                               "s" = the result is a DNS SRV record
                               "a" = the result is an ‘A’or ‘AAAA’ record
                                     "E2U+sip" to make SIP call
                                     "E2U+h323" to make h.323 call
                                                   Regular expression:
                                                   ! = delimiter
                                                   "" = no expression used
                                                   … usual Regex expressions can be used
                                                                 Replace field; . = not used
```

Looking up NAPTR records

Looking up an ENUM NAPTR record

dig 4.3.7.8.enum4.example.com. NAPTR

```
; <<>> ;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38428
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2


;; QUESTION SECTION:
;4.3.7.8.enum4.example.com. IN   NAPTR


;; ANSWER SECTION:
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+sip" "!^.*$!steve.hight@example.com!" .
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+h323" "!^.*$!steve.hight@example.com!"
.


;; AUTHORITY SECTION:
enum4.example.com. 60    IN      NS      int-server1.example.com.


;; ADDITIONAL SECTION:
int-server1.example.com. 3600 IN A       10.44.9.144
int-server1.example.com. 3600 IN AAAA    3ffe:80ee:3706::9:144


;; Query time: 0 msec
;; SERVER: 10.44.8.11#53(10.44.8.11)
;; WHEN: Tue Jul 13 16:51:41 2010
;; MSG SIZE  rcvd: 251


#
```

Looking up a domain NAPTR record

Example: NAPTR record allowing E20 endpoints to detect that they are in the public (external) network.

~ # dig -t NAPTR example.com

```
; <<>> DiG 9.4.1 <<>> -t NAPTR example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1895
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 4


;; QUESTION SECTION:
;example.com.                    IN      NAPTR


;; ANSWER SECTION:
example.com.              2      IN   NAPTR   50 50 "se" "SIPS+D2T" "" _sips._tcp.example.com.
example.com.              2      IN   NAPTR   90 50 "se" "SIP+D2T" "" _sip._tcp.example.com.
example.com.              2      IN   NAPTR   100 50 "se" "SIP+D2U" "" _sip._udp.example.com.


;; AUTHORITY SECTION:
example.com.              320069 IN      NS      nserver2.example.com.
example.com.              320069 IN      NS      nserver.euro.example.com.
example.com.              320069 IN      NS      nserver.example.com.
example.com.              320069 IN      NS      nserver3.example.com.
example.com.              320069 IN      NS      nserver4.example.com.
example.com.              320069 IN      NS      nserver.asia.example.com.


;; ADDITIONAL SECTION:
nserver.example.com.      56190   IN      A       17.111.10.50
nserver2.example.com.     57247   IN      A       17.111.10.59
nserver3.example.com.     57581   IN      A       17.22.14.50
nserver4.example.com.     57452   IN      A       17.22.14.59


;; Query time: 11 msec
;; SERVER: 10.44.8.11#53(10.44.8.11)
;; WHEN: Tue Jul 13 17:08:40 2010
;; MSG SIZE  rcvd: 385


~ #
```