Cisco Expressway Cluster Creation and Maintenance

Deployment Guide

First Published: December 2009

Last Updated: July 2019

X8.11.4

Contents

Preface

Change History

Table 1 Expressway Cluster Deployment Guide Change History

Date	Change	Reason
July 2019	Clarify that registering a device using SIP Outbound consumes RMS licenses per registration.	Clarification
March 2019	Clarify that removal of a cluster peer deletes *all* configuration for the LAN2 interface in dual NIC deployments.	Clarification
February 2019	Cluster Address Mapping section edited. Software version updated to X8.11.4 maintenance release. Other superficial enhancements to text.	Documentation defect, X8.11.4 release
September 2018	Updated for Webex and Spark platform rebranding, CE1200 appliance, and X8.11.1 maintenance release.	X8.11.1 release
August 2018	Corrected text and example in 'Cluster Name and DNS SRV Records' section.	Correction
July 2018	Updated for X8.11	X8.11 release
November 2017	Updated round trip delay and maximum hop distances in 'Prerequisites' section.	Update
October 2017	Strengthened advice on cluster upgrade order.	Clarification
August 2017	Added note that all cluster peers should be configured in the same domain.	Omission
July 2017	Updated for X8.10.	X8.10 release
April 2017	Added section and related edits for cluster address mapping.	X8.9.2 release
December 2016	Added section on clusters in isolated networks in relation to TLS.	X8.9 release
June 2016	Cluster communications now use TLS. Registrations, FindMe, TMSPE support introduced on Expressway.	X8.8 release
November 2015	Updated for X8.7.	
July 2015	Updated for X8.6. New procedure for replacing a peer.	
April 2015	Menu path changes for X8.5 onwards. Republished with X8.5.2.	
December 2014	Updated for X8.5.	
June 2014	Republished for X8.2.	

Table 1 Expressway Cluster Deployment Guide Change History (continued)

Date	Change	Reason
April 2014	Updated for Expressway X8.1.1: ■ New 'Upgrading a cluster' section for Expressway ■ New 'Replacing an Expressway peer' section ■ Updates to 'IP ports and protocols' appendix	
December 2013	First release of Expressway version of this document. For older VCS versions see VCS Configuration Guides page.	

Introduction

This Expressway guide also now applies to VCS. Any VCS-specific information is noted where necessary in the guide. (Older VCS guides on Cisco.com are still valid for the VCS versions they apply to—as specified on the title page of each guide.)

Benefits of clustering Expressway

Expressway clusters are designed to extend the resilience and capacity of an Expressway installation. Expressway peers in a cluster share bandwidth usage as well as routing, zone, FindMe™ and other configuration. Endpoints can register to any of the peers in a cluster. If endpoints lose connection to their initial peer, they can re-register to another one in the cluster.

The Small Expressway VMs are intended for Cisco Business Edition 6000 customers. Therefore clustering of Small VMs only provides redundancy and does not offer any additional scale benefit.

Capacity licensing is done on a per-cluster basis. Any capacity licenses installed on a cluster peer are available to any peer in the cluster. If a cluster peer becomes unavailable, the license capacity installed on that peer remains available to the rest of the cluster for two weeks after it lost contact with the peer. This maintains the overall license capacity of the cluster. Each peer is always limited by its physical capacity, and the license capacity borrowing is only intended to give you time to repair your cluster.

"Capacity" includes the following license types:

- On VCS: traversal and non-traversal call licenses
- On Expressway: Rich Media Session licenses
- On Expressway: Room system and desktop system registration licenses

Every Expressway peer in the cluster must have the same routing capabilities – if any Expressway can route a call to a destination it is assumed that all Expressway peers in that cluster can route a call to that destination. If routing is different on different Expressway peers, then you need to use separate Expressways / Expressway clusters.

Connecting to Cisco TMS

Cisco TMS is not essential for clustering. If you are not using Device Provisioning or FindMe with your cluster, then Cisco TMS is optional but recommended.

You **must** use Cisco TMS in Provisioning Extension mode if:

- You want to use Device Provisioning with the Expressway cluster
- You want to use FindMe with the Expressway cluster

Enabling provisioning and creating a cluster are two separate processes. If you want to enable provisioning on your cluster, do **either** of the following:

- Use the instructions in this guide to create the cluster of Expressways (without provisioning enabled). Then follow the instructions in *Cisco TMS Provisioning Extension Deployment Guide* to enable provisioning across the cluster.
- Use the instructions in *Cisco TMS Provisioning Extension Deployment Guide* to enable provisioning on what will be the primary Expressway. Then follow the instructions in this guide to create the cluster of Expressways.

What's in this guide

This guide is arranged into sections to help you create and maintain your Expressway clusters:

- Clustering Prerequisites, page 8

  Describes the required network environment and minimum configuration of the peer Expressways before you can cluster them.

- Form a Cluster, page 11

  Describes forming a cluster of one, adding peers to a cluster, and configuring cluster address mapping (if necessary).
- Change a Cluster, page 25

  Describes processes like upgrading, taking peers offline, changing the primary peer, and disbanding the cluster.
- Connect the Expressway Cluster to Other Systems, page 36

  Describes connecting the cluster with other systems like Cisco TMS, other Expressways, and endpoints.
- Troubleshooting, page 42

  Some general guidance and also specific scenarios that you might need when the cluster is not working as expected.
- Reference, page 46

  Additional material that may be relevant to your environment but is not directly related to working with clusters.

Clustering Prerequisites

Before setting up a cluster of X8.11.4 Expressway peers or adding an X8.11.4 Expressway to a cluster, ensure that the following requirements are met:

Platform and software versions match

- All clusters peers are running the same Expressway version. The only occasion where different peers are 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, during which time the cluster operates in a partitioned fashion.
- Each peer is using a hardware platform (appliance or virtual machine) with equivalent capabilities. For example, you can cluster peers that are running on standard appliances with peers running on 2 core Medium VMs, but you can't cluster a peer running on a standard appliance with peers running on 8 core Large VMs.

Network conditions are met

- Each peer has a different LAN configuration (a different IPv4 address and a different IPv6 address, where enabled).
- Expressway supports a round trip delay of up to 80ms. This means that each Expressway in the cluster must be within a 40ms hop of all other peers in the cluster.
- Each peer in a cluster is directly routable to each and every other Expressway 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.)
- External firewalls are configured to block access to the clustering TLS ports.
- The network connections between the peers must be reliable during cluster forming or changing procedures.

  Clustering procedures are sensitive to sequencing, particularly after the introduction of X8.11. The primary peer must start first; if other peers start first they can try to assume control of the cluster, resulting in inconsistent configuration state that is hard to recover from.

Basic configuration is done

- Each peer has a different system name to all other peers.
- All cluster peers are configured in the same domain.
- Each peer has a certificate that identifies it to other peers (minimum required for default of **TLS verification mode** set to *Permissive*).

  If you wish to have authenticated TLS connections, the certificate must also be valid and be issued by an authority that is trusted by all peers (**TLS Verification mode** set to *Enforce*).

  We recommend populating the CN of all peer certificates with the same cluster FQDN, and populating each peer certificate's SAN with that peer's FQDN.

  Note: Although using one certificate for multiple Expressways in one cluster is supported, this is not recommended due to the security risk. That is, if one private key is compromised on one device, it means all devices in the cluster are compromised.
- All peers have the same set of option keys installed, with the following exceptions:
  - For VCS: Traversal and non-traversal call licenses
  - For Expressway: Rich Media Sessions
  - For Expressway: Room system and desktop system registration licenses

    All other license keys must be identical on each peer.

    Note: Installing some types of option keys requires you to restart the Expressway.

- H.323 mode is enabled on each peer (**Configuration > Protocols > H.323**, and for **H.323 mode** select *On*).

  The cluster uses H.323 signaling between peers to determine the best route for calls, even if all endpoints are SIP endpoints.
- The firewall rules on each peer are configured to block connections to the clustering TLS ports, from all IP addresses except those of its peers.

  See Sample Firewall Rules for Protecting Intracluster TLS Ports, page 48.

DNS configuration is done

DNS server configuration does not replicate so you must enter the DNS server address(es) on each peer.

- The DNS servers used by the Expressway peers must support both forward and reverse DNS lookups of Cisco TMS and all Expressway peer addresses. The DNS servers must also provide address lookup for any other DNS functionality required, such as:
  - NTP servers or the external manager if they configured using DNS names
  - Microsoft FE Server FQDN lookup
  - LDAP server forward and reverse lookup (reverse lookups are frequently provided through PTR records)

  Note: Cisco Expressway-E typically uses a public DNS, but it's undesirable to use the public DNS to resolve **private** IP addresses. It's also undesirable to cluster on the public addresses of the Cisco Expressway-E peers. For these reasons, we recommend you use cluster address mapping to resolve the peers' FQDNs to **private** IP addresses. For detailed steps, see Cluster Address Mapping for Cisco Expressway-E Clusters, page 19.
- A DNS SRV record is required for the cluster, which contains A or AAAA records for each peer.

  This configuration is advised for video interoperability and business to business (B2B) video calling, but is **not required for Mobile and Remote Access**.
- (For MRA) Create a `collab-edge` SRV record for each peer in the Expressway-E cluster.
- (For B2B only) The Expressway-E cluster has a DNS SRV record that defines all cluster peers.

TMS is configured (if necessary)

- Cisco TMS, if used, is running version 13.2 or later (12.6 or later is permitted if you are not using Cisco TMS for provisioning or FindMe).
- If Cisco TMS is to be used for replicating FindMe and/or Provisioning data, ensure that Provisioning Extension mode functionality is enabled on Cisco TMS (see *Cisco TMS Provisioning Extension Deployment Guide* for details).

Clusters with mixed CE1200 and CE1100 physical appliances

To add a CE1200 appliance to an existing cluster that has CE1100 models in it, configure the Type option to match the other peers (Expressway-E or Expressway-C) through the service setup wizard on the **Status > Overview** page, *before* you add the CE1200 to the cluster.

Cluster capacity for MRA registrations

This section applies if you deploy Cisco Unified Communications Manager and use the Mobile and Remote Access feature.

The cluster capacity for MRA registrations is as follows:

If the cluster peers are…	The maximum MRA registrations capacity is…
CE1200 appliances	5000 per peer (up to 20,000 total in a 6-peer cluster)
CE1100 appliances	2500 per peer (up to 10,000 total in a 6-peer cluster)
Large VMs	2500 per peer (up to 10,000 total in a 6-peer cluster)

If the cluster peers are...	The maximum MRA registrations capacity is...
Mix of CE1200s with CE1100s and/or Large VMs	2500 per peer (up to 10,000 total in a 6-peer cluster) **Note:** The CE1200 capacity "drops" to the capacity of the other cluster peers

Form a Cluster

- You can have up to 6 Expressways in a cluster, including the primary.
- You should add peers to the cluster one by one.
- You should only make configuration changes on the primary Expressway.

  Caution: Do not adjust any cluster-wide configuration until the cluster is stable with all peers running. Cluster database replication will be negatively impacted if any peers are upgrading, restarting, or out of service when you change the cluster's configuration.

  Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the primary's configuration is replicated across the peers. The only exceptions to this are some peer-specific configuration items.

  You may need to wait up to one minute before changes are updated across all peers in the cluster.
- The clustering interface must not have NAT enabled on it.
- Cluster communication failure alarms are raised while the cluster is forming. Alarms should clear when you're finished.
- Configuration replication is suspended to new Expressways before they have properly joined the cluster.
- If the new Expressway peer has two network interfaces, the **Peer *N* address** MUST NOT specify the external interface.

  However, if you need to enforce TLS between peers, you'll need to use the FQDN of the peer as it appears on the peer's certificate. See Cluster Address Mapping for Cisco Expressway-E Clusters, page 19, to map FQDNs to the internal IP addresses.

Preparing Expressway to Join a Cluster

- If necessary, take the new peer out of service:

  a. Enable maintenance mode:

     1. Go to **Maintenance > Maintenance mode**.
     2. Set **Maintenance mode** to *On*.
     3. Click **Save** and click **OK** on the confirmation dialog.

  b. Wait for all calls to clear and registrations to timeout on this peer.

     - If necessary, manually remove any calls on this peer that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
     - If necessary, manually remove any registrations from this peer that do not clear automatically (using the web browser go to **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).

  c. If the Expressway is in a cluster, remove it from its existing cluster then restart it.

  d. Factory reset the Expressway (unless you already did this, because of the restart in previous step).

- Check that the address of your Expressway is not a peer of any other Expressway in your organization.
- Check that the Expressway is not a neighbor, traversal client, or traversal server of any other Expressway.
- Review and modify the configuration to ensure that the Expressway has:
  - A valid Ethernet speed (**System > Network interfaces > Ethernet**).
  - Valid IP address and IP gateway (**System > Network interfaces > IP**).
  - A valid and working NTP server configured (**System > Time**; in the Status section, the State should be "Synchronized").
  - 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**).
  - Go to **System > DNS** and ensure that **System host name** is the DNS hostname for this Expressway (typically the same as the **System name** in **System > Administration**, but excluding spaces, and unique for each Expressway in the cluster). If it is not configured correctly, set it up appropriately and click **Save**.

    Note: <System host name>.<DNS domain name> = FQDN of this Expressway
  - No peers configured (on **System > Clustering** – all Peer N address fields on this page should be blank).

    CAUTION: If you clear all the peer address fields from the clustering page and save the configuration, then the Expressway will factory reset itself the next time you do a restart. This means you will lose all existing configuration except basic networking for the LAN1 interface, including all configuration that you do between when you clear the fields and the next restart.

    If this Expressway is already a member of a cluster, you should remove it from that cluster and restart it before you use it in another cluster.
  - The same set of option keys installed as those that will be installed on all other peers of the cluster (**Maintenance > Option keys**).

    The number of call/RMS/device/room licenses may differ between peers; all other license keys must be identical on each peer.
  - **H.323 Mode** set to *On* (**Configuration > Protocols > H.323**)

- If this Expressway is joining a cluster that is integrated with Cisco TMSPE, Add the Expressway to Cisco TMS, page 41, then:

  a. Check that the new Expressway can see Cisco TMS.

     To do this, go to **System > External manager** and in the Status section, ensure that the **State** is Active.

  b. Check that Cisco TMS knows the Host Name of the Expressway:

     1. Go to **Systems > Navigator** (and any required sub folders).
     2. Select this Expressway.
     3. Select the **Connection** tab.
     4. Set **Host Name** to be the FQDN of this subordinate peer, for example vcs3.uk.company.com.
     5. Click **Save/Try**.
        You can ignore any error messages such as "`DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>`"
     6. Ensure that Cisco TMS updates its DNS.

        1. Select the **Settings** tab.
        2. Click **Force Refresh**.

  c. Check that Cisco TMS can communicate with the new Expressway.

     To do this, on Cisco TMS go to **Systems > Navigator** (and any required sub folders) then click on the name of the Expressway and ensure that it says:

     "✓ System has no open or acknowledged tickets"

- Go to **Status > Alarms**. If there is an alarm that the Expressway must be restarted, go to **Maintenance > Restart options** and then click **Restart**.

Create a New Cluster of Expressway Peers

This process initiates a cluster of a single Expressway. Do not use this process if the cluster already exists.

Important: You **must** create a cluster of one (primary) peer first, and restart the primary, before you add other peers. You can add more peers after you have established a "cluster of one".

1. Decide which Expressway will be the primary peer.

   The primary Expressway will be the source of the configuration information for all Expressway peers in the cluster. Subordinate Expressway peers will have most of their configuration deleted and replaced by that from the primary.

2. Check that the Expressway is running X8.11.4 software.
3. Backup the Expressway (**Maintenance > Backup and restore**).
4. Review and modify the configuration to ensure that the Expressway has:
   - A valid Ethernet speed (**System > Network interfaces > Ethernet**).
   - Valid IP address and IP gateway (**System > Network interfaces > IP**).
   - A valid and working NTP server configured (**System > Time**; in the Status section, the State should be "Synchronized").
   - 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**).
   - Go to **System > DNS** and ensure that **System host name** is the DNS hostname for this Expressway (typically the same as the **System name** in **System > Administration**, but excluding spaces, and unique for each Expressway in the cluster). If it is not configured correctly, set it up appropriately and click **Save**.

     Note: <System host name>.<DNS domain name> = FQDN of this Expressway
   - No peers configured (on **System > Clustering** – all Peer N address fields on this page should be blank).

     CAUTION: If you clear all the peer address fields from the clustering page and save the configuration, then the Expressway will factory reset itself the next time you do a restart. This means you will lose all existing configuration except basic networking for the LAN1 interface, including all configuration that you do between when you clear the fields and the next restart.

     If this Expressway is already a member of a cluster, you should remove it from that cluster and restart it before you use it in another cluster.
   - The same set of option keys installed as those that will be installed on all other peers of the cluster (**Maintenance > Option keys**).

     The number of call/RMS/device/room licenses may differ between peers; all other license keys must be identical on each peer.
   - **H.323 Mode** set to *On* (**Configuration > Protocols > H.323**)
5. Ensure that this Expressway does not list any of the Expressways that are to be peers in this new cluster in any of its neighbor zones or traversal zones (**Configuration > Zones > Zones** then check each neighbor and traversal zone).
6. Set the **H.323 Time to live** to an appropriate value for the size of your deployment. A smaller number, like 60 (seconds), means that if one Expressway becomes inaccessible, the endpoint will quickly register with another peer (**Configuration > Protocols > H.323**).

   Note: By reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.

7. Go to **System > DNS** and ensure that **System host name** is the DNS hostname for this Expressway (typically the same as the **System name** in **System > Administration**, but excluding spaces, and unique for each Expressway in the cluster). If it is not configured correctly, set it up appropriately and click **Save**.

   Note: <System host name>.<DNS domain name> = FQDN of this Expressway
8. Go to **Configuration > Call routing** and set **Call signaling optimization** to *On*.
9. Click **Save**.
10. Enable maintenance mode:

    a. Go to **Maintenance > Maintenance mode**.

    b. Set **Maintenance mode** to *On*.

    c. Click **Save** and click **OK** on the confirmation dialog.
11. Wait for all calls to clear and registrations to timeout on this peer.

    - If necessary, manually remove any calls on this peer that do not clear automatically (using the web browser go to **Status > Calls**, then select the check box next to the calls you want to terminate and click **Disconnect**).
    - If necessary, manually remove any registrations from this peer that do not clear automatically (using the web browser go to **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).
12. (Not applicable to MRA) Go to **System > Clustering** and ensure that **Cluster name** is the routable Fully Qualified Domain Name used in SRV records that address this Expressway cluster, for example `cluster1.example.com`. (See Cluster Name and DNS SRV Records, page 50).

    Change the **Cluster name** if necessary.
13. Click **Save**.

14. On the **Clustering** page configure the fields as follows:

Configuration primary	1
Cluster IP version	Choose *IPv4* or *IPv6* to match the underlying network addressing scheme.
TLS verification mode	Options: *Permissive* (default) or *Enforce*. *Permissive* means that the peers do not validate each others' certificates when establishing intracluster TLS connections. *Enforce* is more secure, but requires that each peer has a valid certificate and that the signing CA is trusted by all other peers. We recommend you form a cluster using FQDN and TLS verification as follows: form your cluster using IP addresses in *Permissive* mode and then change the peer addresses to FQDNs. You can then switch TLS verification mode to *Enforce*. If you are clustering Expressway-E peers in an isolated network, you also need to configure cluster address mappings. For detailed steps, see Cluster Address Mapping for Cisco Expressway-E Clusters, page 19.
Peer 1 address	Enter the address of this Expressway (the primary peer). If **TLS verification mode** is set to *Enforce*, then you must enter an FQDN that matches the subject CN or a SAN on this peer's certificate.

15. Click **Save**.

    To the right of the **Peer 1 address** field the words "This system" should appear (though this may require the page to be refreshed before they appear).
16. Restart the Expressway (go to **Maintenance > Restart options**, then click **Restart** and confirm **OK**).
17. Check that configuration data exists as expected:
    - If FindMe is in use, check that the expected FindMe entries still exist (**Status > Applications > TMS Provisioning Extension Services > FindMe > Accounts**).
    - Check configuration for items from the **System**, **Configuration** and **Application** menus.
18. Check that maintenance mode is disabled.
    a. Go to **Maintenance > Maintenance mode**.
    b. Set **Maintenance mode** to *Off*.
    c. Click **Save**.
19. Backup the Expressway (**Maintenance > Backup and restore**).

You've finished forming a cluster (of one Expressway)

Next Steps

- Go to **Status > Alarms** and ensure that all alarms are acted upon and cleared.
- Add other Expressways to the cluster using Add a Peer to a Cluster, page 18.

Add a Peer to a Cluster

This procedure adds a new peer to an existing X8.11.4 cluster (of one or more peers) and replicates the primary peer's configuration onto the Expressway.

If you do not have an existing cluster, see Create a New Cluster of Expressway Peers, page 14.

1. Go to **System > Clustering** on the primary Expressway.

   One or more of the **Peer *N* address** fields should be empty.
2. In the first empty field, enter the address of the new Expressway peer.
3. Click **Save**.

   Peer 1 should indicate 'This system'. The new peer may indicate 'Unknown' and then with a refresh should indicate 'Failed' because it has not fully joined the cluster yet.
4. Go to **System > Clustering** on one of the subordinate peers already in the cluster, and edit the following fields:

Cluster name	Identical to the **Cluster name** configured on the primary Expressway
Configuration primary	Same number as chosen on the primary Expressway
Cluster IP version	Same version as chosen on the the primary Expressway
TLS verification mode	Same setting as chosen on the primary Expressway*
Peer 1 address ...Peer 6 address	The addresses should be the same, and in the same order, as those entered on the primary Expressway

   *If you intend to use cluster address mapping, all devices in the cluster should be in Permissive mode initially. For more information, see Cluster Address Mapping for Cisco Expressway-E Clusters, page 19

   Save the new clustering configuration.
5. Repeat the previous step for each of the subordinate peers already in the cluster.
6. Go to **System > Clustering** on the new peer:

Cluster name	Identical to the **Cluster name** configured on the primary Expressway
Configuration primary	Same number as chosen on the primary Expressway
Cluster IP version	Same version as chosen on the the primary Expressway
TLS verification mode	Same setting as chosen on the primary Expressway*
Peer 1 address ...Peer 6 address	The addresses should be the same, and in the same order, as those entered on the primary Expressway

   *If you intend to use cluster address mapping, all devices in the cluster should be in Permissive mode initially. For more information, see Cluster Address Mapping for Cisco Expressway-E Clusters, page 19
7. **Save** the new clustering configuration.

   The Expressway raises a cluster communication failure alarm. The alarm clears after the required restart.
8. Restart the Expressway (go to **Maintenance > Restart options**, then click **Restart** and confirm **OK**).

Checks

1. After the restart, wait approximately 2 minutes – this is the frequency with which configuration is copied from the primary.
2. Check the Cluster database status.
3. Check that configuration data exists as expected:
   - If FindMe is in use, check that the expected FindMe entries still exist (**Status > Applications > TMS Provisioning Extension Services > FindMe > Accounts**).
   - Check configuration for items from the **System**, **Configuration** and **Application** menus.

Next Steps

- Add more peers if necessary.
- If you are using Conference Factory (Multiway™) in your cluster, see Impact of Clustering on Other Expressway Applications, page 56.
- If you want peers to resolve their FQDNs to their private IP addresses, seeCluster Address Mapping for Cisco Expressway-E Clusters, page 19

[Optional] Use Fully Qualified Domain Names to Form a Cluster

This chapter is about changing a cluster, that was formed using IP addresses, so that the peers use FQDNs to form the cluster. This is necessary if you want to enforce TLS verification between peers. If you have not yet formed your cluster, see Form a Cluster, page 11.

If you are creating a cluster of Expressway-Es, they might be in an isolated network such as a DMZ, and you'll need to use a local mapping if you want to enforce TLS verification. If you're forming a cluster of Expressway-Cs, you should not need to use cluster address mapping.

Cluster Address Mapping for Cisco Expressway-E Clusters

For secure deployments like MRA, each Expressway-E peer must have a certificate with a SAN containing its public FQDN. The FQDN is mapped in the public DNS to the Expressway-E's public IP address. This configuration enables external entities, like MRA endpoints, to discover the Expressway-E's public interface and establish a secure connection.

Do You Need Cluster Address Mapping?

- If you simply want to cluster Cisco Expressway-E peers and you don't need TLS verification between them, then you can form the cluster using the nodes' private IP addresses. You don't need cluster address mapping.
- If you want the Expressway-E peers in a cluster to verify each other's identities using certificates, you could allow them to use DNS to resolve cluster peer FQDNs to their public IP addresses. This is a perfectly acceptable way to form a cluster if the Expressway-E nodes have only one NIC, are not using static NAT, and have routable IP addresses. You don't need cluster address mapping.

- If your security policy dictates that you enforce TLS verification between the peers, and if the Expressway-Es are using static NAT, or dual NIC, or both, then we do not recommend using the external interfaces or the static NAT addresses to form the cluster.

  Also, do not try to use the public DNS to map the peers' public FQDNs to their private IP addresses, because you will break external connectivity.

  You should use cluster address mapping in these situations.

How Cluster Address Mapping Works

When you use Fully Qualified Domain Names to form the cluster, peers must be able to translate those names into IP addresses. This translation is the main reason for DNS but, if the peers have no access to DNS, or if you need to translate the FQDN into a private IP address, then you can populate the cluster address mapping table to provide a local alternative to the DNS.

Cluster address mappings are FQDN:IP pairs which are shared around the cluster, one pair for each peer. The peers consult the mapping table before they query DNS and, if they find a match, they do not query DNS.

If you choose to enforce TLS, the peers must also read the names from the SAN field of each other's certificates, and check each name against the FQDN side of the mapping. If the SAN matches the FQDN side of the mapping, and if the IP address that presented the certificate matches the IP side of the mapping, then the peer trusts the other peer and they can establish the TLS connection.

Without using DNS, cluster address mapping is the only way to achieve this verification.

Where Does the Suggested Mapping Come From?

If the cluster is already formed, using IP addresses, and the peers already have a **System host name** and a **DNS name** configured on the **System > DNS** page, then you have the option to automatically populate the cluster address mapping table with *assumed mappings* as follows:

`Peer1Hostname.Peer1DNSName` maps to `<Peer1 Private IP address>`

...

`Peer6Hostname.Peer6DNSName` maps to `<Peer6 Private IP address>`

Note: This automatic mapping may be incorrect! If the peers' certificates do not contain these assumed FQDNs in their SAN fields, then the cluster will not form when **TLS verification mode** is changed to *Enforce*. You must check that the SANs contain the entries that you place in the peer FQDN fields.

Configure Cluster Address Mapping (Expressway-E Clusters)

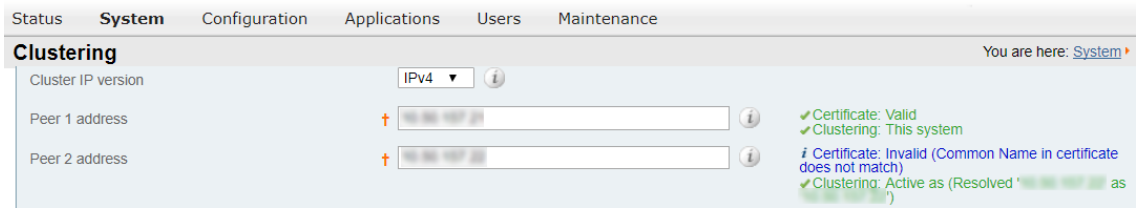
We strongly recommend that you enter the mappings on the primary peer. Address mappings replicate dynamically through the cluster.

The mapping order is unimportant, but if you are using address mappings you must create mappings for every cluster peer, using only **private** IP addresses.

1. Form your cluster using IP addresses (as described in Create a New Cluster of Expressway Peers, page 14 and Add a Peer to a Cluster, page 18) with **TLS verification mode** set to *Permissive*.

2. Verify that the cluster is correctly formed, by checking for green *Clustering* status messages against the peer address fields.

   You will also see blue *Certificate: Invalid …* status messages. This is because your certificates should not correspond with internal/private IP addresses, assuming they are correctly formed to identify peers by FQDN. This is expected behavior and does not prevent you from proceeding.



3. Go to **System > Clustering** on the primary peer, and change the **Cluster address mapping enabled** drop-down to *On* (default is *Off*).

   The **Cluster address mapping** fields display.

4. [Optional, see note above] Click **Suggest mappings based on system information** to autofill the mapping fields for each cluster peer.

   This uses the **System host name** and **DNS name** configured on the **System > DNS** pages of each peer, and maps them to the IP addresses of the inward facing NICs.

   The fields must be empty before you do the autofill.

5. [If you used the autofill option] Check that the suggested mappings correspond to the names in the peers' certificates, and the IP addresses of the NICs that you want to cluster. (The data is built up from information which may not match the certificate or DNS.)

6. Edit the mappings so that the public FQDNs of the Expressway-E peers correspond to the IP addresses of their internal facing NICs.

   (You can check the public FQDNs in the certificate SAN fields, or by querying DNS)

7. Click **Save**.

   The mappings are saved and copied to the other cluster peers.

Note: The cluster is still formed using IP addresses and is still using the *Permissive* mode of TLS verification. The cluster will start using these mappings when you change the **Peer N address** fields to the public FQDNs and change the **TLS verification mode** to *Enforce*.

Change Cluster to Use FQDNs

This topic describes how to systematically change the peer addresses, replacing the IP addresses with FQDNs.

If you are changing an Expressway-E cluster to use FQDNs, then you will use the addresses that you entered in the mapping table (see Cluster Address Mapping for Cisco Expressway-E Clusters, page 19)

In this task, you change one peer's address at a time, across the whole cluster, before moving on to the next address.

Note: While you are changing a peer address, communications between peers are temporarily impacted and you will see alarms that persist until the changes are complete and the cluster agrees on the new addresses.

1. Sign in to all the cluster peers and navigate to **System > Clustering** on each.
2. Choose which peer address you are going to change first. We recommend starting at **Peer 1 address**, because you need to repeat the following process, one by one, for all peer addresses in the list.

3. On every peer in the cluster:
   a. Change the chosen peer address field from the IP address to the corresponding FQDN (if you did mappings, they should be replicated to all peers at this stage).
   b. Click **Save**.

   Caution: Make sure you only change one peer address on each box.
4. Switch to the peer that is identified by the peer address you are currently changing and restart this peer (go to **Maintenance > Restart options**, then click **Restart** and confirm **OK**).

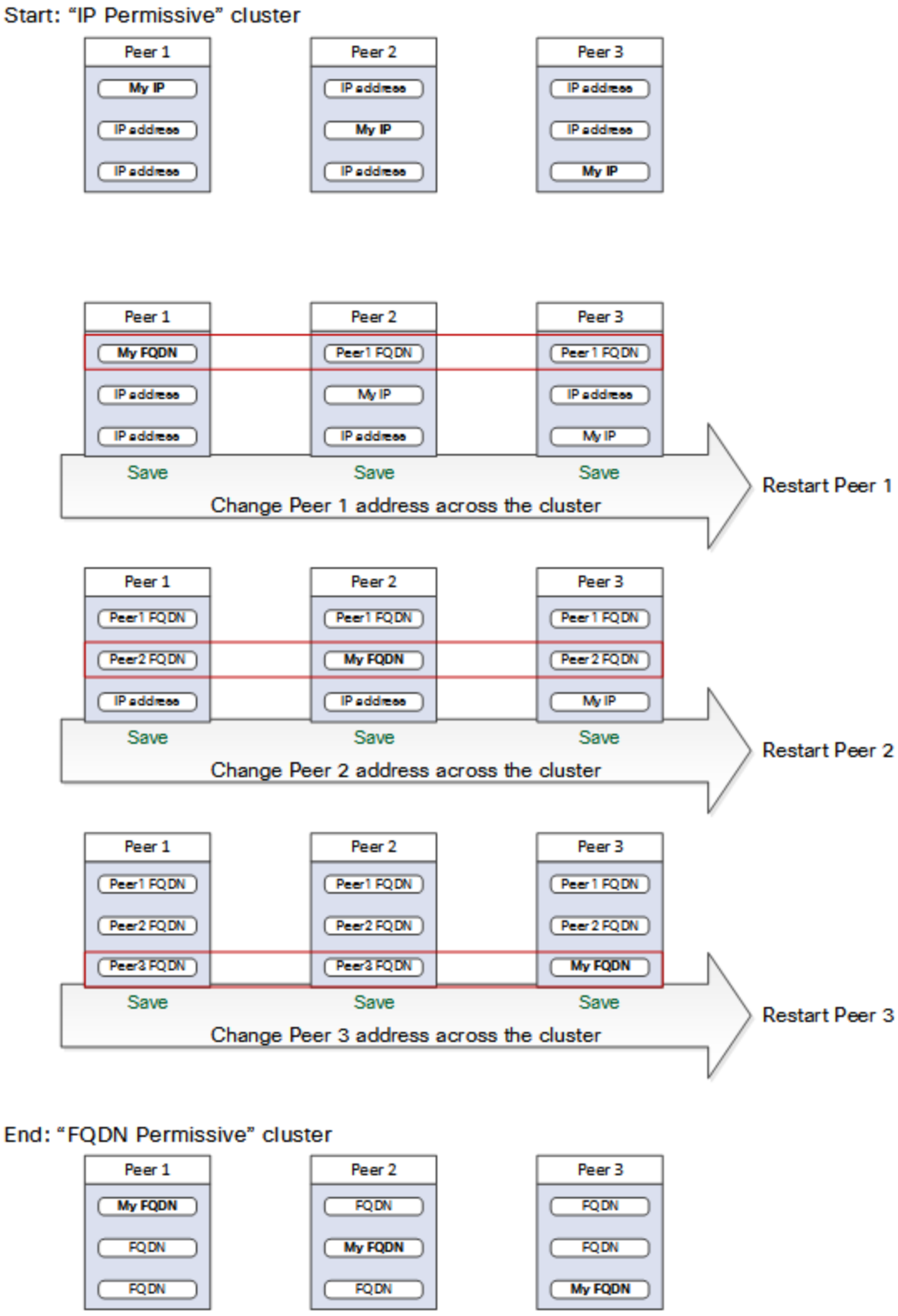
   Note: A single restart is needed when changing a peer address across all peers.
5. Wait for any transient clustering alarms to resolve.

   You've successfully changed this peer's clustering address, from an IP address to an FQDN, across the whole cluster.
6. Choose which peer address you are going to change next, and then repeat steps 3–5. Repeat this loop until you have changed all peer addresses and restarted all of the peers.

The whole cluster should now be operating on FQDNs, and the cluster is still in *Permissive* mode.

If the cluster is an Expressway-E cluster, and you are aiming to enforce TLS verification between the peers, then the peer address fields should match the identities presented in the certificates. Check that both the *Clustering* and *Certificate* status messages are green.

Figure 1 Worked example of a cluster of three peers



Enforce TLS Verification

Caution: Before you proceed, verify that your certificate SANs contain the FQDNs that are in the Peer N address fields. You should see green status messages for clustering and certificate next to each address field before you proceed.

1. On the primary peer, set **TLS verification mode** to *Enforce*.

   Caution: A warning will display if any certificates are invalid and will prevent the cluster working properly in enforced TLS verification mode.

   The new TLS verification mode replicates throughout the cluster.
2. Verify that **TLS verification mode** is now *Enforce* on each other peer.
3. Click **Save** and restart the primary peer.
4. Sign in to each other peer and then restart the peer.
5. Wait for the cluster to stabilize, and check that *Clustering* and *Certificate* status is green for all peers.

Change a Cluster

When your cluster is connected to other systems, any changes to the cluster could impact the integrated systems. When you change a cluster, remember to:

- Check other Expressways that are neighbors, clients, or servers of this cluster and update their zone configurations. For example, you need to update the peer address lists on neighbor zones towards this cluster when you add or remove peers from it.
- Check connections to other systems that integrate with the cluster. For example, Cisco Unified Communications Manager may have trunks to the cluster, or there may be auto-generated MRA zones that need to be refreshed on new cluster peers.
- Check that endpoints which register to the Expressway cluster are aware of new or removed peers, so that they register equally to the changed cluster's peers.
- Change the DNS entries for this cluster if you add or remove peers, or change IP addresses or FQDNs.
- If you use Expressway physical appliances:
  - To add a CE1200 appliance to an existing cluster that has CE1100 models in it, configure the Type option to match the other peers (Expressway-E or Expressway-C) through the service setup wizard on the **Status > Overview** page, *before* you add the CE1200 to the cluster.

    If you are adding a more recent model than existing appliances in the cluster, upgrade the Expressway software on the existing peers to the same version as the new appliance, *before* you create the backup to be later restored onto the new appliance. (A backup can only be restored onto the same software version that it was created on.)
- Re-export SAML metadata and copy it to the IDP. Whenever you add, remove, or replace a peer in a cluster of Expressway-Cs, you will change the SAML metadata of the cluster. If the cluster is configured for SSO of MRA-connected clients, then SSO will fail some of the time until you update the IDP with the cluster's new SAML metadata. This is because the (unique) serial numbers of the peers are used to generate the cluster's metadata. For details, see the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* on the Expressway configuration guides page.

Upgrade an X8.x Cluster to X8.11.4

This procedure describes how to upgrade an existing X8.x cluster to X8.11.4.

Before You Begin

- Choose a period of low activity to do the upgrade.
- Allocate sufficient time to upgrade all peers in the same upgrade "window". The cluster will not re-form correctly until the software versions match on all peers
- For each Expressway peer (including the primary), check the Alarms page (**Status > Alarms**) and make sure that all alarms are acted upon and cleared.
- Check the Release Notes for the new software version and **make sure that all upgrade prerequisites and software dependencies in the notes are in place before you start the upgrade**. Expressway release notes are here and VCS release notes are here.

Upgrade Expressway Cluster Peers to X8.11.4

Caution: To avoid the risk of configuration data being lost and to maintain service continuity, it is ESSENTIAL TO UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME IN SEQUENCE.

Starting with the primary peer, upgrade the cluster peers in sequence as follows:

1. Sign in to the peer as **admin** (on the web interface).
2. Backup the Expressway (**Maintenance > Backup and restore**).

   You must backup the system before you upgrade, in case you need to restore the configuration for any reason.

   Note: If the cluster peers are running different versions of the Expressway, do not make any configuration changes other than the settings required to upgrade. The cluster does not replicate any configuration changes to the subordinate peers that are running on different versions from the primary Expressway.
3. Enable maintenance mode (**Maintenance > Maintenance mode**).

   If maintenance mode is on, the peer will not process any incoming calls. Existing calls will be dropped only if you restart the peer. The other peers in the cluster will continue processing calls.
4. Wait for all calls to clear and registrations to expire on this peer.
   - If necessary, manually disconnect / terminate any calls on this peer that do not do so automatically. Go to **Status > Calls**, and then select the check box next to the calls you want to terminate and click **Disconnect**.
   - If necessary, also manually unregister devices registered to this peer that do not unregister automatically. Go to **Status > Registrations > By device**, and then select the check box next to the device you want to unregister and click **Unregister**.

   Note: 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. Upgrade and restart the peer (**Maintenance > Upgrade**).

   Ignore any cluster-related alarms and warnings that occur during the upgrade process. These are expected and will be resolved when all cluster peers are upgraded and after cluster data synchronization. The alarms will be resolved within 10 minutes of the complete upgrade. These are examples of some of the cluster-related alarms:

   - "Cluster communication failure": Occurs on the primary or any subordinate peers.
   - "Cluster replication error cannot find primary or this subordinate's peer configuration file, manual synchronization of configuration is required"

   The web interface may timeout during the restart process, when the progress bar reaches the end. This may occur if Expressway performs a disk file system check during the upgrade. The Expressway performs this check once every 30 restarts, or if the check was not performed in the last 6 months.
6. Repeat the previous steps for each peer in sequence, until all peers are on the new software version.

The software upgrade on the Expressway cluster is now complete.

Checks:

- On each Expressway (including the primary), go to **System > Clustering** and check that the cluster database status reports as **Active**.
- Check the configuration for items from the System, Configuration, and Application menus.
- If FindMe is in use, check that the expected FindMe entries still exist (**Status > Applications > TMS Provisioning Extension Services > FindMe > Accounts**).

Next steps:

- Backup the Expressway (**Maintenance > Backup and restore**).
- If you use theExpressway for Mobile and Remote Access (MRA) and you upgrade from X8.9n or earlier to X8.10 or later, after the system restarts you must reconfigure the MRA access control settings. See the Release Notes for more details.

Change TLS Version on Cluster Peers

1. Sign in as *admin* to one of the peers, through the web interface.
2. Go to **Maintenance > Security > Ciphers**, change the minimum TLS version of the service as required, and click **Save**.
3. Enable maintenance mode (**Maintenance > Maintenance mode**).
4. Wait for all calls to clear and registrations to expire on this peer.

   - If necessary, manually disconnect / terminate any calls on this peer that do not do so automatically. Go to **Status > Calls**, and then select the check box next to the calls you want to terminate and click **Disconnect**.
   - If necessary, also manually unregister devices registered to this peer that do not unregister automatically. Go to **Status > Registrations > By device**, and then select the check box next to the device you want to unregister and click **Unregister**.
5. Restart the peer.
6. Sign in to each peer in the cluster and repeat steps 3 to 5.

Checks:

Sign in to each peer, go to **Maintenance > Security > Ciphers**, and verify that the minimum TLS version of the service is changed.

Remove a Live Peer From a Cluster (Permanently)

This process removes one Expressway peer from an existing cluster.

- If you are disbanding the whole cluster, see Disband a Cluster, page 32 instead.
- If you want to remove the primary peer, make a different peer the primary before you remove this one. See Change the Primary Peer, page 33
- If you cannot access the peer you want to remove, see Remove a Dead Peer From a Cluster (Permanently), page 30.

On the Expressway that you are removing from the cluster:

1. Go to **System > Clustering**:
2. Delete all entries in the **Peer *N* address** fields.
3. Click **Save**.

   CAUTION: If you clear all the peer address fields from the clustering page and save the configuration, then the Expressway will factory reset itself the next time you do a restart. This means you will lose all existing configuration except basic networking for the LAN1 interface, including all configuration that you do between when you clear the fields and the next restart.

   If you need to avoid the factory reset, restore the clustering peer address fields as they were. Replace the original peer addresses in the same order, and then save the configuration to clear the banner.
4. Restart the Expressway (go to **Maintenance > Restart options**, then click **Restart** and confirm **OK**).
   The peer initiates a factory reset when you do the restart. It comes back up with all configuration removed, except:

   The factory reset is automatically triggered when the peer restarts, to remove sensitive data and clustering configuration. The reset clears all configuration except the following basic networking information, which is preserved for the LAN1 interface so that you can still access the Expressway. If you use the **dual-NIC option, be aware that any LAN2 configuration is removed completely by the reset**.

   - IP addresses preserved
   - Server certificate, associated private key, and CA trust store preserved
   - Admin and root accounts and passwords preserved
   - SSH keys preserved
   - Option keys preserved
   - HTTPS access enabled
   - SSH access enabled

On the primary Expressway:

1. Go to **System > Clustering**.
2. Delete the address of the Expressway that has been removed.
3. If the Expressway being removed is not the last field in the list, move any other addresses up the list so that there are no empty fields between entries.
4. If the primary Expressway peer's address has been moved up the list in the previous step, alter the **Configuration primary** value to match its new location.
5. Click **Save**.

On all the remaining subordinate Expressway peers:

1. Go to **System > Clustering**.
2. Edit the **Peer *N* address** and **Configuration primary** fields so that they are identical to those configured on the primary Expressway.
3. Click **Save**.
4. Repeat for all remaining subordinate Expressway peers until they all have identical clustering configuration.

You have finished removing a live Expressway from the cluster.

Remove a Dead Peer From a Cluster (Permanently)

This procedure removes an out-of-service peer from a cluster if it needs to be RMAd, or cannot be accessed for some other reason.

- If you are disbanding the whole cluster, see Disband a Cluster, page 32 instead.
- If you can access the peer you want to remove, see Remove a Live Peer From a Cluster (Permanently), page 28.
- If you want to remove the primary peer, make a different peer the primary before you remove this one. See Change the Primary Peer, page 33

Note: This procedure does not clear configuration from the Expressway. If you manage to revive the system, you must not start using it until you have reset its default configuration (factory reset).

On the primary Expressway:

1. Go to **System > Clustering**.
2. Delete the address of the Expressway that has been removed.
3. If the Expressway being removed is not the last field in the list, move any other addresses up the list so that there are no empty fields between entries.
4. If the primary Expressway peer's address has been moved up the list in the previous step, alter the **Configuration primary** value to match its new location.
5. Click **Save**.

On all the remaining subordinate Expressway peers:

1. Go to **System > Clustering**.
2. Edit the **Peer *N* address** and **Configuration primary** fields so that they are identical to those configured on the primary Expressway.
3. Click **Save**.
4. Repeat for all remaining subordinate Expressway peers until they all have identical clustering configuration.

You have removed the inaccessible peer from the Expressway cluster.

Clear Configuration From This Peer

If you ever recover the peer that you removed, you must clear its configuration before you reconnect it to the network:

1. Go to **System > Clustering**:
2. Delete all entries in the **Peer *N* address** fields.
3. Click **Save**.

4. Restart the Expressway (go to **Maintenance > Restart options**, then click **Restart** and confirm **OK**).
   The Expressway initiates a factory reset when you do the restart. It comes back up with all configuration removed, except:

   The factory reset is automatically triggered when the peer restarts, to remove sensitive data and clustering configuration. The reset clears all configuration except the following basic networking information, which is preserved for the LAN1 interface so that you can still access the Expressway. If you use the **dual-NIC option, be aware that any LAN2 configuration is removed completely by the reset**.

   - IP addresses preserved
   - Server certificate, associated private key, and CA trust store preserved
   - Admin and root accounts and passwords preserved
   - SSH keys preserved
   - Option keys preserved
   - HTTPS access enabled
   - SSH access enabled

Now you can bring it back into the cluster, see Add a Peer to a Cluster, page 18

Disband a Cluster

This process removes all Expressway 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 Expressway will retain enough configuration to enable you to access the web interface, but all other configuration is cleared.

The procedure involves removing peers one by one, and finally clearing the clustering configuration from the primary peer. In X8.11 and later, clearing the clustering configuration prepares the Expressway for a factory reset. You must be certain you want to factory reset the primary, because there are some situations where you need to have Expressway configured as a 'cluster of one'.

To disband the cluster:

1. Remove any peers that you cannot access. See Remove a Dead Peer From a Cluster (Permanently), page 30.
2. If you're using Cisco TMSPE, sign in to Cisco TMS and stop provisioning to the cluster:
   a. Select **Systems > Navigator** (and any required sub folders), then click on any Expressway in the cluster.
   b. Select the **Provisioning** tab.
   c. Disable all 4 services (clear checkboxes).
   d. Click **Save**.
3. Remove each of the subordinate peers turn. See Remove a Live Peer From a Cluster (Permanently), page 28.

   When you remove the last subordinate peer, you should only have the primary peer remaining in the cluster.

   The cluster is now a 'cluster of one' and you can stop here if you want to retain this Expressway with its configuration.
4. If you want to factory reset the primary peer, sign in to it and follow the process to Remove a Live Peer From a Cluster (Permanently), page 28.

You've finished disbanding the cluster.

Change the Primary Peer

You can do this process even if the current primary peer is not accessible. Make sure you follow the steps in the order listed here, to avoid putting the cluster in a state where multiple peers are contending to be the primary.

On the "new" primary Expressway:

1. Go to **System > Clustering**.
2. From the **Configuration primary** drop-down menu select the ID number of the peer entry that says 'This system'.
3. Click **Save**.

   While changing the primary peer, ignore any alarms on Expressway that report 'Cluster primary mismatch' or 'Cluster replication error' – they will be rectified as part of this procedure.

On all other Expressway peers, starting with the "old" primary peer (if it is still accessible):

1. Go to **System > Clustering**.
2. From the **Configuration primary** drop-down menu select the ID number of the "new" primary Expressway.
3. Click **Save**.

Check all peers:

Note that any alarms raised on the Expressway peers that relate to 'Cluster primary mismatch' and 'Cluster replication error' should clear automatically after approximately 2 minutes.

1. Confirm that the change to the **Configuration primary** has been accepted by going to **System > Clustering** and refreshing the page.
2. If any Expressways have not accepted the change, repeat the steps above.
3. Check that the cluster database status reports as Active.

Cisco TMS:

No changes are required; Cisco TMS will see the primary change on the Expressway cluster and report this appropriately.

If the old primary is not available:

If you are changing the primary peer because the "old" primary is not accessible, see Remove a Dead Peer From a Cluster (Permanently), page 30 procedure.

If there is any chance of reviving the "old" primary, you must isolate it from the other peers and factory reset it if possible.

You have changed the primary peer of the cluster.

Change the Address of a Peer

To change the address of an Expressway peer you must remove the Expressway from the cluster, change its address, and then add the Expressway back into the cluster.

The process is as follows:

1. Ensure that the Expressway whose address you want to change is not the primary Expressway.

   If it is the primary Expressway, follow the steps in Change the Primary Peer, page 33 to make a different peer the primary.
2. Carry out the process documented in Remove a Live Peer From a Cluster (Permanently), page 28.
3. Change the address of the Expressway.
4. Carry out the process documented in Add a Peer to a Cluster, page 18.

Replace a Peer

This section summarizes the procedure for replacing a cluster peer Expressway with a different unit.

1. Ensure that the Expressway to be replaced is not the primary Expressway.

   If it is the primary Expressway, follow the steps in Change the Primary Peer, page 33 to make a different peer the primary.
2. Remove the existing peer from the cluster:
   a. If the cluster peer to be replaced is not accessible, use the procedure defined in Remove a Dead Peer From a Cluster (Permanently), page 30
   b. If the cluster peer to be replaced is accessible, use the procedure defined in Remove a Live Peer From a Cluster (Permanently), page 28
3. Add the replacement peer to the cluster using the procedure defined in Add a Peer to a Cluster, page 18

IMPORTANT: additional information if you have clusters with physical appliances

To add a CE1200 appliance to an existing cluster that has CE1100 models in it, configure the Type option to match the other peers (Expressway-E or Expressway-C) through the service setup wizard on the **Status > Overview** page, *before* you add the CE1200 to the cluster.

If you are adding a more recent model than existing appliances in the cluster, upgrade the Expressway software on the existing peers to the same version as the new appliance, *before* you create the backup to be later restored onto the new appliance. (A backup can only be restored onto the same software version that it was created on.)

Replace a Peer and Migrate its Configuration

This procedure assumes that you are replacing an accessible Expressway peer with a different Expressway.

1. Ensure that the Expressway to be replaced is not the primary Expressway.

   If it is the primary Expressway, follow the steps in Change the Primary Peer, page 33 to make a different peer the primary.
2. **Remove the peer by deleting its clustering configuration, but do not restart it yet**. See Remove a Live Peer From a Cluster (Permanently), page 28
3. Backup the configuration of the removed peer before you restart it.
4. Generate and apply option keys for the new Expressway. You must apply the same set of keys that are applied to the other peers.
5. Restore the backup from the removed peer onto the new Expressway.
6. Check the DNS configuration of the new Expressway is the same as the other peers, and synchronize it with the same NTP servers.
7. Add the replacement peer to the cluster using the procedure defined in Add a Peer to a Cluster, page 18.

   You should use the new peer's address in place of the removed peer's address when following that procedure.

   The most important steps are summarized here:

   a. Add the new peer's address to the clustering configuration on the primary, in place of the old peer's address.
   b. Add the new peer's address to the clustering configuration on other existing peers, in place of the old peer's address.
   c. Enter the new clustering configuration on the new peer (cluster name, shared secret, ordered peer list).
8. Restart the new peer.
9. Wait for approximately five minutes, then check the cluster status and resolve any alarms.
10. Restart the removed peer to initiate a factory reset and clear the old configuration.

Connect the Expressway Cluster to Other Systems

Neighboring Between Expressway Clusters

You can neighbor your local Expressway (or Expressway cluster) to a remote Expressway cluster; this remote cluster could be a neighbor, traversal client, or traversal server to your local Expressway. In this case, when a call is received on your local Expressway and is passed via the relevant zone to the remote cluster, it will be routed to whichever peer in that neighboring cluster has the lowest resource usage. That peer will then forward the call as appropriate to one of its:

- locally registered endpoints (if the endpoint is registered to that peer)
- peers (if the endpoint is registered to another peer in that cluster)
- external zones (if the endpoint has been located elsewhere)

For Expressway: Lowest resource usage is determined by comparing the number of available media sessions (maximum – current use) on the peers, and choosing the peer with the highest number. Peers that are in maintenance mode are not considered.

For VCS: Lowest resource usage is determined by comparing the number of available traversal calls (maximum – current use) on the peers, and choosing the peer with the highest number. Peers that are in maintenance mode are not considered.

When configuring a connection to a remote cluster, you create a single zone and configure it with details of all the peers in the cluster. Adding this information to the zone ensures that the call is passed to that cluster regardless of the status of the individual peers.

You also need to enter the address of all peers in the remote cluster when the connection is via a **neighbor** or **traversal client** zone. You do not do this for **traversal server** zones, as these connections are not configured by specifying the remote system's address.

Note: Systems that are configured as peers must **not** also be configured as neighbors to each other, and vice versa.

Neighboring your clusters

To neighbor your local Expressway (or Expressway cluster) to a remote Expressway cluster, you create a single zone to represent the cluster and configure it with the details of all the peers in that cluster:

1. On your local Expressway (or, if the local Expressway is a cluster, on the primary peer), create a zone of the appropriate type. This zone will represent the connection to the cluster.
2. In the **Location** section, enter the IP address or FQDN of each peer in the remote cluster in the **Peer 1** to **Peer 6** address fields.

Note that:

- Ideally you should use FQDNs in these fields. Each FQDN must be different and must resolve to a single IP address for each peer. With IP addresses, you may not be able to use TLS verification, because many CAs will not supply certificates to authenticate an IP address.
- The order in which the peers in the remote Expressway cluster are listed here does not matter.
- Whenever you add an extra Expressway to a cluster (to increase capacity or improve redundancy, for example) you will need to modify any Expressways which neighbor to that cluster to let them know about the new cluster peer.

Configure Endpoints to Work With a Cluster

When configuring endpoints it is desirable for them to know about all the Expressway peers in a cluster. So that at initial registration or later, if endpoints lose connection to their Expressway peer, they are able to register with another peer in the cluster. This section describes the available configuration methods, listed in preferred order.

For more details about DNS SRV and round-robin DNS, see the URI dialing section in the *Expressway Administrator Guide* and Cluster Name and DNS SRV Records, page 50.

Note: SIP and H.323 endpoints behave differently.

SIP Endpoints

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

Option 1 – SIP Outbound (preferred)

IMPORTANT: For endpoints running Cisco Collaboration Endpoint software, this option is not supported from version CE8.0.

SIP outbound allows an endpoint to be configured to register to two or more Expressway peers simultaneously. The benefit of this is that if the connection between one peer and the endpoint breaks, 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.

Important: Registering a device using SIP Outbound with multiple Cisco Expressways consumes room licenses per registration, not per device. For example, two room licenses are consumed if a device is registered with two Cisco Expressways.

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

- Proxy 1
  - Server discovery = Manual
  - Server Address =

    DNS name of cluster peer or
    IP address of cluster peer
- Proxy 2
  - Server discovery = Manual
  - Server Address =

    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 Expressway 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 Expressway 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.

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 is repeated until the endpoint can register with a Expressway.

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

To minimize DNS traffic, the DNS SRV cache timeout should be set to a fairly long time, such as 24 hours.

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 Expressway 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 Expressway 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 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 Expressway peer that it is given. (The DNS server will have supplied the next cluster peer's IP address.) This is repeated until the endpoint can register with a Expressway.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection to its Expressway it will perform another DNS lookup to find a new Expressway to register to (the DNS server providing a Expressway 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 Expressway is not accessible the endpoint is quickly pointed at a different Expressway.

Option 4 – Static IP (least preferred)

Use this option if the Expressway 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 Expressway peer

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

The endpoint will continue to use the first Expressway 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 Expressway until it is accessible again.

H.323 Endpoints

The options are listed in preference order for providing resilience of connectivity of endpoints to a cluster of Expressways where 1 or more Expressway 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 Expressway 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 Expressway 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.

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 Expressway. On registering with the Expressway, the Expressway will respond with the H.323 "Alternate Gatekeepers" list containing the list of Expressway cluster peer members.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection to its Expressway 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 Expressway 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 Expressway 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 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 Expressway 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 Expressway. On registering with the Expressway, the Expressway will respond with the H.323 'Alternate Gatekeepers' list containing the list of Expressway cluster peer members.

The endpoint will continue to use the first Expressway 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 Expressway at startup, the endpoint is quickly pointed at a different Expressway.

Option 3 – Static IP (least preferred)

Use this option if the Expressway 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 Expressway peer

On startup the endpoint will try and register with the Expressway 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 Expressway. On registering with the Expressway, the Expressway will respond with the H.323 "Alternate Gatekeepers" list containing the list of Expressway cluster peer members.

The endpoint will continue to use the first Expressway 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.

Add the Expressway to Cisco TMS

For more detail about Cisco TMS administration, see *Cisco TelePresence Management Suite Administrator Guide*, for your version, at Cisco TelePresence Management Suite (TMS Maintain and Operate Guides page)

On the Expressway:

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

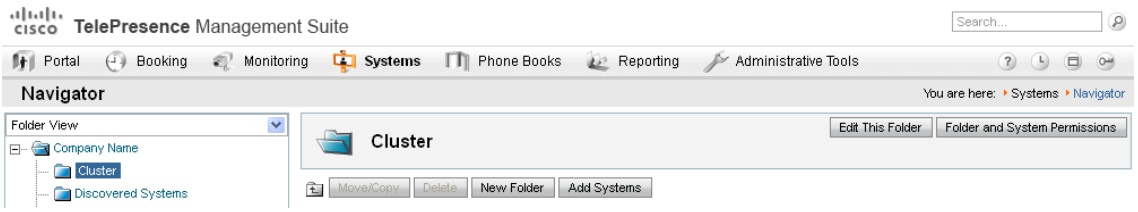
   (If SNMP was previously disabled, an alarm may appear indicating the need for a restart. If so, restart the system via **Maintenance > Restart options**.)
2. Go to **System > External manager** and ensure that:
   a. **Address** is set to the IP address or FQDN of Cisco TMS.
   b. **Path** is set to *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'.

      (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** of 'Active' or 'Initialising'.[1]

On Cisco TMS:

1. Select **Systems > Navigator**.
2. Select (or create) an appropriate folder in which to put the Expressway (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 Expressway.
5. Click **Next**.
6. Look for ✓System added.

   Note: When you add an Expressway to TMS, the TMS UI shows it as a VCS . This is a known issue.
7. Click **Finish Adding Systems**, **Add System despite warnings** or **Add More Systems** as appropriate.

On Expressway:

Go to **System > External manager** and check that the **State** now shows Active.

[1]Cisco TMS may force the protocol to be HTTPS. The configuration for this is found in **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*.

Troubleshooting

Restarting Sequence

Whenever you have formed, connected, upgraded, or changed a cluster, you should check whether any peers need restarting. Sometimes you will need to restart only one peer, typically if you've made a peer-specific configuration change.

When you're working with the cluster configuration, you sometimes need to restart more than one peer. In this case, you should always restart in the following sequence:

1. Restart the primary peer, and wait for it to be accessible via web interface.
2. Check cluster replication status on the primary and status of all peers. Wait a few minutes, refreshing the peer's web interfaces occasionally.
3. Restart other peers, if required, one at a time. Each time, wait a few minutes after it is accessible and check its replication status.

Check Replication Status

You may need to wait about 5 minutes after making clustering changes before the Expressway peers report successful status.

1. Go to **System > Clustering** on each peer and check that the cluster database status reports as Active.

   If there is a failure status, refresh the browser first. If the status is still not Active, check the alarms.

Force Refresh in Cisco TMS

If you're using Cisco TMS, check that Cisco TMS has all the correct settings for the cluster by forcing a refresh as follows:

1. On Cisco TMS, go to **Systems > Navigator**
2. Find and click on the name of the Expressway.
3. Select the **Settings** tab.
4. Click **Force Refresh**.
5. Repeat for all Expressway peers in the cluster (including the primary Expressway).

Expressway Alarms and Warnings

"Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined"

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

The **Cluster name** should be the routable Fully Qualified Domain Name used in SRV records that address this Expressway cluster, for example "cluster1.example.com". (See Cluster Name and DNS SRV Records, page 50).

"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 primary or this subordinate's peer configuration file, manual synchronization of configuration is required"

- "Cluster replication error: configuration primary ID is inconsistent, manual synchronization of configuration is required"
- "Cluster replication error: this peer's configuration conflicts with the primary's configuration, manual synchronization of configuration is required"

If a subordinate Expressway reports an alarm: "Cluster replication error – <details> synchronization of configuration"

On that subordinate Expressway:

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

   ```
   xcommand ForceConfigUpdate
   ```

   This will delete the subordinate Expressway configuration and then force it to update its configuration from the primary Expressway.

   Caution: Only use this command if the configuration on the primary Expressway is known to be in a good state. We recommend that you take a backup before running this command.

Cluster replication error persists after ForceConfigUpdate

In X8.11 we introduced a unique encryption key per cluster peer. Also, in some upgrade cases, for example, if peers are upgraded in the wrong order, subordinate peers may not synchronize with the primary. These two issues compound each other, allowing peers to be in a state where they cannot decrypt the configuration from the primary.

The symptom of this is that the Cluster replication alarm persists after you tried `xcommand forceconfigupdate` on a subordinate peer. This is probably after a recent upgrade to X8.11 on the primary peer.

You can avoid the problem by always upgrading the primary first, but if you have got this persistent error, you can resolve it as follows:

1. Sign in to the primary peer and check that it is in a good state.
2. Ensure that the clustering configuration shows this peer to be the primary.
3. Upgrade the primary again, using the same package that you originally used to upgrade.

The replication alarm clears after the primary peer has upgraded and rebooted. This normally happens within ten minutes after reboot, but could be up to twenty minutes after reboot.

"Cluster replication error: the NTP server is unreachable"

Configure an accessible NTP server on the Expressway **System > Time** page.

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

Check and correct the list of peers for this Expressway on the primary Expressway, and copy to all other Expressway peers (**System > 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 **Configuration > Protocols > H.323**).

"Expressway database failure: Please contact your Cisco support representative"

The support representative will help you work through the following steps:

1. Take a system snapshot and provide it to your support representative.
2. Remove the Expressway from the cluster using: Remove a Live Peer From a Cluster (Permanently), page 28.
3. Restore that Expressway's database by restoring a backup taken on that Expressway previously.
4. Add the Expressway back to the cluster using Add a Peer to a Cluster, page 18.

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

1. Take a system snapshot and provide it to TAC.
2. Remove the Expressway from the cluster using: Remove a Live Peer From a Cluster (Permanently), page 28.
3. Log in as root and run `clusterdb_destroy_and_purge_data.sh`
4. Restore that Expressway's database by restoring a backup taken on that Expressway previously.
5. Add the Expressway back to the cluster using Add a Peer to a Cluster, page 18.

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

Cisco TMS Warnings

Cisco TMS Cluster Diagnostics

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

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

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

for each of the Expressway 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 Impact of Clustering on Other Expressway Applications, page 56.

Expressway'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 Expressway uses HTTPS for feedback. If enabled, Cisco TMS will (on a time period defined by Cisco TMS) re-configure the Expressway's **System > External manager Protocol** to *HTTPS*.

If HTTPS must be used for Expressway to supply feedback to Cisco TMS, see Add the Expressway to Cisco TMS, page 41 for information about how to set up certificates.

Cisco TMS will force HTTPS on Expressway if:

- **TMS Services > Enforce Management Settings on Systems** = *On* (**Administrative Tools > Configuration > Network Settings**)
  and

- **Secure-Only Device Communication > Secure-Only Device Communication** = *On* (**Administrative Tools > Configuration > Network Settings**)

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 Expressway to provide feedback to Cisco TMS using HTTPS (if HTTP is sufficient).

Reference

Peer-Specific Items

Most items of configuration are applied via the primary peer to all peers in a cluster. However, the following items (marked with a † on the web interface) must be specified separately on each cluster peer.

Note: You should not modify configuration data that applies to all peers on any peer other than the primary peer. At best it will result in the changes being overwritten from the primary; at worst it will cause cluster replication to fail.

Cluster configuration (System > Clustering)

The list of **Peer *N* address**es (including the peer's own address) that make up the cluster has to be specified on each peer and they must be identical on each peer.

The **Cluster name**, **Configuration primary**, and **Cluster IP version** must be specified on each peer and must be identical for all peers.

Note: If you need to enable cluster address mapping, we recommend forming the cluster on IP addresses first. Then you will only need to add the mappings on one peer.

Ethernet speed (System > Network interfaces > Ethernet)

The **Ethernet speed** is specific to each peer. Each peer may have slightly different requirements for the connection to their Ethernet switch.

IP configuration (System > Network interfaces > IP)

LAN configuration is specific to each peer.

- Each peer must have a unique IP address, whether that is an **IPv4 address**, an **IPv6 address**, or both.
- **IP gateway** configuration is peer-specific. Each peer can use a different gateway.

Note that the IP protocol is applied to all peers, because each peer must support the same protocols.

IP static routes (System > Network interfaces > Static routes)

Any static routes you add are peer-specific and you may create different routes on different peers if required. If you want all peers in the cluster to be able to use the same static route, you must create the route on each peer.

System name (System > Administration)

The **System name** must be different for each peer in the cluster.

DNS servers and DNS host name (System > DNS)

DNS servers are specific to each peer. Each peer can use a different set of DNS servers.

The **System host name** and **Domain name** are specific to each peer.

NTP servers and time zone (System > Time)

The **NTP servers** are specific to each peer. Each peer may use one or more different NTP servers.

The **Time zone** is specific to each peer. Each peer may have a different local time.

SNMP (System > SNMP)

SNMP settings are specific to each peer. They can be different for each peer.

Logging (Maintenance > Logging)

The Event Log and Configuration Log on each peer only report activity for that particular Expressway. The **Log level** and the list of **Remote syslog servers** are specific to each peer. We recommend that you set up a remote syslog server to which the logs of all peers can be sent. This allows you to have a global view of activity across all peers in the cluster.

Security certificates (Maintenance > Security)

The trusted CA certificate, server certificate and certificate revocation lists (CRLs) used by the Expressway must be uploaded individually per peer.

Administration access (System > Administration)

The following system administration access settings are specific to each peer:

- Serial port / console
- SSH service
- Web interface (over HTTPS)
- Redirect HTTP requests to HTTPS
- Automated protection service

Option keys (Maintenance > Option keys)

Option keys that control features are specific to the peer where they are applied. Option keys that control licenses are pooled for use by the whole cluster.

Each peer must have an identical set of feature option keys installed, which means you must purchase a key for each peer in the cluster.

License option keys can be applied to one or more peers in the cluster, and the sum of the installed licenses is available across the cluster. This license pooling behavior includes the following option keys:

- Expressway: Rich media sessions
- Expressway: Telepresence room systems
- Expressway: Desktop systems
- VCS: Traversal calls
- VCS: Non-traversal calls

Note: In some cases a peer will raise an alarm that it has no key to enable licenses the peer needs, even though there are licenses available in the cluster. You can acknowledge and ignore this category of alarm, unless the only peer that has the required licenses is out of service.

Active Directory Service (Configuration > Authentication > Devices > Active Directory Service)

When configuring the connection to an Active Directory Service for device authentication, the **NetBIOS machine name (override)**, and domain administrator **Username** and **Password** are specific to each peer.

Conference Factory template (Applications > Conference Factory)

The template used by the Conference Factory application to route calls to a conferencing server must be unique for each peer in the cluster.

Sample Firewall Rules for Protecting Intracluster TLS Ports

To protect your cluster peers against denial-of-service attacks, we encourage you to use the Expressway's in-built firewall rules to filter all TCP access to the clustering ports.

On each peer:

1. Go to **System > Protection > Firewall rules > Configuration**.
2. Add a rule to drop TCP connections to ports 4371 and 4372, for all IP addresses in the appropriate (IPv4 or IPv6) range.

3. Add lower priority rules, one for each of the other peers' IP addresses, that allow TCP connections to those ports.

   (Lower numbered rules are implemented before higher numbered rules.)

4. Activate the firewall rules.

Figure 2 Creating a custom rule to allow a specific peer to connect to this peer's clustering ports

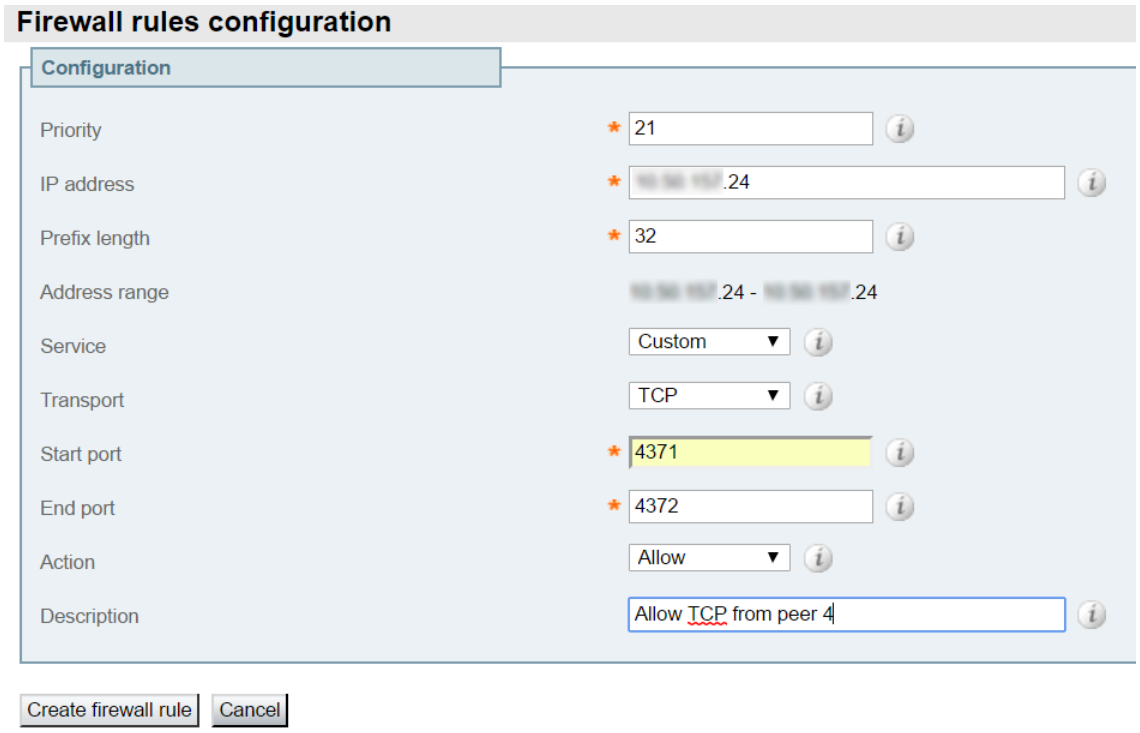
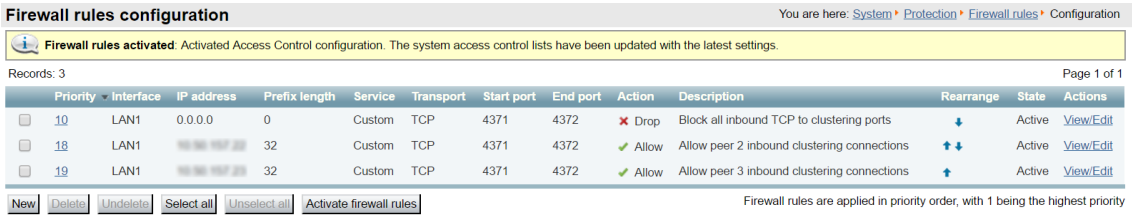


Figure 3 Example list of rules, showing recommended priority order



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. HTTP, 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.
- As 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 inaccessible) 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 inaccessible.)

The generic format of a DNS SRV query is:

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

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.

Further details on DNS SRV can be found in *Expressway Administrator Guide* and *RFC 2782*.

DNS SRV Configuration for Mobile and Remote Access

This section summarizes the public (external) and local (internal) DNS requirements. For more information, see the *Cisco Jabber Planning Guide* (for your version) on the Jabber Install and Upgrade Guides page.

Public DNS

The public (external) DNS must be configured with `_collab-edge._tls.<domain>` SRV records so that endpoints can discover the Expressway-Es to use for Mobile and Remote Access. SIP service records are also required (for general deployment, not specifically for Mobile and Remote Access). For example, for a cluster of 2 Expressway-E systems:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	collab-edge	tls	10	10	8443	expe1.example.com
example.com	collab-edge	tls	10	10	8443	expe2.example.com
example.com	sips	tcp	10	10	5061	vcse1.example.com
example.com	sips	tcp	10	10	5061	vcse2.example.com

Local DNS

The local (internal) DNS requires `_cisco-uds._tcp.<domain>` SRV records. For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	cisco-uds	tcp	10	10	8443	cucmserver1.example.com
example.com	cisco-uds	tcp	10	10	8443	cucmserver2.example.com

Notes:

- **Important! From version X8.8 onward, you must create forward and reverse DNS entries for all Expressway-E systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates.**
- Ensure that the `cisco-uds` SRV records are NOT resolvable outside of the internal network, otherwise the Jabber client will not start Mobile and Remote Access negotiation via the Expressway-E.
- You must create internal DNS records, for both forward and reverse lookups, for all Unified Communications nodes used with Mobile and Remote Access. This allows Expressway-C to find the nodes when IP addresses or hostnames are used instead of FQDNs.

DNS SRV Configuration for Video Conferencing

The format of DNS SRV queries for sip (RFC 3263) and H.323 used by Expressway 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 location (RAS) signaling, such as 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 location (RAS) signaling, such as LRQ
- _h323cs._tcp.<fully.qualified.domain> – for H.323 call signaling
- _h323rs._udp.<fully.qualified.domain> – for H.323 registrations

UDP is not a recommended transport medium for video signaling; SIP messaging for video system is too large to be reliably carried on datagram-based (rather than stream-based) transports.

The Expressway **Cluster name** (configured on the **System > Clustering** page) should be an FQDN, where the domain part is the domain used for the SRV records which point to that Expressway cluster.

Example

DNS SRV records for 2 peers of an Expressway-E cluster for example.com

where:

- FQDN of Expressway-E peer 1: expe1.example.com
- FQDN of Expressway-E peer 2: expe2.example.com
- FQDN of Expressway-E cluster: cluster.example.com

```
_sips._tcp.example.com. 86400 IN SRV 1 1 5061 expe1.example.com.
_sips._tcp.example.com. 86400 IN SRV 1 1 5061 expe2.example.com.

_sip._tcp.example.com. 86400 IN SRV 1 1 5060 expe1.example.com.
_sip._tcp.example.com. 86400 IN SRV 1 1 5060 expe2.example.com.

_h323ls._udp.example.com. 86400 IN SRV 1 1 1719 expe1.example.com.
_h323ls._udp.example.com. 86400 IN SRV 1 1 1719 expe2.example.com.

_h323cs._tcp.example.com. 86400 IN SRV 1 1 1720 expe1.example.com.
_h323cs._tcp.example.com. 86400 IN SRV 1 1 1720 expe2.example.com.
```

```
_h323rs._udp.example.com. 86400 IN SRV 1 1 1719 expe1.example.com.
_h323rs._udp.example.com. 86400 IN SRV 1 1 1719 expe2.example.com.
```

Notes:

- 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 peers should have one value and the other (secondary) cluster peers should have a larger value.
- Weights should be the same – so that there is equal use of each peer.

Checking DNS SRV Settings

Check DNS SRV connectivity from Expressway

1. Go to **Maintenance > Tools > Network utilities > Connectivity Test**
2. Enter a **Service Record Domain** you want to query, for example, `call.ciscospark.com`.
3. Enter the **Service Record Protocols** you want to test, for example, `_sips._tcp`.

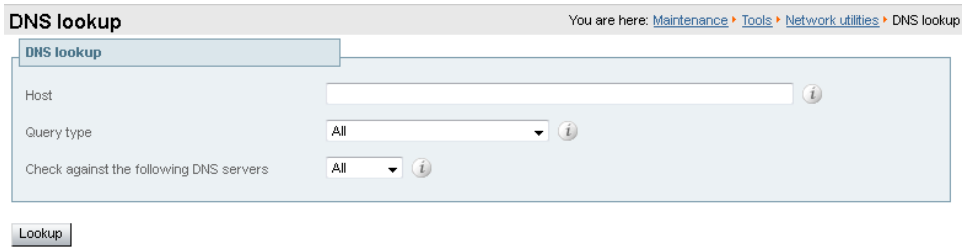
   Use commas to delimit multiple protocols, for example, `_sip._tcp,_sips._tcp`.
4. Click **Run**.

   The Expressway queries DNS for SRV records comprised of the service, protocol and domain combinations, for example: `_sip._tcp.call.ciscospark.com` and `_sips._tcp.call.ciscospark.com`.

   By default the system will submit the query to all of the system's default DNS servers (**System > DNS**).

Use DNS lookup tool on Expressway

1. Go to **Maintenance > Tools > Network utilities > DNS lookup**.
2. Enter the SRV path in the **Host** field.
3. Click **Lookup**.



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 expe1.example.com.
```

```
_sip._tcp.example.com. 1183     IN      SRV     1 0 5060 expe2.example.com.

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

;; ADDITIONAL SECTION:
expe1.example.com.      1536     IN      A       194.73.59.53
expe2.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

~ #
```

Clusters in Isolated Networks

Note: The background information in this appendix is valid, but the issue and workaround described have been invalidated by a fix in X8.9.2. That fix allows privately mapping peer FQDNs to peer IP addresses, instead of using the IP addresses returned by DNS lookup.

As of X8.8, Expressway peers use TLS to communicate with each other. You have the option of permissive TLS – the certificates are not verified – or enforced TLS where the certificates are verified.

In the latter case, each peer will need to DNS look up the common name (CN), and perhaps also subject alternate names (SANs), that they read from their peers' certificates. They compare the returned IP addresses against the IP addresses that gave them the certificates and if they match, the connection is authenticated.

In isolated networks, the peers will not typically be able to reach the internal DNS servers, because that would require unsolicited inbound requests. In a dual-NIC setup, you probably also don't want to put the peers' private IP addresses into the public DNS.

The issue is compounded by not being able to use IP addresses as common names or subject alternate names on server certificates: certificate authorities do not advocate this and probably will not issue such certificates.

Expressway-E peers have dual NICs, with no static NAT

You can enforce TLS between cluster peers:

1. Enter public DNS servers on the DNS configuration of each peer.
2. Choose which of the LAN interfaces will take the public facing address.
3. Configure the public DNS to resolve each peer's FQDN to its public IP address.
4. Populate the CN of all peer certificates with the same cluster FQDN, and populating each peer certificate's SAN with that peer's FQDN.
5. Enter the cluster FQDN and peer FQDNs on the clustering configuration page and set the **TLS verification mode** to *Enforce*.

The peers will now use the public DNS to verify each others' identities, as presented on their certificates.

Expressway-E peers have dual NICs, with static NAT enabled

In addition to its private IP address in the isolated network, you can give one of the NICs a public IP address that translates to its private address. In this case, you cannot use FQDNs to form the cluster.

This is because the public DNS record for each peer's FQDN would match its translated (public) IP address, but the peers would see each other's private addresses when swapping certificates. The mismatch between IP addresses would prevent the TLS connection being established, and the cluster would not form.

To form the cluster:

1. Enter public DNS servers on the DNS configuration of each peer.
2. Choose which of the LAN interfaces on each peer will have static NAT enabled.
3. Enter the private IP addresses of the other LAN interfaces on the clustering configuration pages, and set the TLS mode to Permissive.

The peers will now use the private IP addresses to form the cluster, but will not check the contents of the certificates against the DNS records.

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 *ENUM Dialing on Expressway Deployment Guide*).

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 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" "!^.*$!bob@example.com!" .
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+h323" "!^.*$!bob@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
```

Looking up a domain NAPTR record

Example: NAPTR record allowing endpoints to detect that they are in the public (external) network. The flag "s" is extended to "se" to indicate that it is "external".

```
~ # 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
```

Impact of Clustering on Other Expressway Applications

Conference Factory (Multiway™)

When using Conference Factory (Multiway) in a cluster, note that:

- The Conference Factory application configuration is NOT replicated across a cluster.
- The Conference Factory template MUST be DIFFERENT on each of the Expressway 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 primary Expressway 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 Expressway serves the conference ID, it cannot serve a conference ID that any other Expressway could have served.

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

See *Cisco TelePresence Multiway Deployment Guide* for more information.

Microsoft Interoperability

If Microsoft infrastructure is deployed with an Expressway cluster, see *Expressway and Microsoft Infrastructure Deployment Guide*.

Cisco Legal Information

Cisco Trademark