Firewall Traversal

This section describes how to configure your Expressway-C and Expressway-E in order to traverse firewalls.

About Firewall Traversal

The purpose of a firewall is to control IP traffic entering your network. Firewalls generally block unsolicited incoming requests, meaning that any calls originating from outside your network will be prevented. However, firewalls can be configured to allow outgoing requests to certain trusted destinations, and to allow responses from those destinations. This principle is used by Cisco's Expressway technology to enable secure traversal of any firewall.

The Expressway Solution

The Expressway solution consists of:

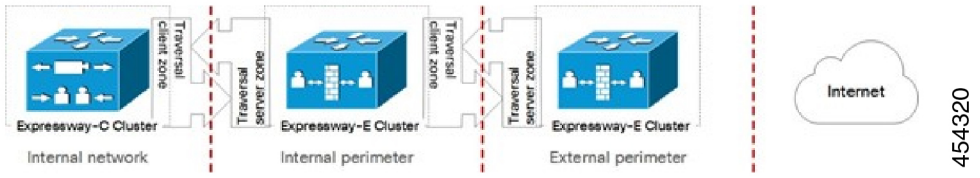
- An Expressway-E located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.
- An Expressway-C or other traversal-enabled endpoint located in a private network, which acts as the firewall traversal client.

The two systems work together to create an environment where all connections between the two are outbound. That is, established from the client to the server. And so able to successfully traverse the firewall.

Chained firewall traversal

For business-to-business Expressway deployments, you can configure firewall traversal chaining. As well as acting as a traversal server, Expressway-E can act as a traversal client to another Expressway-E.

Figure 1: Example of Two Chained Expressway-Es



If you chain two Expressway-Es for example (pictured), the first Expressway-E is a traversal server for the Expressway-C. That first Expressway-E is also a traversal client of the second Expressway-E. The second Expressway-E is a traversal server for the first Expressway-E.

Note

- Traversal chaining is not supported for Mobile and Remote Access deployments.
- This capability was formally introduced to the Cisco Expressway Series in version X8.10. It has been possible with the Cisco TelePresence VCS since firewall traversal was introduced.

Recommendations and Prerequisites

Note We recommend that both the Expressway-E and the Expressway-C run the same software version.

Do not use a shared address for the Expressway-E and the Expressway-C, as the firewall cannot distinguish between them. If you use static NAT for IP addressing on the Expressway-E, make sure that any NAT operation on the Expressway-C does not resolve to the same traffic IP address. We do not support shared NAT addresses between Expressway-E and Expressway-C.

How Does it Work?

The traversal client constantly maintains a connection through the firewall to a designated port on the traversal server. This connection is kept alive by the client sending packets at regular intervals to the server. When the traversal server receives an incoming call for the traversal client, it uses this existing connection to send an incoming call request to the client. The client then initiates the necessary outbound connections required for the call media and/or signaling.

This process ensures that from the firewall's point of view, all connections are initiated from the traversal client inside the firewall out to the traversal server.

For firewall traversal to function correctly, the Expressway-E must have one traversal server zone configured on it for each client system that is connecting to it (this does not include traversal-enabled endpoints which register directly with the Expressway-E; the settings for these connections are configured in a different way). Likewise, each Expressway client must have one traversal client zone configured on it for each server that it is connecting to.

The ports and protocols configured for each pair of client-server zones must be the same. See the Configuring a Traversal Client and Server for a summary of the required configuration on each system. Because the

Expressway-E listens for connections from the client on a specific port, you are recommended to create the traversal server zone on the Expressway-E before you create the traversal client zone on the Expressway-C.

Both the traversal client and the traversal server must be Cisco Expressway systems (neither can be a Cisco VCS).

Endpoint Traversal Technology Requirements

The “far end” (at home or at a hotel, for example) endpoint requirements to support firewall traversal are summarized below:

- For H.323, the endpoint needs to support Assent or H460.18 and H460.19.
- For SIP, the endpoint just needs to support standard SIP.
  - Registration messages will keep the “far end” firewall ports open for Expressway to send messages to that endpoint. The Expressway waits for media from the endpoint behind the firewall, before returning media to it on that same port – the endpoint does have to support media transmission and reception on the same port.
  - The Expressway also supports SIP outbound, which is an alternative method of keeping firewalls open without the overhead of using the full registration message.
- SIP and H.323 endpoints can register to the Expressway-E or they can just send calls to the Expressway-E as the local “DMZ” firewall has relevant ports open to allow communication to the Expressway-E over SIP and H.323 ports.

Endpoints can also use About ICE to find the optimal (in their view of what optimal is) path for media communications between themselves. Media can be sent directly from endpoint to endpoint, from endpoint via the outside IP address of the destination firewall to the destination endpoint, or from the endpoint via a TURN server to destination endpoint.

- The Expressway supports ICE for calls where the Expressway does not have to traverse media (for example if there is no IPv4/IPv6 conversion or SIP / H.323 conversion required); typically this means 2 endpoints which are able to support ICE, directly communicating to an Expressway-E cluster.
- The Expressway-E has its own built-in Configuring TURN Services to support ICE-enabled endpoints.

H.323 Firewall Traversal Protocols

The Expressway supports two different firewall traversal protocols for H.323: Assent and H.460.18/H.460.19.

- Assent is Cisco’s proprietary protocol.
- H.460.18 and H.460.19 are ITU standards which define protocols for the firewall traversal of signaling and media respectively. These standards are based on the original Assent protocol.

A traversal server and traversal client must use the same protocol in order to communicate. The two protocols each use a different range of ports.

SIP Firewall Traversal Protocols

The Expressway supports the Assent protocol for SIP firewall traversal of media.

The signaling is traversed through a TCP/TLS connection established from the client to the server.

Media Demultiplexing

The Expressway-E uses media demultiplexing in the following call scenarios:

- Any H.323 or SIP call leg to/from an Expressway-C through a traversal zone configured to use Assent.
- Any H.323 call leg to/from an Expressway-C through a traversal server zone configured to use H460.19 in demultiplexing mode.
- H.323 call legs between an Expressway-E and an Assent or H.460.19 enabled endpoint.

The Expressway-E uses non-demultiplexed media for call legs directly to/from SIP endpoints (that is endpoints which do not support Assent or H.460.19), or if the traversal server zone is not configured to use H.460.19 in demultiplexing mode.

Media demultiplexing ports on the Expressway-E are allocated from the general range of **traversal media ports**. This applies to all RTP/RTCP media, regardless of whether it is H.323 or SIP.

The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration** > **Local Zones** > **Traversal Subzone**. In Large Expressway systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The Expressway-E listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the Expressway-E (**Configuration** > **Traversal** > **Ports**). If you choose not to configure a particular pair of ports (Use **configured demultiplexing ports** = *No*), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).

Note Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

For example, in a SIP call from within an enterprise to an endpoint at home through an Expressway-C/Expressway-E pair, the only demultiplexing that would occur would be on the Expressway-E ports facing the Expressway-C:

Enterprise endpoint	⟷	**Expressway-C**		⟷	**Expressway-E**		⟷	**Home endpoint**
		Non-demuxed	**Non-demuxed**		**Demuxed**	**Non-demuxed**		
RTP ports		36002	36004		36000	36002		
RTCP ports		36003	36005		36001	36003		

However, an H.323 call from within an enterprise to an Assent capable H.323 endpoint at home through the same Expressway-C/Expressway-E would perform demultiplexing on both sides of the Expressway-E:

Enterprise endpoint	⟷	**Expressway-C**	⟷	**Expressway-E**	⟷	**Home endpoint**

		Non-demuxed	Non-demuxed		Demuxed	Demuxed		
RTP ports		36002	36004		36000	36000		
RTCP ports		36003	36005		36001	36001		

If the Expressway-E has Advanced Networking, it will still use the same port numbers as described above, but they will be assigned to the internal and external IP addresses.

Firewall Traversal Configuration Overview

This section provides an overview to how the Expressway can act as a traversal server or as a traversal client.

Expressway as a Firewall Traversal Client

The Expressway can act as a firewall traversal client on behalf of SIP and H.323 endpoints registered to it, and any systems that are neighbored with it. To act as a firewall traversal client, the Expressway must be configured with information about the systems that will act as its firewall traversal server.

You do this by adding a traversal client zone on the Expressway client (**Configuration** > **Zones** > **Zones**) and configuring it with the details of the traversal server. See Configuring Traversal Client Zones for more information. You can create more than one traversal client zone if you want to connect to multiple traversal servers.

Expressway-C or Expressway-E?

- Typically you use an Expressway-C as a firewall traversal client. However, an Expressway-E can also do this role.
- The firewall traversal server used by the Expressway client must be an Expressway-E.

Expressway as a Firewall Traversal Server

The Expressway-E has all the functionality of an Expressway-C (including being able to act as a firewall traversal client). However, its main feature is that it can act as a firewall traversal server for other Cisco systems and any traversal-enabled endpoints that are registered directly to it. It can also provide TURN relay services to ICE enabled endpoints.

Configuring Traversal Server Zones

For the Expressway-E to act as a firewall traversal server for Cisco systems, you must create a traversal server zone on the Expressway-E (**Configuration** > **Zones** > **Zones**) and configure it with the details of the traversal client. See Configuring Traversal Server Zones for more information.

You must create a separate traversal server zone for every system that is its traversal client.

Configuring Other Traversal Server Features

- For the Expressway-E to act as a firewall traversal server for traversal-enabled endpoints (such as Cisco MXP endpoints and any other endpoints that support the ITU H.460.18 and H.460.19 standards), no additional configuration is required. See Configuring Expressway-E and Traversal Endpoint Communications for more information.
- To enable TURN relay services and find out more about ICE, see About ICE and TURN Services.
- To reconfigure the default ports used by the Expressway-E, see Configuring Ports for Firewall Traversal.

Firewall Traversal and Advanced Networking

The Advanced Networking option key enables the LAN 2 interface on the Expressway-E (the option is not available on an Expressway-C). The LAN 2 interface is used in situations where the Expressway-E is located in a DMZ that consists of two separate networks - an inner DMZ and an outer DMZ - and your network is configured to prevent direct communication between the two.

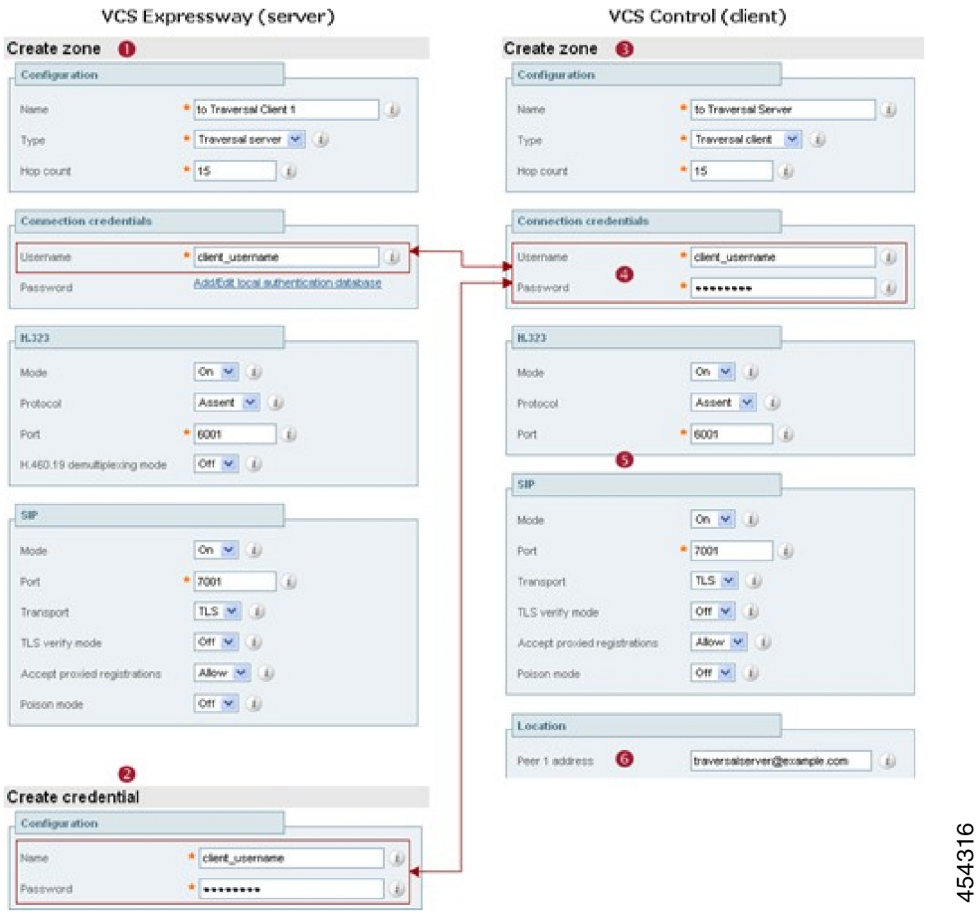
With the LAN 2 interface enabled, you can configure the Expressway with two separate IP addresses, one for each network in the DMZ. Your Expressway then acts as a proxy server between the two networks, allowing calls to pass between the internal and outer firewalls that make up your DMZ.

When Advanced Networking is enabled, all ports configured on the Expressway, including those relating to firewall traversal, apply to both IP addresses; you cannot configure ports separately for each IP address.

Configuring a Traversal Client and Server

The basic steps in configuring a traversal client and server are as follows:

Step	Description
1	On the Expressway-E, create a traversal server zone (this represents the incoming connection from the Expressway-C). In the **Username** field, enter the Expressway-C's authentication username.
2	On the Expressway-E, add the Expressway-C's authentication username and password as credentials into the local authentication database.
3	On the Expressway-C, create a traversal client zone (this represents the connection to the Expressway-E).
4	Enter the same authentication **Username** and **Password** as specified on the Expressway-E.
5	Configure all the modes and ports in the H.323 and SIP protocol sections to match identically those of the traversal server zone on the Expressway-E.
6	Enter the Expressway-E's IP address or FQDN in the **Peer 1 address** field.



Configuring Ports for Firewall Traversal

Note Specific port information is collected in a separate document. See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.

Ports play a vital part in firewall traversal configuration. The correct ports must be set on the Expressway-E, traversal client and firewall in order for connections to be permitted.

Ports are initially configured on the Expressway-E by the Expressway-E administrator. The firewall administrator and the traversal client administrator should then be notified of the ports, and they must configure their systems to connect to these specific ports on the server. The only port configuration required on the traversal client is the range of ports it uses for outgoing connections; the firewall administrator may need to know this information so that if necessary they can configure the firewall to allow outgoing connections from those ports.

The Port Usage pages (under **Maintenance** > **Tools** > **Port usage**) list all the IP ports that are being used on the Expressway, both inbound and outbound. This information can be provided to your firewall administrator so that the firewall can be configured appropriately.

When Advanced Networking is enabled, all ports configured on the Expressway, including those relating to firewall traversal, apply to both IP addresses; you cannot configure ports separately for each IP address.

The Expressway solution works as follows:

1. Each traversal client connects via the firewall to a unique port on the Expressway-E.
2. The server identifies each client by the port on which it receives the connection, and the authentication credentials provided by the client.
3. After the connection is established, the client regularly sends a probe to the Expressway-E to keep the connection alive.
4. When the Expressway-E receives an incoming call for the client, it uses this initial connection to send an incoming call request to the client.
5. The client then initiates one or more outbound connections. The destination ports used for these connections differ for signaling and/or media, and depend on the protocol being used (see the following sections for more details).

Configuring the Firewall

For Expressway firewall traversal to function correctly, your firewall must be configured to:

- Allow initial outbound traffic from the client to the ports being used by the Expressway-E.
- Allow return traffic from those ports on the Expressway-E back to the originating client.

Note We recommend that you turn off any H.323 and SIP protocol support on the firewall. They are not needed with the Expressway solution and may interfere with its operation.

Configuring Traversal Server Ports

The Expressway-E has specific listening ports used for firewall traversal. Rules must be set on your firewall to allow connections to these ports. In most cases the default ports should be used. However, you have the option to change these ports if necessary by going to the **Ports** page (**Configuration** > **Traversal** > **Ports**).

The configurable ports for signaling are:

- **H.323 Assent call signaling port**
- **H.323 H.460.18 call signaling port**

RTP and RTCP Media Demultiplexing Ports

The port configuration options depend upon the type of appliance or VM:

- **Small/Medium systems**: 1 pair of RTP and RTCP media demultiplexing ports are used. They can either be explicitly specified or they can be allocated from the start of the general range of traversal media ports.
- **Large systems**: 6 pairs of RTP and RTCP media demultiplexing ports are used. They are always allocated from the start of the traversal media ports range.

Configuring Ports for Connections From Traversal Clients

Each traversal server zone specifies an H.323 port and a SIP port to use for the initial connection from the traversal client. Each time you configure a new traversal server zone on the Expressway-E, you are allocated default port numbers for these connections:

- H.323 ports start at UDP/6001 and increment by 1 for every new traversal server zone.
- SIP ports start at TCP/7001 and increment by 1 for every new traversal server zone.

You can change these default ports if necessary but you must ensure that the ports are unique for each traversal server zone. After the H.323 and SIP ports have been set on the Expressway-E, matching ports must be configured on the corresponding traversal client.

Note

- The default port used for the initial connections from MXP endpoints is the same as that used for standard RAS messages, that is UDP/1719. While you can change this port on the Expressway-E, most endpoints will not support connections to ports other than UDP/1719, therefore we recommend that you leave this as the default.
- You must allow outbound connections through your firewall to each of the unique SIP and H.323 ports that are configured on each of the Expressway-E's traversal server zones.

The call signaling ports are configured via **Configuration** > **Traversal** > **Ports**. The traversal media port range is configured via **Configuration** > **Local Zone** > **Traversal Subzone**.

If your Expressway-E does not have any endpoints registering directly with it, and it is not part of a cluster, then UDP/1719 is not required. You therefore do not need to allow outbound connections to this port through the firewall between the Expressway-C and Expressway-E.

Configuring TURN Ports

The Expressway-E can be enabled to provide About ICE and TURN Services (Traversal Using Relays around NAT) which can be used by ICE-enabled SIP endpoints.

The ports used by these services are configurable via **Configuration** > **Traversal** > **TURN**.

The ICE clients on each of the SIP endpoints must be able to discover these ports, either by using SRV records in DNS or by direct configuration.

Configuring Ports for Connections Out to the Public Internet

In situations where the Expressway-E is attempting to connect to an endpoint on the public internet, you will not know the exact ports on the endpoint to which the connection will be made. This is because the ports to be used are determined by the endpoint and advised to the Expressway-E only after the server has located the

endpoint on the public internet. This may cause problems if your Expressway-E is located within a DMZ (where there is a firewall between the Expressway-E and the public internet) as you will not be able to specify in advance any rules that will allow you to connect out to the endpoint's ports.

You can however specify the ports on the Expressway-E that are used for calls to and from endpoints on the public internet so that your firewall administrator can allow connections via these ports.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.

Firewall Traversal and Authentication

The Expressway-E allows only authenticated client systems to use it as a traversal server.

Upon receiving the initial connection request from the traversal client, the Expressway-E asks the client to authenticate itself by providing its authentication credentials. The Expressway-E then looks up the client's credentials in its own authentication database. If a match is found, the Expressway-E accepts the request from the client.

The settings used for authentication depend on the type of traversal client:

Traversal client	Expressway-E traversal server
Expressway-C (or Expressway-E) The Expressway client provides its **Username** and **Password**. These are set on the traversal client zone by using **Configuration** > **Zones** > **Zones** > **Edit zone**, in the **Connection credentials** section.	The traversal server zone for the Expressway client must be configured with the client's authentication **Username**. This is set on the Expressway-E by using **Configuration** > **Zones** > **Zones** > **Edit zone**, in the **Connection credentials** section. There must also be an entry in the Expressway-E's authentication database with the corresponding client username and password.
Endpoint The endpoint client provides its **Authentication ID** and **Authentication Password**.	There must be an entry in the Expressway-E's authentication database with the corresponding client username and password.

Note All Expressway traversal clients must authenticate with the Expressway-E, even if the Expressway-E is not using device authentication for endpoint clients.

Authentication and NTP

All Expressway traversal clients that support H.323 must authenticate with the Expressway-E. The authentication process makes use of timestamps and requires that each system uses an accurate system time. The system time on an Expressway is provided by a remote NTP server. Therefore, for firewall traversal to work, all systems involved must be configured with details of an NTP server.

Configuring Expressway-E and Traversal Endpoint Communications

Traversal-enabled H.323 endpoints can register directly with the Expressway-E and use it for firewall traversal.

The **Locally registered endpoints** page (**Configuration** > **Traversal** > **Locally registered endpoints**) allows you to configure the way in which the Expressway-E and traversal-enabled endpoints communicate.

The options available are:

Field	Description
H.323 Assent mode	Determines whether or not H.323 calls using Assent mode for firewall traversal are allowed.
H.460.18 mode	Determines whether or not H.323 calls using H.460.18/19 mode for firewall traversal are allowed.
H.460.19 demux mode	Determines whether the Expressway-E operates in demultiplexing mode for calls from locally registered endpoints. *On*: Uses the media demultiplexing ports for all calls. *Off*: Each call uses a separate pair of ports for media.
H.323 preference	Determines which protocol the Expressway-E uses if an endpoint supports both Assent and H.460.18.
UDP probe retry interval	The frequency (in seconds) with which locally registered endpoints send a UDP probe to the Expressway-E.
UDP probe retry count	The number of times locally registered endpoints attempt to send a UDP probe to the Expressway-E.
UDP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a UDP probe to the Expressway-E after a call is established, in order to keep the firewall's NAT bindings open.
TCP probe retry interval	The frequency (in seconds) with which locally registered endpoints send a TCP probe to the Expressway-E.
TCP probe retry count	The number of times locally registered endpoints attempt to send a TCP probe to the Expressway-E.
TCP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a TCP probe to the Expressway-E after a call is established, in order to keep the firewall's NAT bindings open.

About ICE and TURN Services

About ICE

ICE (Interactive Connectivity Establishment) provides a mechanism for SIP client NAT traversal. ICE is not a protocol, but a framework which pulls together a number of different techniques such as TURN (Traversal Using Relays around NAT) and STUN (Session Traversal Utilities for NAT).

It allows endpoints (clients) residing behind NAT devices to discover paths through which they can pass media, verify peer-to-peer connectivity via each of these paths and then select the optimum media connection path. The available paths typically depend on any inbound and outbound connection restrictions that have been configured on the NAT device. Such behavior is described in RFC 4787.

An example usage of ICE is two home workers communicating via the internet. If the two endpoints can communicate via ICE the Expressway-E may (depending on how the NAT devices are configured) only need to take the signaling and not take the media (and is therefore a non-traversal call). If the initiating ICE client attempts to call a non-ICE client, the call set-up process reverts to a conventional SIP call requiring NAT traversal via media latching where the Expressway also takes the media.

For more information about ICE, see RFC 5245.

ICE Passthrough for MRA Deployments

From X12.5, we support Interactive Connectivity Establishment (ICE) passthrough to allow MRA-registered endpoints to pass media directly between endpoints by bypassing the WAN and the Cisco Expressway Series.

Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway guide* on the Expressway Configuration Guides page.

About TURN

TURN services are relay extensions to the STUN network protocol that enable a SIP client to communicate via UDP or TCP from behind a NAT device.

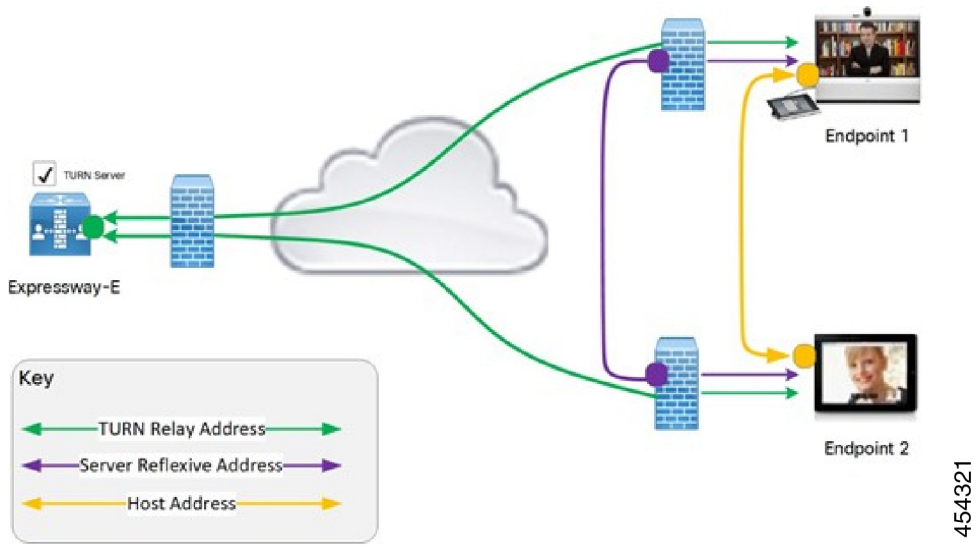
For more information about TURN see RFC 5766, and for detailed information about the base STUN protocol, see RFC 5389.

Each ICE client requests the TURN server to allocate relays for the media components of the call. A relay is required for each component in the media stream between each client.

After the relays are allocated, each ICE client has 3 potential connection paths (addresses) through which it can send and receive media:

- Its host address which is behind the NAT device (and thus not reachable from endpoints on the other side of the NAT).
- Its publicly-accessible address on the NAT device.
- A relay address on the TURN server.

Figure 2: ICE Media connection paths



The endpoints then decide, by performing connectivity checks through ICE, how they are going to communicate. Depending upon how the NAT devices are configured, the endpoints may be able to communicate between their public-facing addresses on the NAT devices or they may have to relay the media via the TURN server. If both endpoints are behind the same NAT device they can send media directly between themselves using their internal host addresses.

After the media route is selected, the TURN relay allocations are released if the chosen connection paths do not involve routing via the TURN server. Note that the signaling always goes via the Expressway, regardless of the final media communication path chosen by the endpoints.

Note The TURN server can relay media between any two ICE clients, even if one or both are inside the enterprise internal firewall.

Capabilities and Limitations

- From X12.6.1, due to security enhancements, the Expressway-E TURN server no longer functions as a generic STUN server and will not accept unauthenticated STUN binding requests. This leads to the following scenarios:
  - Scenario A: If you use the B2BUA as a TURN client for Microsoft interoperability (as described in the *Cisco Expressway with Microsoft Infrastructure Deployment Guide*), the B2BUA will not send any STUN binding requests to the TURN server to check if it is alive or not. This means that from Expressway X12.6.1, the B2BUA may try to use a TURN server that is not reachable and hence that **calls may fail**.
  - Scenario B: Depending on the CMS version deployed, the CMS WebRTC solution may use STUN bind requests towards TURN server on Expressway-E, which will cause failures. So if you use Meeting Server WebRTC, check that your CMS version is compatible before you install Expressway version X12.6.1 or later software. Bug ID CSCvv01243 refers. (For more information about

Expressway-E TURN server configuration, see the *Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide*.)

- Small or Medium systems support up to 1800 relay allocations. This is typically enough to support their maximum concurrent call limits, but does depend on the network topology and the number of media stream components used for the call. For example, some calls use Duo Video, or other calls use only audio.
- A Large system supports up to 6000 relays. The full relay capacity is available on one external port when port multiplexing is enabled or spread across six external ports when port range is configured. When it is spread across the ports, each port is limited to handling 1000 relays.

  This limit is not strictly enforced. Therefore we recommend creating DNS SRV record with six A/AAAA entries, with the same address, for each port address in the range. After creating the record, configure the clients with the SRV record of the Expressway-E TURN server. If TURN multiplexing is enabled, we recommend creating an SRV record only for the external port that listens to TURN requests.
- On a Large system, you can configure the TURN server to listen for TURN requests on a range of ports, from 3478 to 3483 by default. From X8.11, if TURN multiplexing is enabled, the Expressway-E accepts all TURN requests on the first port in the range (typically UDP 3478). The Expressway internally demultiplexes those requests onto the port range. The TURN clients must send requests on the configured single port, but the full capacity of the large Expressway-E TURN server is available.
- From X8.11, Expressway-E can listen to both TURN and Cisco Meeting Server requests on the TCP port 443. When Expressway-E receives a connection request through port 443, it forwards the request either to the TURN server or to the Meeting Server Web Proxy depending on the request type. As a result, it allows external users to use TURN services and join Meeting Server spaces from an environment with restricted firewall policies.

  If the web administrator port is configured to listen on port 443 (**System** > **Administration Settings**), for Expressway versions before X12.7 it must be changed from 443 to any other valid port. From X12.7, you do not need to do this if the Expressway is configured to use its Dedicated Management Interface as the only administration interface. That is, on the **System** > **Administration settings** page, **Use Dedicated Management Interface only (for administration)** is set to *Yes*.
- On a Large system, if TCP 443 TURN service is enabled, and the TURN multiplexing feature is also enabled, then 6000 TCP TURN relays are supported.
- Clustered Expressways: if the requested TURN server's relays are fully allocated the server will respond to the requesting client with the details of an alternative server in the cluster (the TURN server currently with the most available resources).
- The Expressway's TURN services are supported over single and dual network interfaces (via the Advanced Networking option). For dual network interfaces, the TURN server listens on both interfaces but relays are allocated only on the Expressway's externally facing LAN interface.
- Expressway-E's TURN server does not support Microsoft ICE (which is not standards-based). To enable communications between the Expressway and Microsoft clients that are registered through a Microsoft Edge Server you need to use the Microsoft interoperability service.
- The TURN server does not support bandwidth requests. Traversal zone bandwidth limits do not apply.
- The Expressway-E TURN server supports TURN media over TCP and UDP. Configuration of the supported protocols is available only through the CLI command **xConfiguration Traversal Server TURN ProtocolMode**.

- The Expressway-E TURN server supports UDP relays over TCP.

STUN Packets Sometimes Sent Over the Internal Interface

Expressway always sends STUN packets that it receives through its external LAN interface, using the external LAN IP address as the packet source address. Typically the packets are sent from the external interface, and so the IP addresses usually match up. However, in the following cases, note that Expressway sends the STUN packets out from the *internal* LAN interface:

- If the TURN client is using a relay session to send a message to a device in the same subnet as the internal IP of the Expressway-E, or
- If the TURN client is using a relay session to send a message to a device in a subnet which matches a static route that uses the internal gateway IP of the Expressway-E.

This behavior may create the impression that there is a mismatch in the IP address, but in fact the system is working as designed.

Configuring TURN Services

TURN relay services are only available on the Expressway-E. (From X8.11, the TURN Relay option key is not required to use TURN services.)

The **TURN** page (**Configuration** > **Traversal** > **TURN**) is used to configure the Expressway-E's TURN settings. If you are configuring your Expressway-E for delegated credential checking you can also determine, via the **Authentication realm**, the traversal zone through which credential checking of TURN server requests is delegated.

The configurable options are:

Field	Description	Usage Tips
TURN services	Determines whether the Expressway offers TURN services to traversal clients.	If you need to modify other TURN settings while the **TURN services** is already set to *On*: **1.** Change **TURN services** to *Off* and **Save**. **2.** Modify the required TURN settings. **3.** Change **TURN services** to *On* and **Save**. This is because changes to other TURN settings do not come into effect until the **TURN services** is restarted

Field	Description	Usage Tips
TCP 443 TURN service	Determines if the TURN server must listen to TCP request from TURN clients on TCP port 443. The options are: • *On*: The TURN server listens to the TCP requests from TURN clients on the TCP port 443 and the UDP requests on the configured port. • *Off*: TURN server does not listen to TURN clients on TCP port 443. However this setting does not affect the ports configured to listen to TURN requests.	Before enabling this feature, make sure the following: • **TURN services** is set to *On*. • Before X12.7, if the web administrator port is configured to listen on port 443 (**System** > **Administration Settings**), it must be changed from 443 to any other valid port. From X12.7, you do not need to do this if the Expressway is configured to use its Dedicated Management Interface as the only administration interface. That is, on the **System** > **Administration settings** page, **Use Dedicated Management Interface only (for administration)** is set to *Yes*.

Field	Description	Usage Tips

TURN port multiplexing	On Large systems, enables the full capacity of the Expressway TURN server on a single listening port and internally demultiplexes those requests onto the range of ports.
	Note This option is only available on Large systems.
	The possible options are:
	• *On:*
	  • The Expressway listens on a single configurable external port instead of a range.
	  • If **TCP 443 TURN services** is *On*, the configurable external port only multiplexes UDP TURN requests.
	  Note If **TCP 443 TURN services** is *On*, the external port does not multiplexes the TCP TURN requests due to technical limitation.
	• *Off*: The TURN server listens to the TCP and UDP requests on the range of ports.
		Before enabling this feature, make sure that the **TURN services** is set to *On*.

TURN requests port	The listening port for TURN requests. The default port is 3478.	On a Large system, this option is available only if **TURN port multiplexing** is set to *On*. To allow endpoints to discover TURN services, create DNS SRV records for **_turn._udp.** and **_turn._tcp** (either for the single port, or range of ports as appropriate).
TURN requests port range start	If **TURN port multiplexing** is *Off*, this port represents the first port in the configurable range on Large systems. The default port range start is 3478.	This option is available only on Large systems and if **TURN port multiplexing** is set to *Off*.

Field	Description	Usage Tips
TURN requests port range end	If **TURN port multiplexing** is *Off*, this port represents the upper port in the configurable range on Large systems. The default port range end is 3483.	This option is available only on Large systems and if **TURN port multiplexing** is set to *Off*.
Delegated credential checking	Controls whether the credential checking of TURN server requests is delegated, via a traversal zone, to another Expressway. The associated **Authentication realm** determines which traversal zone is used. *Off*: Use the relevant credential checking mechanisms (local database or H.350 directory via LDAP) on the Expressway performing the authentication challenge. *On*: Delegate the credential checking to a traversal client. The default is *Off*.	See delegated credential checking for more information.
Authentication realm	The realm sent by the server in its authentication challenges.	Ensure that the client's credentials are stored in the local authentication database.
Media port range start	The lower port in the range used for the allocation of TURN relays. The default TURN relay media port range is 24000 to 29999.	
Media port range end	The upper port in the range used for the allocation of TURN.	

TURN server status

A summary of the TURN server status is displayed at the bottom of the **TURN** page. When the TURN server is active, the summary also displays the number of active TURN clients and the number of active relays.

Click on the active relay links to access the TURN relay usage page, which lists all the currently active TURN relays on the Expressway. You can also review further details of each TURN relay including permissions, channel bindings and counters.