Reference

This chapter explains the following:

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 Port

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 1: Creating a custom rule to allow a specific peer to connect to this peer's clustering ports

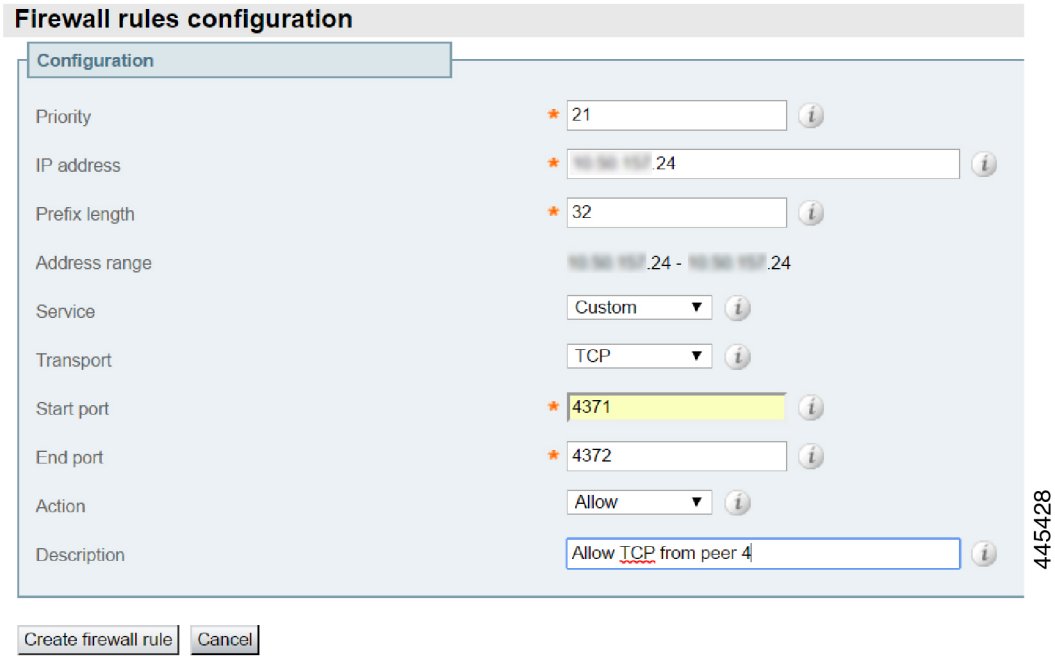
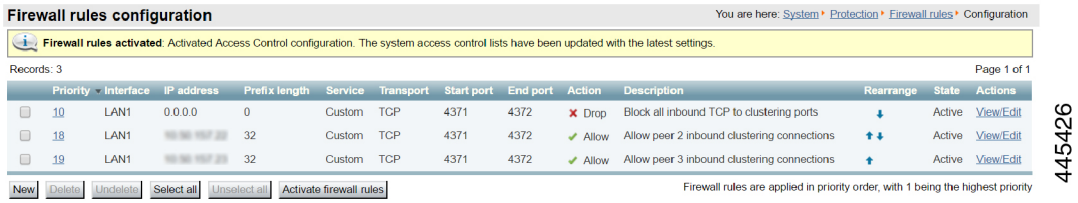


Figure 2: Example list of rules, showing recommended priority order



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 MRA. For more information, see the Cisco Jabber Planning Guide for your version on the Jabber Install and Upgrade Guides page.

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.**

Public DNS (external domains)

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. You also need SIP service records for general deployment (not specifically for MRA). For example, for a cluster of 2 Expressway-E systems:

Table 1:

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 (internal domains)

Although we recommend that the local, internal DNS is configured with *_cisco-uds._tcp.*<*domain*> SRV records, from X12.5 this is no longer a requirement. Example records:

Table 2:

Domain	Service	Protocol	Priority	Weight	Port	Target Host
example.com	cisco-uds	tcp	10	10	8443	cucm1.example.com
example.com	cisco-uds	tcp	10	10	8443	cucm2.example.com

Create internal DNS records, for both forward and reverse lookups, for all Unified Communications nodes used with MRA. This allows Expressway-C to find the nodes when IP addresses or hostnames are used instead of FQDNs.

Ensure that the cisco-uds SRV records are NOT resolvable outside of the internal network, otherwise the Jabber client will not start MRA negotiation via the Expressway-E.

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.
```

Note

- Priorities are all the same. Only use different priorities if you have different clusters allowing failover from one primary cluster to another (secondary) cluster. In that case the primary cluster 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`.

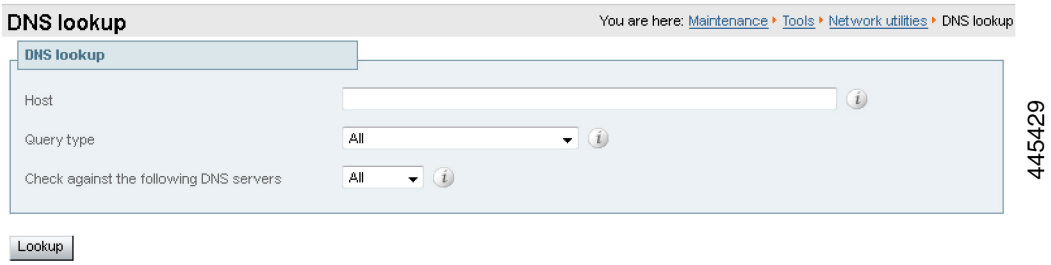
   Use commas to delimit multiple protocols, for example, `_sip._tcp`, `_sips._tcp`.
4. Click **Run**.

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 in 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.