Cisco Expressway Basic Configuration

Deployment Guide

Cisco Expressway X8.1

D15060.03

August 2014

Contents

Introduction

Cisco Expressway is designed specifically for comprehensive collaboration services provided through Cisco Unified Communications Manager. It features established firewall-traversal technology and helps redefine traditional enterprise collaboration boundaries, supporting our vision of any-to-any collaboration.

This document describes how to configure an Expressway-E and an Expressway-C as the cornerstones of a basic video infrastructure deployment.

- It takes the video network administrator through the series of tasks required to set up the Expressways and then describes how to check that the system is working as expected.
- It provides the required DNS, NAT and firewall configuration information but assumes that the network administrator has a working knowledge of configuring these systems.

Detailed reference information is contained in this document's appendices:

- Appendix 1: Configuration details [p.36] lists the Expressway configuration details used in this document.
- Appendix 2: DNS records [p.40] describes the DNS records required for this example deployment.
- Appendix 3: Firewall and NAT settings [p.42] includes details of required NAT and firewall configurations. This document describes a small subset of the numerous NAT and firewall deployment options that are made possible by using the Expressway-E dual network interface and NAT features.
- Appendix 4: Advanced network deployments [p.45] explains how to deploy your system with a static NAT and Dual Network Interface architecture.

Descriptions of system configuration parameters can be found in *Expressway Administrator Guide* and the Expressway web application's online field help and page help .

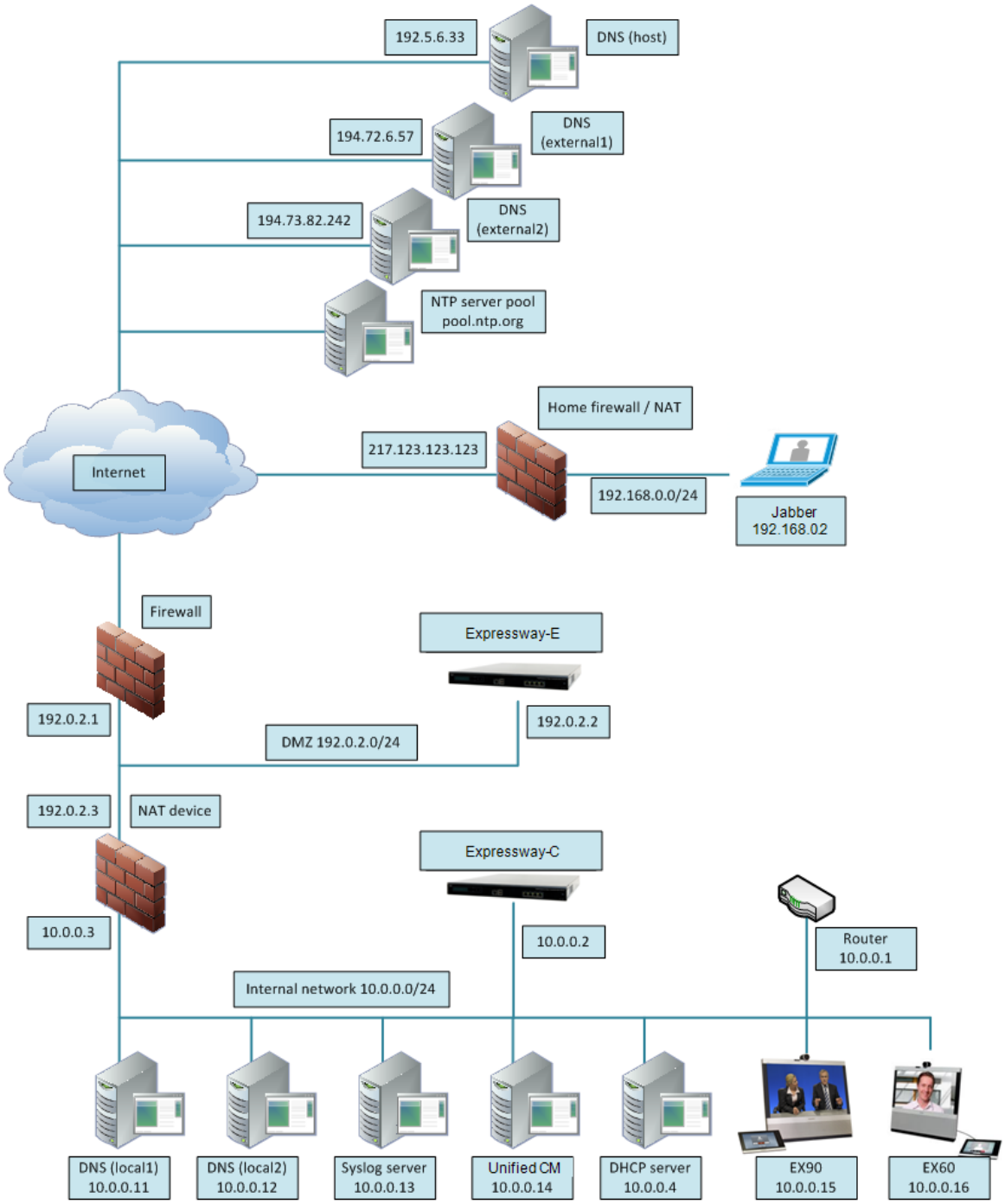
This document does not describe details of how to deploy a cluster of Expressways. For more details on clustering, see *Expressway Cluster Creation and Maintenance Deployment Guide*.

To configure your Expressway system for Unified Communications services, see *Unified Communications Mobile and Remote Access via Expressway Deployment Guide*.

Note that endpoints or other devices cannot register to the Expressway.

Example network deployment

The example network shown below is used as the basis for the deployment described in this document.



This example network includes internal and DMZ segments – in which Expressway-C and Expressway-E platforms are respectively deployed.

Network elements

Internal network elements

The internal network elements are devices which are hosted on the organization's local area network.

Elements on the internal network have an internal network domain name. This internal network domain name is not resolvable by a public DNS. For example, the Expressway-C is configured with an internally resolvable name of expc.internal-domain.net (which resolves to an IP address of 10.0.0.2 by the internal DNS servers).

Expressway-C

The Expressway-C is a SIP Proxy and communications gateway for Unified CM.

The Expressway-C is configured with a traversal client zone to communicate with the Expressway-E to allow inbound and outbound calls to traverse the NAT device.

EX90 and EX60

These are example endpoints hosted on the internal network which register to Unified CM.

Note that endpoints or other devices cannot register to the Expressway. Registration requests will be rejected and will be logged with 'License limit exceeded' messages.

DNS (local 1 & local 2)

DNS servers used by the Expressway-C, to perform DNS lookups (resolve network names on the internal network).

DHCP server

The DHCP server provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.

Router

The router device acts as the gateway for all internal network devices to route towards the DMZ (to the NAT device internal address).

Unified CM

Endpoint devices register to Unified CM and the Expressway acts as a Unified Communications gateway for third-party devices and to provide mobile and remote access.

To configure your Expressway system for Unified Communications services, see *Unified Communications Mobile and Remote Access via Expressway Deployment Guide*.

Syslog server

A logging server for Syslog messages (see Task 13: Configuring logging (optional) [p.30]).

DMZ network element

Expressway-E

The Expressway-E is a SIP Proxy for devices which are located outside the internal network (for example, home users and mobile worker registering to Unified CM across the internet and 3rd party businesses making calls to, or receiving calls from this network).

The Expressway-E is configured with a traversal server zone to receive communications from the Expressway-C in order to allow inbound and outbound calls to traverse the NAT device.

The Expressway-E has a public network domain name. For example, the Expressway-E is configured with an externally resolvable name of expe.example.com (which resolves to an IP address of 192.0.2.2 by the external / public DNS servers).

External network elements

Jabber

An example remote endpoint, which is registering over the internet to Unified CM via the Expressway-E and Expressway-C.

DNS (Host)

The DNS owned by service provider which hosts the external domain example.com.

DNS (external 1 & external 2)

The DNS used by the Expressway-E to perform DNS lookups.

NTP server pool

An NTP server pool which provides the clock source used to synchronize both internal and external devices.

NAT devices and firewalls

The example deployment includes:

- NAT (PAT) device performing port address translation functions for network traffic routed from the internal network to addresses in the DMZ (and beyond — towards remote destinations on the internet).
- Firewall device on the public-facing side of the DMZ. This device allows all outbound connections and inbound connections on specific ports. See Appendix 3: Firewall and NAT settings [p.42].
- Home firewall NAT (PAT) device which performs port address and firewall functions for network traffic originating from the EX60 device.
- See Appendix 4: Advanced network deployments [p.45] for information about how to deploy your system with a static NAT and Dual Network Interface architecture.

SIP and H.323 domain

The example deployment is configured to route SIP (and H.323) signaling messages for calls made to URIs which use the domain example.com.

- DNS SRV records are configured in the public (external) and local (internal) network DNS server to enable routing of signaling request messages to the relevant infrastructure elements.
- The internal SIP domain (example.com) is the same as the public DNS name. This enables both registered and non-registered devices in the public internet to call endpoints registered to the internal infrastructure.

The DNS SRV configurations are described in Appendix 2: DNS records [p.40].

Prerequisites and process summary

Prerequisites

Before starting the system configuration, make sure you have access to:

- the *Expressway Administrator Guide* and *Expressway Getting Started Guide* (for reference purposes)
- your Expressway system
- a PC connected via Ethernet to a LAN which can route HTTP(S) traffic to the Expressway
- a web browser running on the PC
- a serial interface on the PC and cable (if the initial configuration is to be performed over the serial interface)

The following non-Expressway system configuration should also be completed:

- internal and external DNS records (see Appendix 2: DNS records [p.40])
- NAT & firewall configuration (see Appendix 3: Firewall and NAT settings [p.42])
- DHCP server configuration (not described in this document)

Summary of process

The configuration process consists of the following tasks.

Expressway system configuration:

- Task 1: Performing initial configuration [p.9]
- Task 2: Setting the system name [p.9]
- Task 3: Configuring DNS [p.10]
- Task 4: Replacing the default server certificate [p.12]
- Task 5: Configuring NTP servers [p.13]

Routing configuration:

- Task 6: Configuring transforms [p.14]
- Task 7: Configuring the traversal zone [p.15]
- Task 8: Configuring traversal zone search rules [p.19]
- Task 9: Configuring the DNS zone [p.22]
- Task 10: Configuring DNS zone search rules [p.23]
- Task 11: Configuring external (unknown) IP address routing [p.24]

Optional configuration tasks:

- Task 12: Configuring routes to a neighbor zone (optional) [p.29]
- Task 13: Configuring logging (optional) [p.30]
- Task 14: Restricting access to ISDN gateways (optional) [p.31]

Expressway system configuration

Task 1: Performing initial configuration

Assuming the Expressway is in the factory delivered state, follow the Initial configuration steps described in the *Expressway Getting Started Guide* to configure the basic network parameters:

- LAN1 IP (IPv4 or IPv6) address
- Subnet mask (if using IPv4)
- Default Gateway IP address (IPv4 or IPv6)

Note that Expressway requires a static IP address (it will not pick up an IP address from a DHCP server).

The initial configuration can be performed in one of three ways:

- using a serial cable
- via the front panel of the Expressway appliance
- via the default IP address of 192.168.0.100

See the “Initial configuration” section in *Expressway Getting Started Guide* for details.

This deployment guide is based on configuration using the web interface. If you cannot access the Expressway using the web interface after completing the initial configuration (assigning the IP address), speak to your network administrator.

The follow configuration values are used in the example deployment:

	Expressway-C	Expressway-E
LAN1 IPv4 address	10.0.0.2	192.0.2.2
IPv4 gateway	10.0.0.1	192.0.2.1
LAN1 subnet mask	255.255.255.0	255.255.255.0

Task 2: Setting the system name

The **System name** defines the name of the Expressway.

The **System name** appears in various places in the web interface, and in the display on the front panel of the appliance (so that you can identify it when it is in a rack with other systems).

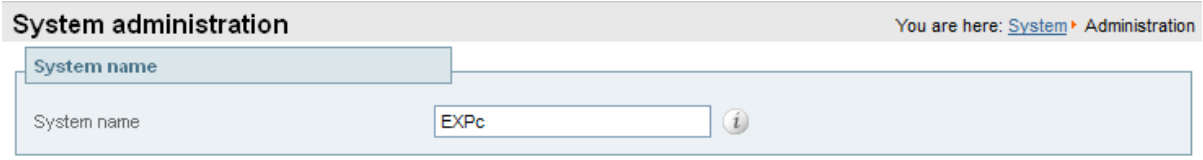
You are recommended to give the Expressway a name that allows you to easily and uniquely identify it. If the system name is longer than 16 characters, only the last 16 characters will be shown in the display on the front panel.

To configure the **System name**:

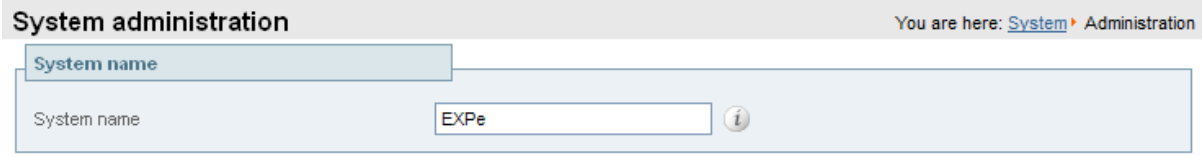
1. Go to **System > Administration**.
2. Configure the **System name** as follows:

	Expressway-C	Expressway-E
System name	Enter `EXPc`	Enter `EXPe`

3. Click **Save**.



Expressway-C



Expressway-E

Task 3: Configuring DNS

System host name

The **System host name** defines the DNS hostname that this system is known by. Note that this is not the fully-qualified domain name, just the host label portion.

Note that <**System host name**>.<**Domain name**> = FQDN of this Expressway.

To configure the **System host name**:

1. Go to **System > DNS**.
2. Configure the **System host name** as follows:

	Expressway-C	Expressway-E
System host name	Enter `expc`	Enter `expe`

3. Click **Save**.

Domain name

The **Domain name** is the name to append to an unqualified host name before querying the DNS server.

To configure the **Domain name**:

1. Go to **System > DNS**.
2. Configure the **Domain name** as follows:

	Expressway-C	Expressway-E
Domain name	Enter `internal-domain.net`	Enter `example.com`

3. Click **Save**.

DNS servers

The DNS server addresses are the IP addresses of up to 5 domain name servers to use when resolving domain names. You must specify at least one default DNS server to be queried for address resolution if you want to either:

- use FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, neighbor zones and peers)
- use features such as URI dialing or ENUM dialing

The Expressway only queries one server at a time; if that server is not available the Expressway will try another server from the list.

In the example deployment 2 DNS servers are configured for each Expressway, which provides a level of DNS server redundancy. The Expressway-C is configured with DNS servers which are located on the internal network. The Expressway-E is configured with DNS servers which are publicly routable.

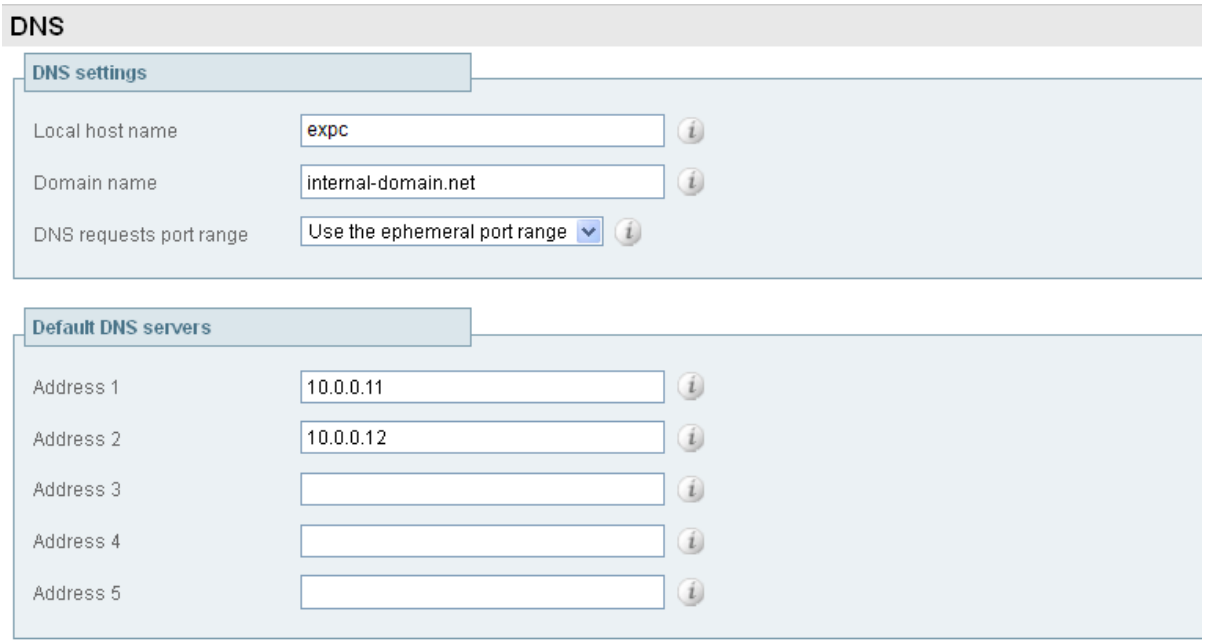
To configure the **Default DNS server** addresses:

1. Go to **System > DNS**.
2. Configure the DNS server **Address** fields as follows:

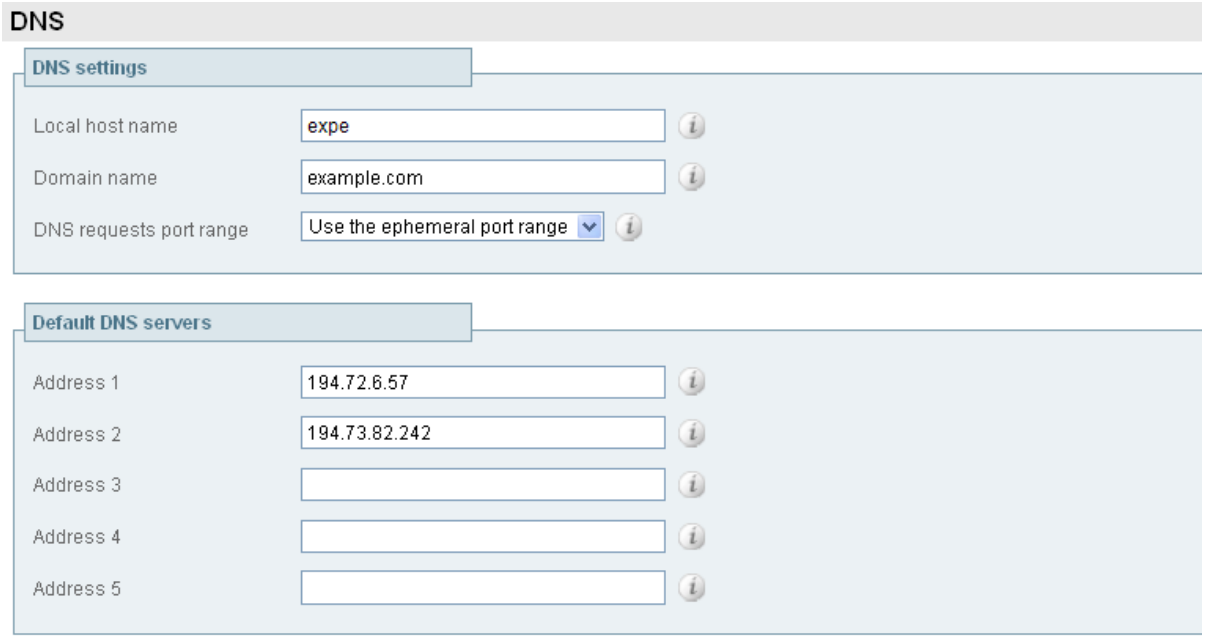
	Expressway-C	Expressway-E
Address 1	Enter `10.0.0.11`	Enter `194.72.6.57`
Address 2	Enter `10.0.0.12`	Enter `194.73.82.242`

3. Click **Save**.

Expressway-C has a Fully Qualified Domain Name of expc.internal-domain.net



Expressway-E has a Fully Qualified Domain Name of expe.example.com



Task 4: Replacing the default server certificate

For extra security, you may want to have the Expressway communicate with other systems (such as LDAP servers, neighbor Expressways, or clients such as SIP endpoints and web browsers) using TLS encryption.

For this to work successfully in a connection between a client and server:

- The server must have a certificate installed that verifies its identity. This certificate must be signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

The Expressway allows you to install appropriate files so that it can act as either a client or a server in connections using TLS. The Expressway can also authenticate client connections (typically from a web browser) over HTTPS. You can also upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates.

The Expressway can generate server certificate signing requests (CSRs). This removes the need to use an external mechanism to generate and obtain certificate requests.

For secure communications (HTTPS and SIP/TLS) we recommend that you replace the Expressway default certificate with a certificate generated by a trusted certificate authority.

Note that in connections:

- to an endpoint, the Expressway acts as the TLS server
- to an LDAP server , the Expressway is a client
- between two Expressway systems, either Expressway may be the client with the other Expressway being the TLS server
- via HTTPS, the web browser is the client and the Expressway is the server

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend that you confirm that your system is working correctly before you attempt to secure the connection with TLS. You are also recommended to use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

Note: be careful not to allow your CA certificates or CRLs to expire as this may cause certificates signed by those CAs to be rejected.

To load the trusted CA list, go to **Maintenance > Security certificates > Trusted CA certificate**.

To generate a CSR and/or upload the Expressway's server certificate, go to **Maintenance > Security certificates > Server certificate**.

Additional server certificate requirements apply when configuring your Expressway system for Unified Communications. For full information, see *Expressway Certificate Creation and Use Deployment Guide*.

Task 5: Configuring NTP servers

The **NTP server** address fields set the IP addresses or Fully Qualified Domain Names (FQDNs) of the NTP servers to be used to synchronize system time.

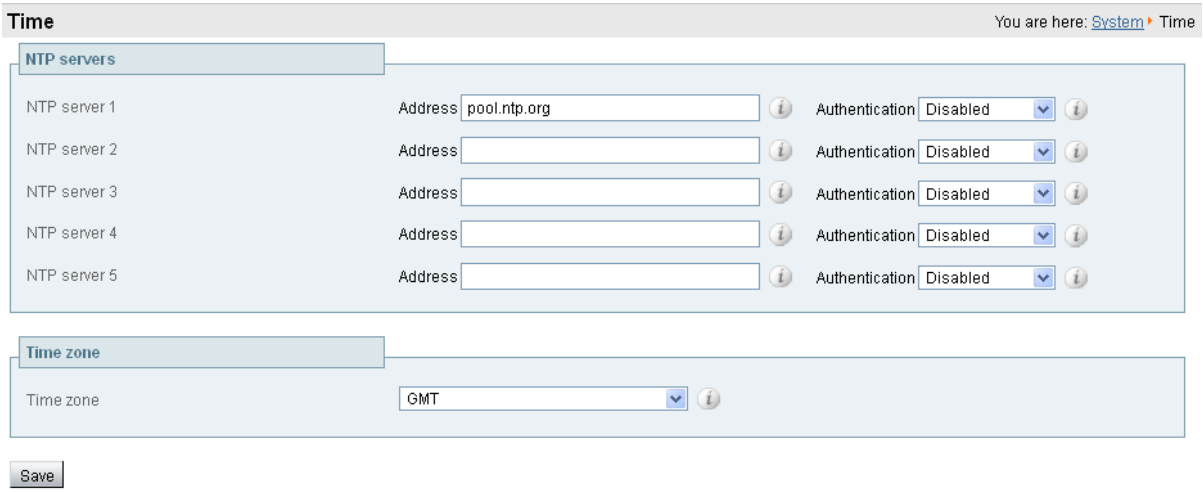
The **Time zone** sets the local time zone of the Expressway.

To configure the NTP server address and Time zone:

1. Go to **System > Time**.
2. Configure the fields as follows (on both Expressway-C and Expressway-E):

	Expressway-C	Expressway-E
NTP server 1	Enter `pool.ntp.org`	Enter `pool.ntp.org`
Time zone	*GMT* in this example	*GMT* in this example

3. Click **Save**.



Routing configuration

Pre-search transforms

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The transformation is applied by the Expressway before any searches are sent to external zones.

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices. This means that the same call searches will work for calls from both H.323 and SIP endpoints.

For example, if the called address is an H.323 E.164 alias “01234”, the Expressway will automatically append the configured domain name (in this case example.com) to the called address (that is, 01234@example.com making it into a URI), before attempting to set up the call.

- Pre-search transforms should be used with care because they apply to all signaling messages – if they match, they will affect the routing of Unified Communications messages, provisioning and presence requests as well as call requests.
- Transformations can also be carried out in search rules – consider whether it is best to use a pre-search transform or a search rule to modify the called address to be looked up.

Search rules

Search rules define how the Expressway routes calls (to destination zones, such as to Unified CM or to a Cisco VCS) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule.

The search rules described in this document are used to ensure that SIP (and H.323, if registered to a Cisco VCS for example) endpoints can dial H.323 devices that have registered E.164 numbers or H.323 IDs without a domain portion. The search rules first search for received destination aliases without the domain portion of the URI, and then search with the full URI.

The routing configuration in this document searches for destination aliases that have valid SIP URIs (that is, using a valid SIP domain, such as id@domain).

You can configure routing which enables calls to unregistered devices on an internal network (routing to the addresses of IP of the devices) by configuring a search rule with a mode of *Any IP address*. However this is not recommended (and not described in this document). The best practice is to register all devices and route using destination aliases.

Task 6: Configuring transforms

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices.

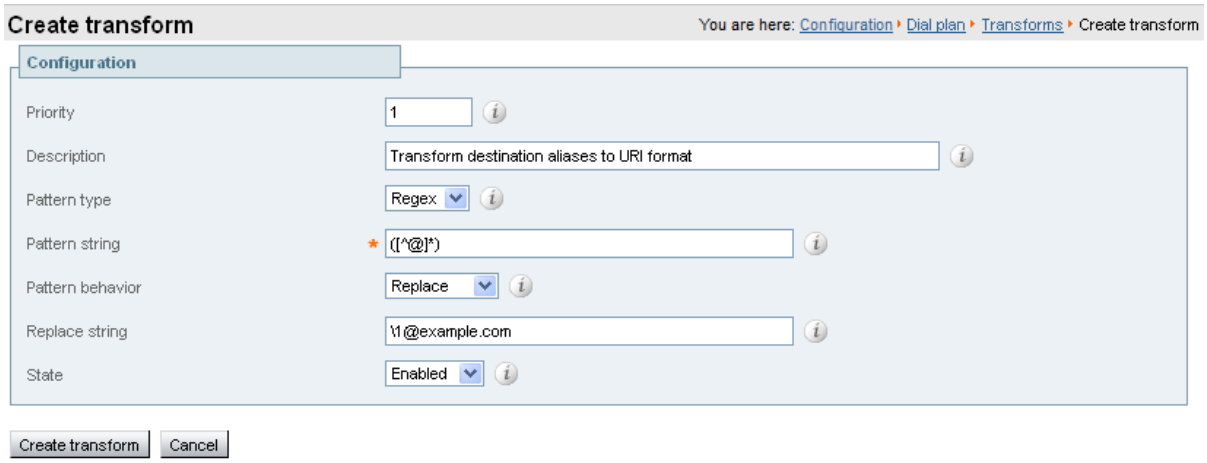
The following transform modifies the destination alias of all call attempts made to destination aliases which do not contain an ‘@’. The old destination alias has @example.com appended to it. This has the effect of standardizing all called destination aliases into a SIP URI format.

To configure the transform:

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the transform fields as follows:

	Expressway-C	Expressway-E
Priority	Enter `1`	Same as Expressway-C
Description	Enter `Transform destination aliases to URI format`	
Pattern type	*Regex*	
Pattern string	Enter `([^@]*)`	
Pattern behavior	*Replace*	
Replace string	Enter `\1@example.com`	
State	*Enabled*	

4. Click **Create transform**.



Task 7: Configuring the traversal zone

The traversal zone configuration defines a connection between the Expressway-C and Expressway-E platforms.

- A traversal zone connection allows firewall traversal for signaling and media between the two platforms.
- The Expressway-C is configured with a traversal client zone, and the Expressway-E with a traversal server zone.

To configure the traversal zone:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

	Expressway-C	Expressway-E
Name	Enter `Traversal zone`	Enter `Traversal zone`
Type	*Traversal client*	*Traversal server*
Username	Enter `exampleauth`	Enter `exampleauth`
Password	Enter `ex4mpl3.c0m`	Not applicable
H.323 Mode	*On*	*On*
H.323 Protocol	*Assent*	*Assent*
H.323 Port	Enter `6001`	Enter `6001`
H.323 H.460.19 demultiplexing mode	Not applicable	*Off*
SIP Mode	*On*	*On*
SIP Port	Enter `7001`	Enter `7001`
SIP Transport	*TLS*	*TLS*
SIP TLS verify mode	*Off*	*Off*
Location Peer 1 address	Enter `192.0.2.2`	Not applicable

4. Click **Create zone**.

Create zone

You are here: Configuration ▸ Zones ▸ Zones ▸ Create zone

Configuration

Name *	TraversalZone
Type *	Traversal client
Hop count *	15

Connection credentials

Username *	exampleauth
Password *	••••••••••••

H.323

Mode	On
Protocol	Assent
Port *	6001

SIP

Mode	On
Port *	7001
Transport	TLS
TLS verify mode	Off
Media encryption mode	Auto
ICE support	Off
Poison mode	Off

Authentication

Authentication policy	Do not check credentials

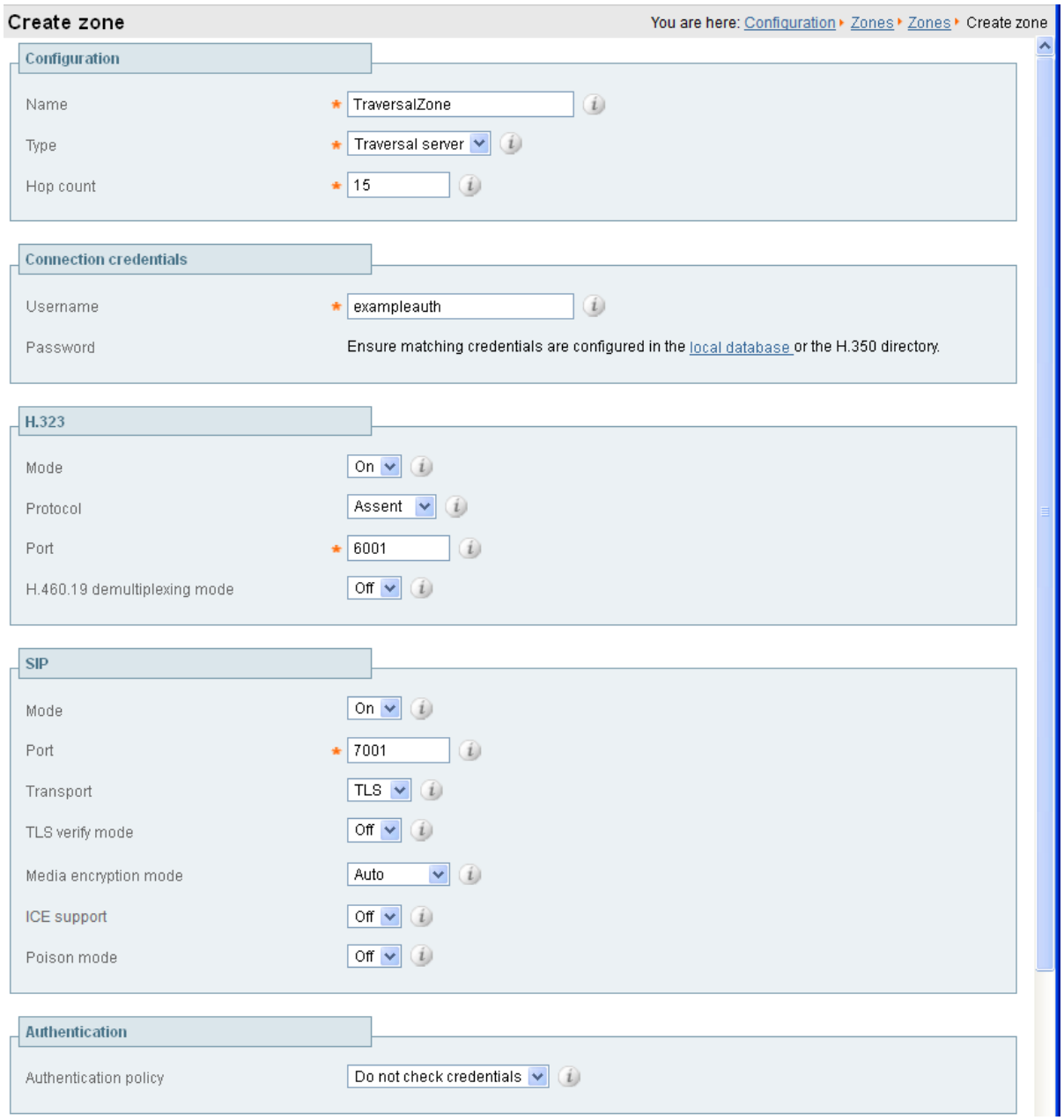
Client settings

Retry interval *	120

Location

Peer 1 address	192.0.2.2

Expressway-C



Expressway-E

To configure the authentication credentials in the **Local authentication database** (which are configured in the Expressway-E only):

1. Go to **Configuration > Authentication > Devices > Local database**.
2. Click **New**.

3. Configure the fields as follows:

	Expressway-C	Expressway-E
Name	Not applicable	Enter `exampleauth`
Password	Not applicable	Enter `ex4mpl3.c0m`

4. Click **Create credential**.

Configuring traversal zones for Unified Communications

To support Unified Communications features such as mobile and remote access or Jabber Guest, there must be a secure traversal zone connection between the Expressway-C and the Expressway-E:

- The traversal client zone and the traversal server zone must be configured to use SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** must be *Force encrypted*.
- Both Expressways must trust each other's server certificate. As each Expressway acts both as a client and as a server you must ensure that each Expressway's certificate is valid both as a client and as a server.
- If a H.323 or a non-encrypted connection is required, a separate pair of traversal zones must be configured.

Task 8: Configuring traversal zone search rules

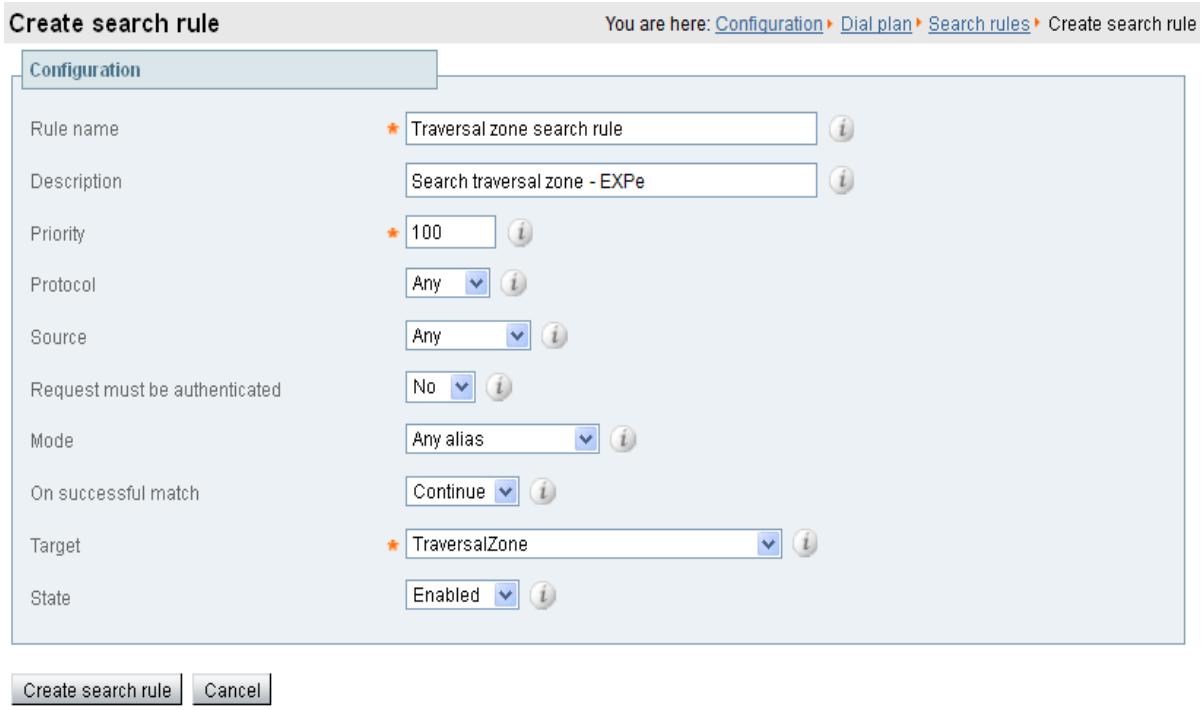
To create the search rules to route calls via the traversal zone.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

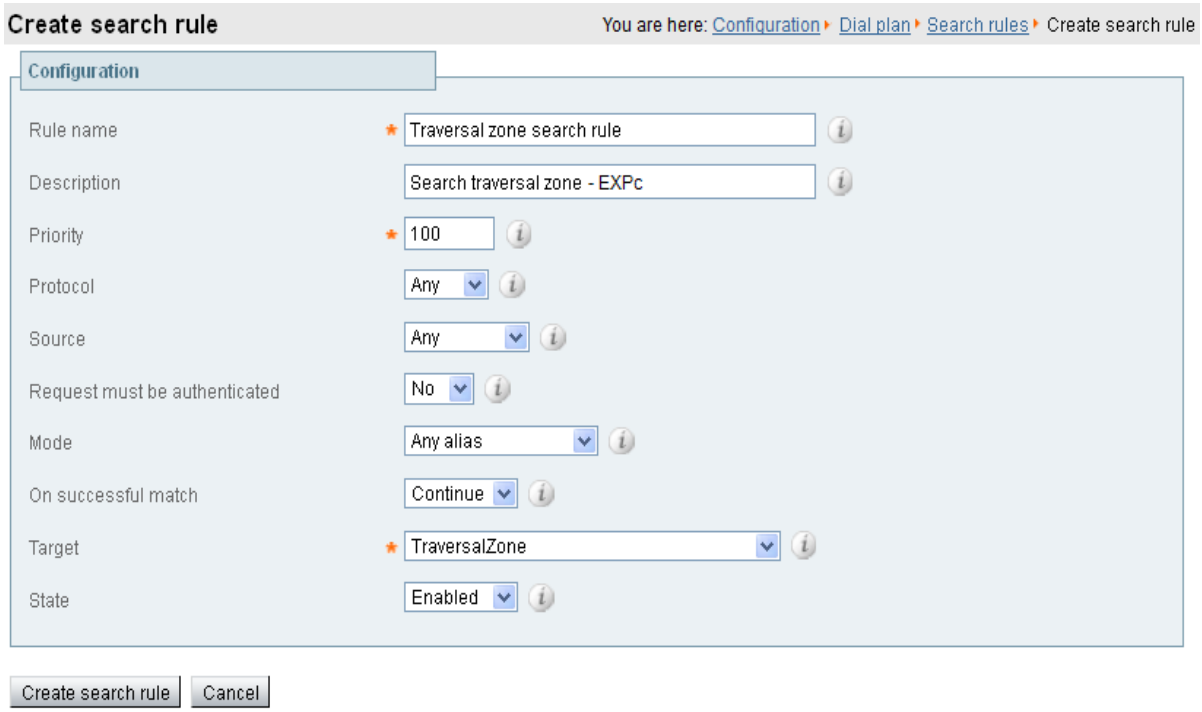
3. Configure the fields as follows:

	Expressway-C	Expressway-E
Rule name	"Traversal zone search rule" for example	"Traversal zone search rule" for example
Description	"Search traversal zone - EXPe" for example	"Search traversal zone - EXPc" for example
Priority	100	100
Protocol	*Any*	*Any*
Source	*Any*	*Any*
Request must be authenticated	*No*	*No*
Mode	*Any alias*	*Any alias*
On successful match	*Continue*	*Continue*
Target	*Traversal zone*	*Traversal zone*
State	*Enabled*	*Enabled*

4. Click **Create search rule**.



Expressway-C



Expressway-E

Task 9: Configuring the DNS zone

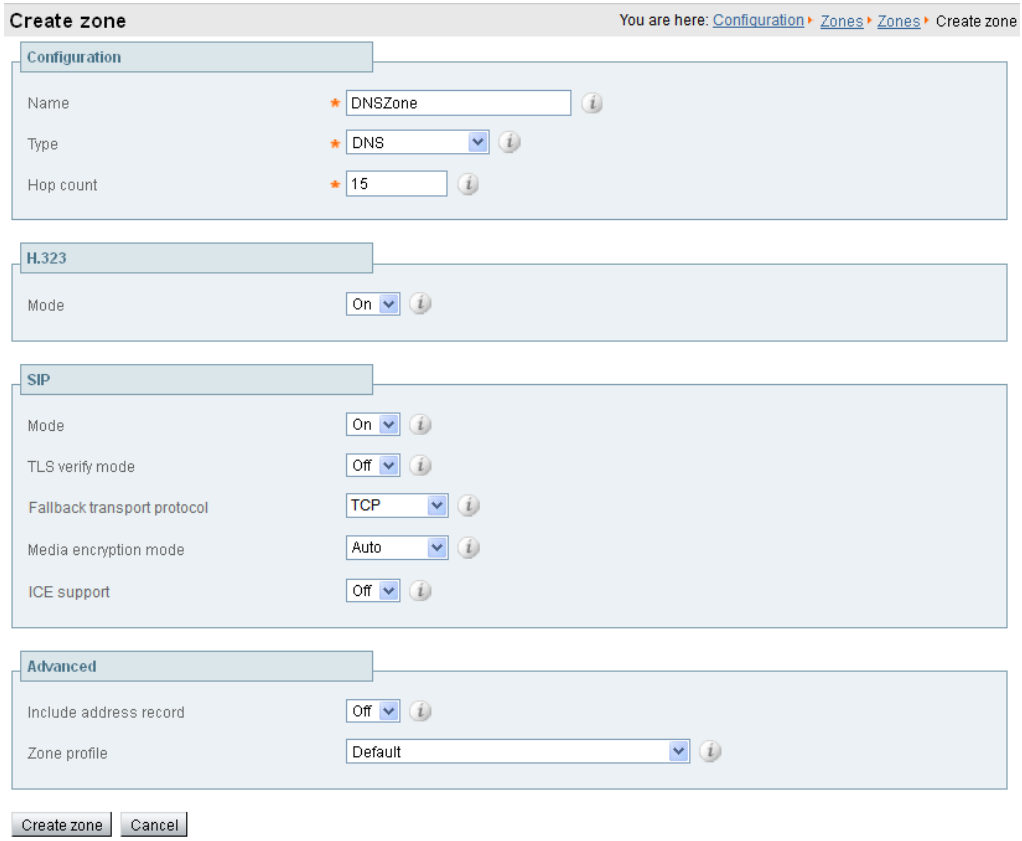
The DNS zone is used to search for externally hosted systems (such as for business to business calling). Destination aliases are searched for by a name using a DNS lookup.

To configure the DNS zone:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

	Expressway-C	Expressway-E
Name	Not applicable	Enter `DNSZone` for example
Type	Not applicable	*DNS*
H.323 Mode	Not applicable	*On*
SIP Mode	Not applicable	*On*
Fallback transport protocol	Not applicable	*TCP*
Include address record	Not applicable	*Off*

4. Click **Create zone**.



Task 10: Configuring DNS zone search rules

The DNS search rule defines when the DNS zone should be searched.

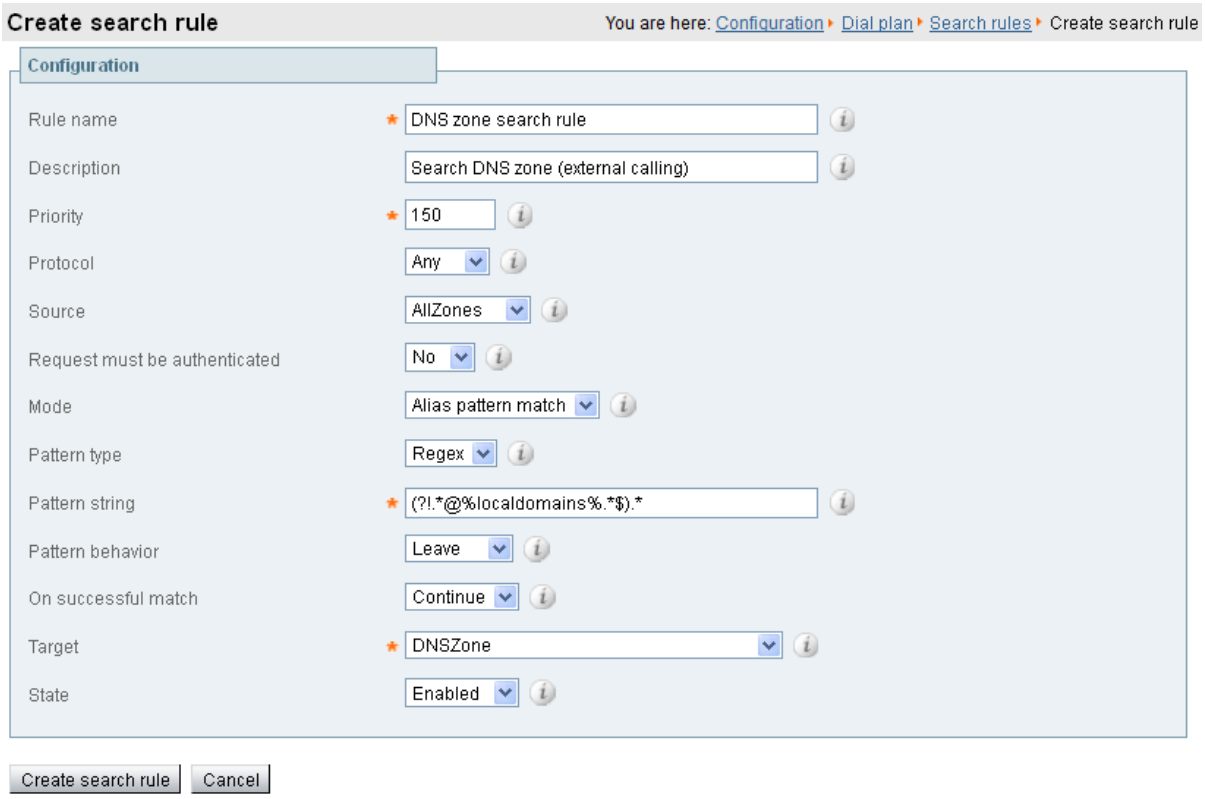
A specific regular expression is configured which will prevent searches being made using the DNS zone (i.e. on the public internet) for destination addresses (URIs) using any SIP domains which are configured on the local network (local domains).

To create the search rules to route via DNS:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows:

	Expressway-C	Expressway-E
Rule name	Not applicable	Enter `DNS zone search rule` for example
Description	Not applicable	Enter `Search DNS zone (external calling)` for example
Priority	Not applicable	`150`
Protocol	Not applicable	*Any*
Source	Not applicable	*All zones*
Request must be authenticated	Not applicable	*No*
Mode	Not applicable	*Alias pattern match*
Pattern type	Not applicable	*Regex*
Pattern string	Not applicable	Enter `(?!.*@%localdomains%.*$).*`
Pattern behavior	Not applicable	*Leave*
On successful match	Not applicable	*Continue*
Target	Not applicable	*DNSZone*
State	Not applicable	*Enabled*

4. Click **Create search rule**.



Note that the regular expression used to prevent local domains being searched via the DNS zone can be broken down into the following components:

(.*) = match all pattern strings

(?!.*@%localdomains%.*$).* = do not match any pattern strings ending in @localdomains

In the deployment example, calls destined for @cisco.com would be searched via the DNS zone, whereas calls destined for @example.com would not.

Task 11: Configuring external (unknown) IP address routing

The following configuration defines how an Expressway routes calls (and other requests) to external IP addresses. An external IP address is an IP address which is not 'known' to the Expressway and therefore assumed to be a publicly routable address.

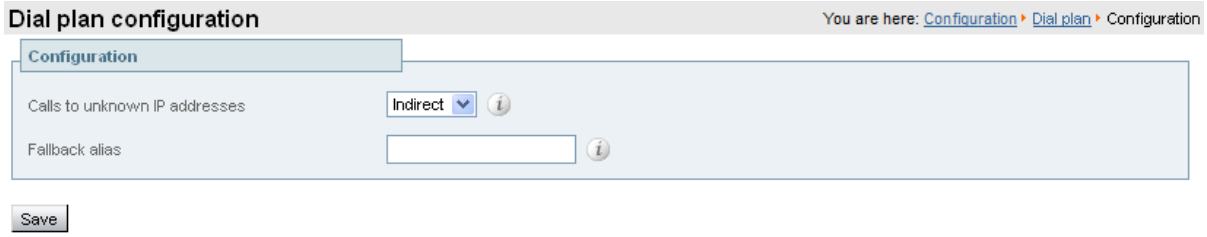
- All requests destined for external IP addresses, originating at the Expressway-C are routed to the Expressway-E using a search rule.
- The Expressway-E then attempts to open a connection directly to the IP address.

To configure how the Expressway will handle calls to unknown IP addresses:

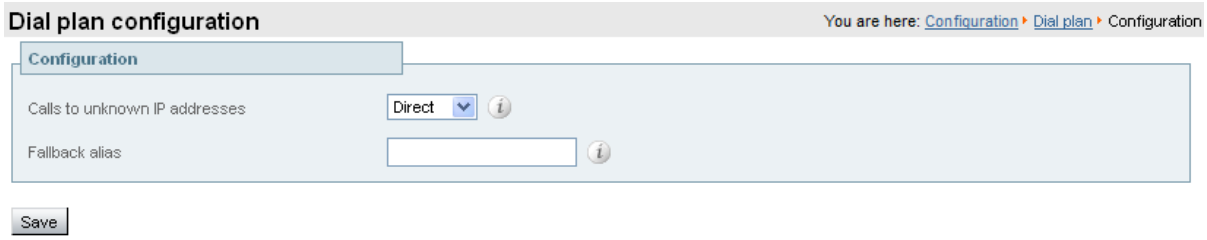
1. Go to **Configuration > Dial plan > Configuration**.
2. Configure the fields as follows:

	Expressway-C	Expressway-E
Calls to unknown IP addresses	*Indirect*	*Direct*

3. Click **Save**.



Expressway-C



Expressway-E

To create the search rules to route calls to IP addresses to the Expressway-E:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows:

	Expressway-C	Expressway-E
Rule name	Enter `External IP address search rule`	Not applicable
Description	Enter `Route external IP address`	Not applicable
Priority	Enter `100`	Not applicable
Protocol	*Any*	Not applicable
Source	*Any*	Not applicable
Request must be authenticated	*No*	Not applicable
Mode	*Any IP address*	Not applicable
On successful match	*Continue*	Not applicable
Target	*Traversal Zone*	Not applicable
State	*Enabled*	Not applicable

4. Click **Create search rule**.

Create search rule

You are here: Configuration ▸ Dial plan ▸ Search rules ▸ Create search rule

Configuration

Rule name *	External IP address search rule
Description	Route external IP address
Priority *	100
Protocol	Any
Source	Any
Request must be authenticated	No
Mode	Any IP address
On successful match	Continue
Target *	TraversalZone
State	Enabled

Create search rule | Cancel

System checks

Zone status

Go to **Status > Zones** on both Expressway-C and Expressway-E to check that the traversal zone is **Active**. You can also check the zone status via **Configuration > Zones > Zones**.

If the traversal zone is not active:

- Review the traversal zone configuration.
- Confirm that the relevant ports are enabled for outbound routing on the NAT and firewall devices located between the Expressway-C and Expressway-E (see Appendix 3: Firewall and NAT settings [p.42]).
- Confirm that the username and password credentials are configured correctly (and match) on Expressway-C and Expressway-E traversal zones and in the authentication database on the Expressway-E.

Call signaling

If calls do not complete:

- Review the Expressway-C search rule configuration.
- Review the Expressway-E search rule configuration.
- Check the search history page for search attempts and failures (**Status > Search history**).
- Check the Event Log for call connection failure reasons (**Status > Logs > Event Log**).

Maintenance routine

Creating a system backup

To create a backup of Expressway system data:

1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file.
   If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format:
   <software version>_<hardware serial number>_<date>_<time>_backup.tar.gz.
   (The file extension is normally **.tar.gz.enc** if an encryption password is specified. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be **.tar.gz.gz** by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)
   The preparation of the system backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
5. Save the file to a designated location.

Log files are not included in the system backup file.

Optional configuration tasks

Task 12: Configuring routes to a neighbor zone (optional)

You can optionally set up neighbor zones and associated search rules on the Expressway-C if you need to route calls to other systems such as a Cisco VCS or Unified CM.

Example: Cisco VCS neighbor zone

For example, you may want to route calls towards devices (typically H.323 devices) that are registered to a Cisco VCS. In this example, the devices that are registered to Cisco VCS have an address (destination alias) in the format <alias>@vcs.domain. (Note that you may need additional rules or transforms if the H.323 devices have registered E.164 numbers or H.323 IDs without a domain portion).

To configure a neighbor zone to the Cisco VCS:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

	Expressway-C	Expressway-E
Name	Enter `Neighbor zone to VCS`	Not applicable
Type	*Neighbor*	
H.323 Mode	*On*	
H.323 Port	Enter `1719`	
SIP Mode	*On*	
SIP Port	Enter `5061`	
SIP Transport	*TCP*	
Location Peer 1 address	Enter the address of the Cisco VCS neighbor system	

4. Click **Create zone**.

To configure the search rule to route calls to the Cisco VCS:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the search rule fields as follows:

	Expressway-C	Expressway-E
Rule name	Enter `Route to VCS`	Not applicable
Description	Enter `Search VCS neighbor zone`	
Priority	Enter `100`	
Protocol	*Any*	
Source	*Any*	
Request must be authenticated	*No*	
Mode	*Alias pattern match*	
Pattern type	*Suffix*	
Pattern string	Enter `@vcs.domain`	
Pattern behavior	*Leave*	
On successful match	*Continue*	
Target	*Neighbor zone to VCS*	
State	*Enabled*	

4. Click **Create search rule**.

SIP trunks to Unified CM

To configure a SIP trunk to Unified CM, see *Cisco Unified Communications Manager with Expressway Deployment Guide*.

Task 13: Configuring logging (optional)

The following configuration will enable event logs to be sent to an external logging server (using the SYSLOG protocol).

- The **Log level** controls the granularity of event logging. 1 is the least verbose, 4 the most.
- A minimum log level of 2 is recommended, as this level provides both system and basic signaling message logging.

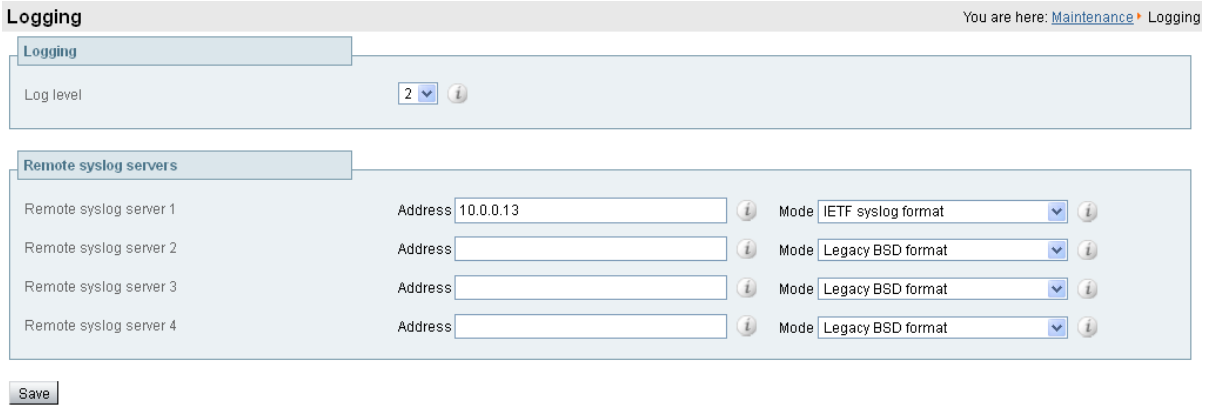
Expressway-E external logging server configuration requires additional firewall / NAT configuration – See Appendix 3: Firewall and NAT settings [p.42].

To configure a logging server:

1. Go to **Maintenance > Logging**.
2. Configure the fields as follows:

	Expressway-C	Expressway-E
Log level	*2*	*2*
Remote syslog server 1: Address	Enter `10.0.0.13`	Enter `10.0.0.13`
Remote syslog server 1: Mode	*IETF syslog format*	*IETF syslog format*

3. Click **Save**.



Task 14: Restricting access to ISDN gateways (optional)

Expressway users are recommended to take appropriate action to restrict unauthorized access to any ISDN gateway resources (also known as toll-fraud prevention). This optional step shows some methods in which this can be achieved.

In these examples, an ISDN gateway is a neighbour zone that routes calls starting with a 9.

Expressway-E

Two search rules are created on the Expressway-E:

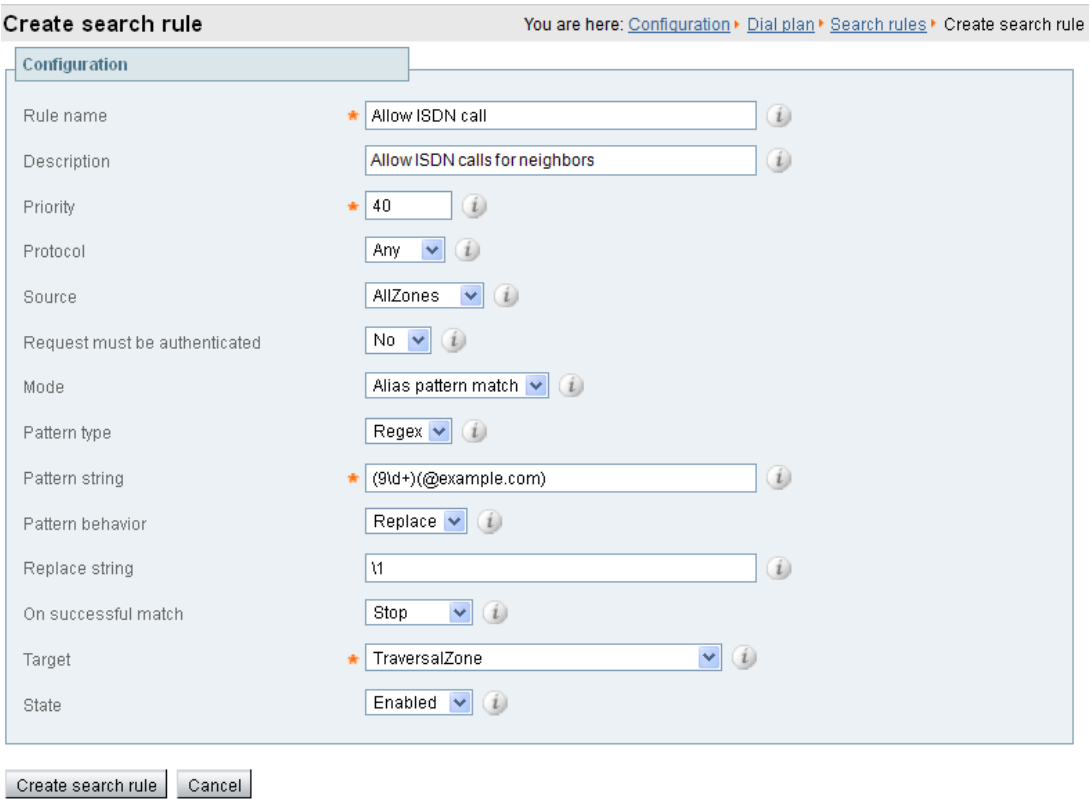
- both search rules have a pattern string that matches calls directed at the ISDN gateway — in this example, calls that are prefixed by a 9
- the first rule has a **Source** of *All zones*; this allows calls from neighbor zones to be passed through to the traversal zone
- the second rule is similar to the first rule but has a **Source** of *All*; this means that non-registered endpoints (which are excluded from the previous rule) are included by this rule and can be stopped by defining the **Replace string** as "do-not-route-this-call"
- both rules stop any further search rules from being looked at (**On successful match** = *Stop*).

To create the search rules:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows:

	Expressway-E
Rule name	Enter `Allow ISDN call` for example
Description	Enter `Allow ISDN calls for neighbors`
Priority	Enter `40` (these rules must be the highest priority in the search rule configuration)

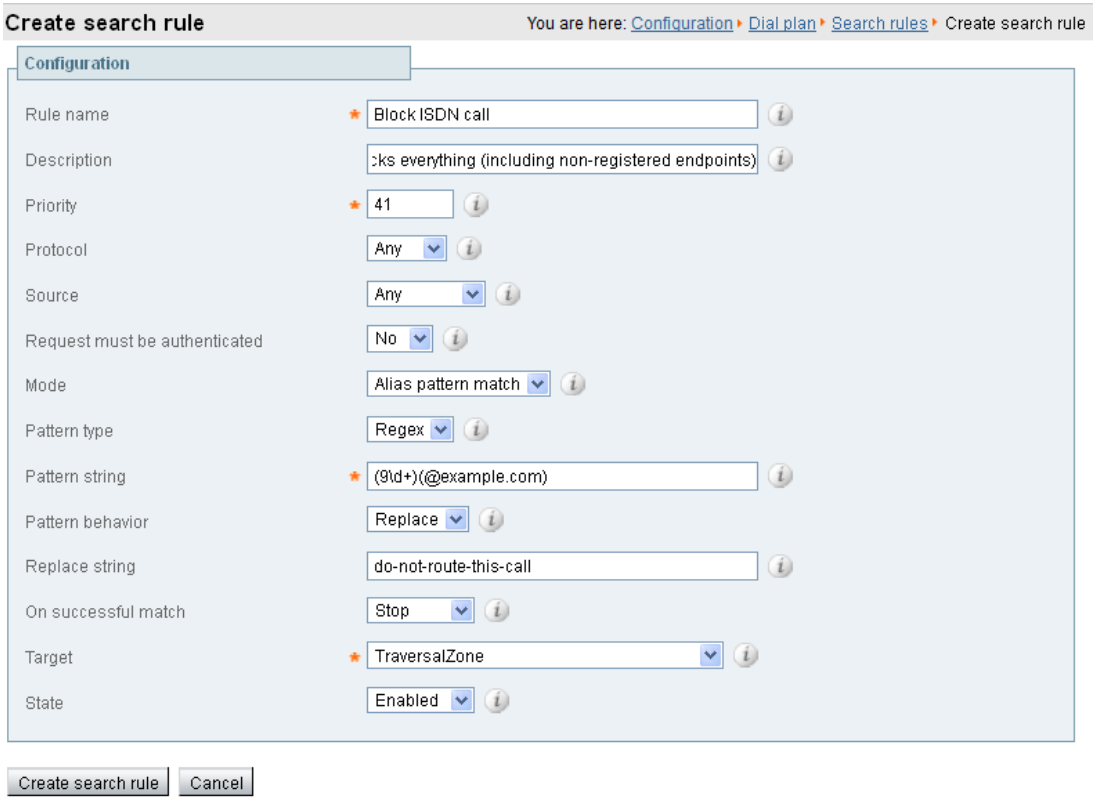
	Expressway-E
Protocol	*Any*
Source	*All zones*
Request must be authenticated	*No*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	Enter `(9\d+)(@example.com)`
Pattern behavior	*Replace*
Replace string	Enter `\1`
On successful match	*Stop*
Target	*TraversalZone*
State	*Enabled*



4. Click **Create search rule**.
5. Click **New**.
6. Configure the fields as follows:

	Expressway-E
Rule name	Enter `Block ISDN call` for example

	Expressway-E
Description	Enter `Blocks everything (including non-registered endpoints)`
Priority	Enter `41`
Protocol	*Any*
Source	*Any*
Request must be authenticated	*No*
Mode	*Alias pattern match*
Pattern type	*Regex*
Pattern string	Enter `(9\d+)(@example.com)`
Pattern behavior	*Replace*
Replace string	Enter `do-not-route-this-call` for example
On successful match	*Stop*
Target	*TraversalZone*
State	*Enabled*



7. Click **Create search rule**.

Expressway-C

This example shows how to configure the Expressway-C to stop calls coming in via the gateway from being able to route calls back out of the gateway. This is done by loading some specially constructed CPL onto the Expressway-C and configuring its **Call policy mode** to use *Local CPL*.

Creating a CPL file

The CPL file to be uploaded onto the Expressway can be created in a text editor.

Here are 2 example sets of CPL. In these examples the “GatewayZone” is the neighbour zone to the ISDN gateway:

This example CPL excludes any checking of whether the calling party is authenticated or not:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!--Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not send calls back out of this gateway -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>
```

This example CPL also ensures that the calling party is authenticated:

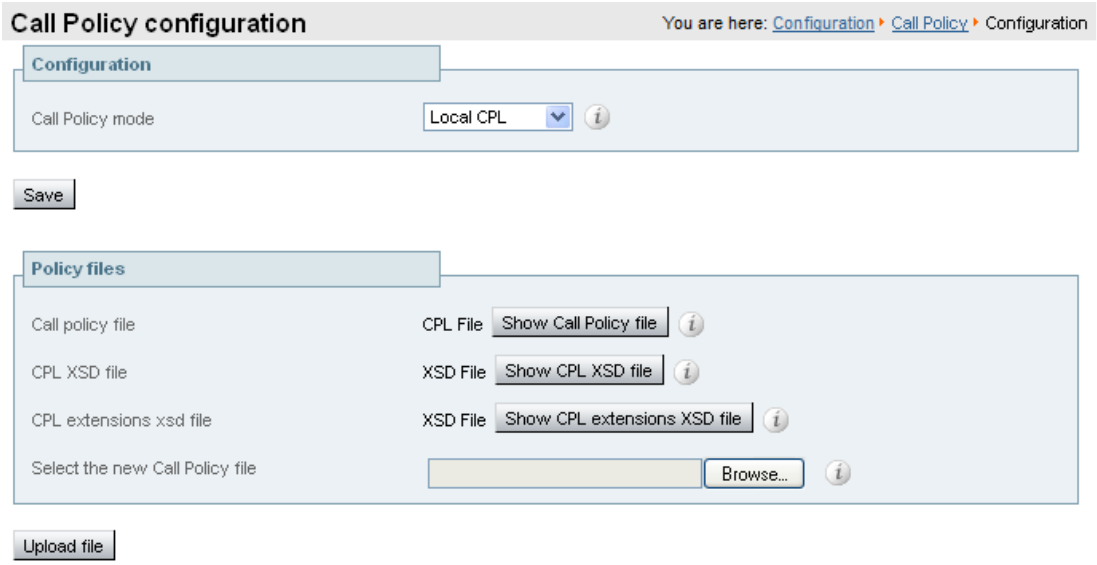
```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!-- Check that calling party is authenticated -->
    <taa:rule authenticated-origin="" destination="9.*">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN call denied as unauthenticated caller"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
```

```
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>
```

Loading the CPL onto Expressway-C

To configure the Expressway-C to use the CPL:

1. Go to **Configuration > Call Policy > Configuration**.
2. Click **Browse...** and select your CPL file (created above) from your file system.
3. Click **Upload file**.
   - You should receive a "File upload successful" message.
   - If you receive an "XML invalid" message then you must correct the problems with the CPL file and upload it again.
4. Select a **Call policy mode** of *Local CPL*.
5. Click **Save**.



Appendix 1: Configuration details

This appendix summarizes the configuration required for the Expressway-C and Expressway-E. It is broken down into 3 sections:

- Expressway-C (configuration to apply to the Expressway-C only)
- Expressway-E (configuration to apply to the Expressway-E only)
- Expressway-C and Expressway-E (configuration to apply to both the Expressway-C and Expressway-E)

Expressway-C configuration details

Configuration item	Value	Expressway page
System configuration		
System name	EXPc	System > Administration
LAN1 IPv4 address	10.0.0.2	System > IP
IPv4 gateway	10.0.0.1	System > IP
LAN1 subnet mask	255.255.255.0	System > IP
DNS server address 1	10.0.0.11	System > DNS
DNS server address 2	10.0.0.12	System > DNS
DNS Domain name	internal-domain.net	System > DNS
DNS System host name	expc	System > DNS
NTP server 1	pool.ntp.org	System > Time
Time zone	GMT	System > Time
Traversal zone		
Zone Name	TraversalZone	Configuration > Zones > Zones
Zone Type	Traversal client	Configuration > Zones > Zones
Protocol SIP port	7001	Configuration > Zones > Zones
Protocol H.323 port	6001	Configuration > Zones > Zones
Location Peer 1 address	192.0.2.2	Configuration > Zones > Zones
Authentication username	exampleauth	Configuration > Zones > Zones
Authentication password	ex4mpl3.c0m	Configuration > Authentication > Devices > Local database
Traversal search rule		
Rule name	Traversal zone search rule	Configuration > Dial plan > Search rules
Description	Search traversal zone (Expressway-C)	Configuration > Dial plan > Search rules
Priority	100	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Any alias	Configuration > Dial plan > Search rules

Configuration item	Value	Expressway page
On successful match	Continue	Configuration > Dial plan > Search rules
Target	TraversalZone	Configuration > Dial plan > Search rules
Direct IP search rule		
Rule name	External IP address search rule	Configuration > Dial plan > Search rules
Description	Route external IP address	Configuration > Dial plan > Search rules
Priority	100	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Any IP address	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	TraversalZone	Configuration > Dial plan > Search rules
IP call routing		
Calls to unknown IP addresses	Indirect	Configuration > Dial plan > Configuration

Expressway-E configuration details

Configuration item	Value	Expressway page
System configuration		
System name	EXPe	System > Administration
LAN1 IPv4 address	192.0.2.2	System > IP
IPv4 gateway	192.0.2.1	System > IP
LAN1 subnet mask	255.255.255.0	System > IP
DNS server address 1	194.72.6.57	System > DNS
DNS server address 2	194.73.82.242	System > DNS
DNS Domain name	example.com	System > DNS
DNS System host name	expe	System > DNS
NTP server 1	pool.ntp.org	System > Time
Time zone	GMT	System > Time
Traversal zone		
Zone Name	TraversalZone	Configuration > Zones > Zones
Zone Type	Traversal server	Configuration > Zones > Zones
Client authentication username	exampleauth	Configuration > Zones > Zones
Protocol SIP port	7001	Configuration > Zones > Zones
Protocol H.323 port	6001	Configuration > Zones > Zones

Configuration item	Value	Expressway page
Name	exampleauth	Configuration > Authentication > Devices > Local database
Password	ex4mpl3.c0m	Configuration > Authentication > Devices > Local database
Traversal zone search rule		
Rule name	Traversal zone search rule	Configuration > Dial plan > Search rules
Description	Search traversal zone (Expressway-E)	Configuration > Dial plan > Search rules
Priority	100	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Any alias	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	TraversalZone	Configuration > Dial plan > Search rules
DNS zone		
Zone Name	DNSZone	Configuration > Zones
Zone Type	DNS	Configuration > Zones > Zones
DNS zone search rule		
Rule name	DNS zone search rule	Configuration > Dial plan > Search rules
Zone name	Search DNS zone (external DNS)	Configuration > Dial plan > Search rules
Priority	150	Configuration > Dial plan > Search rules
Source	All zones	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	((?!*@%localdomains%$).*)	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	DNSZone	Configuration > Dial plan > Search rules
IP call routing		
Calls to unknown IP addresses	Direct	Configuration > Dial plan > Configuration

Expressway-C and Expressway-E configuration details

Configuration item	Value	Expressway page
Transform		
Pattern string	([^@]*)	Configuration > Dial plan > Transforms
Pattern type	Regex	Configuration > Dial plan > Transforms

Configuration item	Value	Expressway page
Pattern behavior	Replace	Configuration > Dial plan > Transforms
Replace string	\1@example.com	Configuration > Dial plan > Transforms
Local search rule 1		
Rule name	Local zone – no domain	Configuration > Dial plan > Search rules
Priority	48	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+)@example.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Replace	Configuration > Dial plan > Search rules
Replace string	\1	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules
Local search rule 2		
Rule name	Local zone – full URI	Configuration > Dial plan > Search rules
Priority	50	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+)@example.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Leave	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules

Appendix 2: DNS records

DNS configuration on host server

The following records are required in the external DNS which hosts the externally routable domain: example.com to allow messages from non-registered endpoints (or other infrastructure devices) to be routed to the Expressway-E

Host DNS A record

Host	Host IP address
expe.example.com	192.0.2.2

DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
example.com.	h323cs	tcp	10	10	1720	expe.example.com.
example.com.	h323ls	udp	10	10	1719	expe.example.com.
example.com.	sip	tcp	10	10	5060	expe.example.com.
example.com.	sip	udp *	10	10	5060	expe.example.com.
example.com.	sips	tcp	10	10	5061	expe.example.com.
example.com.	turn	udp	10	10	3478 **	expe.example.com.

* SIP UDP is disabled on Expressway by default.

** On Large VM server deployments you should configure multiple records for the range 3478 – 3483.

For example, the DNS records would be:

```
_h323cs._tcp.example.com. 86400 IN SRV 10 10 1720 expe.example.com.
_h323ls._udp.example.com. 86400 IN SRV 10 10 1719 expe.example.com.
_sip._tcp.example.com.    86400 IN SRV 10 10 5060 expe.example.com.
_sip._udp.example.com.    86400 IN SRV 10 10 5060 expe.example.com.
_sips._tcp.example.com.   86400 IN SRV 10 10 5061 expe.example.com.
_turn._udp.example.com.   86400 IN SRV 10 10 3478 expe.example.com.
expe.example.com.         86400 IN A 192.0.2.2
```

If you have a cluster of Expressway-Es, you must set up DNS A and SRV records for each peer/host in the cluster. See *Expressway Cluster Creation and Maintenance Deployment Guide* for more information.

DNS configuration (internal DNS server)

The following records are required in the local DNS which hosts the internally routable domain: internal-domain.net to allow internal messages to be routed to the Expressway-C.

Local DNS A record

Host	Host IP address
expc.internal-domain.net	10.0.0.2

Local DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
internal-domain.net.	h323cs	tcp	10	10	1720	expc.internal-domain.net.
internal-domain.net.	h323ls	udp	10	10	1719	expc.internal-domain.net.
internal-domain.net.	sip	tcp	10	10	5060	expc.internal-domain.net.
internal-domain.net.	sip	udp *	10	10	5060	expc.internal-domain.net.
internal-domain.net.	sips	tcp	10	10	5061	expc.internal-domain.net.

* SIP UDP is disabled on Expressway by default.

For example, the DNS records would be:

```
_h323cs._tcp.internal-domain.net. 86400 IN SRV 10 10 1720 expc.internal-domain.net.
_h323ls._udp.internal-domain.net. 86400 IN SRV 10 10 1719 expc.internal-domain.net.
_sip._tcp.internal-domain.net.    86400 IN SRV 10 10 5060 expc.internal-domain.net.
_sip._udp.internal-domain.net.    86400 IN SRV 10 10 5060 expc.internal-domain.net.
_sips._tcp.internal-domain.net.   86400 IN SRV 10 10 5061 expc.internal-domain.net.
expc.internal-domain.net.         86400 IN A 10.0.0.2
```

If you have a cluster of Expressway-Cs, you must set up DNS A and SRV records for each peer/host in the cluster. See *Expressway Cluster Creation and Maintenance Deployment Guide* for more information.

Appendix 3: Firewall and NAT settings

Internal firewall configuration

In many deployments outbound connections (from internal network to DMZ) will be permitted by the NAT/firewall device. If the administrator wants to restrict this further, the following tables provide the permissive rules required. For further information, see *Expressway IP Port Usage for Firewall Traversal*.

Ensure that any SIP or H.323 'fixup' ALG or awareness functionality is disabled on the NAT firewall – if enabled this will adversely interfere with the Expressway functionality.

Outbound (Internal network > DMZ)

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
Management	Management computer	EXPe	As required	>=1024	TCP	192.0.2.2	80 / 443 / 22 / 23
SNMP monitoring	Management computer	EXPe	As required	>=1024	UDP	192.0.2.2	161
H.323 traversal calls using Assent							
Q.931/H.225 and H.245	EXPc	EXPe	Any	15000 to 19999	TCP	192.0.2.2	2776
RTP Assent	EXPc	EXPe	Any	36002 to 59999 *	UDP	192.0.2.2	36000 *
RTCP Assent	EXPc	EXPe	Any	36002 to 59999 *	UDP	192.0.2.2	36001 *
SIP traversal calls							
SIP TCP/TLS	EXPc	EXPe	10.0.0.2	25000 to 29999	TCP	192.0.2.2	Traversal zone ports, e.g. 7001
RTP Assent	EXPc	EXPe	10.0.0.2	36002 to 59999 *	UDP	192.0.2.2	36000 *
RTCP Assent	EXPc	EXPe	10.0.0.2	36002 to 59999 *	UDP	192.0.2.2	36001 *

* The default media port range is 36000 to 59999. The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

Inbound (DMZ > Internal network)

As Expressway-C to Expressway-E communications are always initiated from the Expressway-C to the Expressway-E (Expressway-E sending messages by responding to Expressway-C's messages) no ports need to be opened from DMZ to Internal for call handling.

However, if the Expressway-E needs to communicate with local services, such as a Syslog server, some of the following NAT configurations may be required:

Purpose	Source	Destination	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
Logging	EXPe	Syslog server	192.0.2.2	30000 to 35999	UDP	10.0.0.13	514
Management	EXPe	Cisco TMS server	192.0.2.2	>=1024	TCP	10.0.0.14	80 / 443
LDAP (for log in, if required)	EXPe	LDAP server	192.0.2.2	30000 to 35999	TCP		389 / 636
NTP (time sync)	EXPe	Local NTP server	192.0.2.2	123	UDP		123
DNS	EXPe	Local DNS server	192.0.2.2	>=1024	UDP		53

Traffic destined for logging or management server addresses (using specific destination ports) must be routed to the internal network.

External firewall configuration requirement

In this example it is assumed that outbound connections (from DMZ to external network) are all permitted by the firewall device.

Ensure that any SIP or H.323 "fixup" ALG or awareness functionality is disabled on the NAT firewall – if enabled this will adversely interfere with the Expressway functionality.

Inbound (Internet > DMZ)

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
H.323 calls using Assent							
Q.931/H.225 and H.245	Endpoint	EXPe	Any	>=1024	TCP	192.0.2.2	2776
RTP Assent	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	36000
RTCP Assent	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	36001
H.323 endpoints with public IP addresses							
Q.931/H.225	Endpoint	EXPe	Any	>=1024	TCP	192.0.2.2	1720
H.245	Endpoint	EXPe	Any	>=1024	TCP	192.0.2.2	15000 to 19999
RTP & RTCP	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	36002 to 59999
SIP endpoints using UDP / TCP or TLS							
SIP TCP	Endpoint	EXPe	Any	>=1024	TCP	192.0.2.2	5060
SIP UDP	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	5060
SIP TLS	Endpoint	EXPe	Any	>=1024	TCP	192.0.2.2	5061

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
RTP & RTCP	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	36002 to 59999
TURN server control	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	3478 **
TURN server media	Endpoint	EXPe	Any	>=1024	UDP	192.0.2.2	24000 to 29999

** On Large VM server deployments you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

Outbound (DMZ > Internet)

If you want to restrict communications from the DMZ to the wider Internet, the following table provides information on the outgoing IP addresses and ports required to permit the Expressway-E to provide service to external endpoints.

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
H.323 endpoints with public IP address							
Q.931/H.225	EXPe	Endpoint	192.0.2.2	15000 to 19999	TCP	Any	1720
H.245	EXPe	Endpoint	192.0.2.2	15000 to 19999	TCP	Any	>=1024
RTP & RTCP	EXPe	Endpoint	192.0.2.2	36000 to 59999	UDP	Any	>=1024
SIP endpoints using UDP / TCP or TLS							
SIP TCP & TLS	EXPe	Endpoint	192.0.2.2	25000 to 29999	TCP	Any	>=1024
SIP UDP	EXPe	Endpoint	192.0.2.2	5060	UDP	Any	>=1024
RTP & RTCP	EXPe	Endpoint	192.0.2.2	36000 to 59999	UDP	Any	>=1024
TURN server media	EXPe	Endpoint	192.0.2.2	24000 to 29999	UDP	Any	>=1024
Other services (as required)							
DNS	EXPe	DNS server	192.0.2.2	>=1024	UDP	DNS servers	53
NTP (time sync)	EXPe	NTP server	192.0.2.2	123	UDP	NTP servers	123

Appendix 4: Advanced network deployments

This section discusses network deployments that use static NAT or Dual Network Interface architectures.

Prerequisites

Deploying an Expressway-E behind a NAT **mandates** the use of the **Advanced Networking** option key. It enables the static NATing functionality of the Expressway-E as well as dual network interfaces. Although certain call scenarios involving an Expressway-E behind NAT could potentially work with the help of router/firewall-based ALGs, proper functionality cannot be guaranteed; you must use the Expressway to perform the static NATing on its own interface. More background on this can be found in the Routers/firewalls with SIP/H.323 ALG [p.49] section later in this appendix. The **Advanced Networking** option is available only on the Expressway-E.

When deploying an Expressway-E behind a NAT with static NAT configuration in place on the Expressway-E, it is highly recommended to disable SIP and H.323 ALGs (SIP / H.323 awareness) on routers/firewalls carrying network traffic to or from the Expressway-E (experience shows that these tend to be unable to handle video traffic properly).

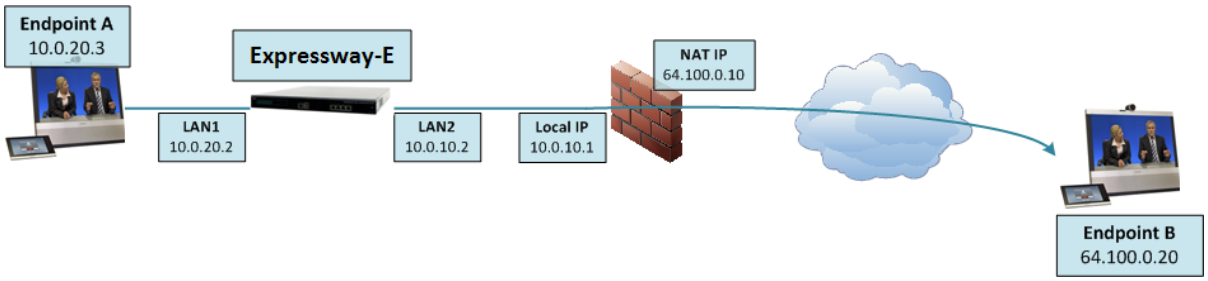
Background

When deploying an Expressway-E for business to business communications, or for supporting home workers and travelling workers, it is usually desirable to deploy the Expressway-E in a NATed DMZ rather than having the Expressway-E configured with a publicly routable IP address.

Network Address Translation (NAT) poses a challenge with SIP and H.323 applications, as with these protocols, IP addresses and port numbers are not only used in OSI layer 3 and 4 packet headers, but are also referenced within the packet payload data of H.323 and SIP messages themselves.

This usually breaks SIP/H.323 call signaling and RTP media packet flows, since NAT routers/firewalls will normally translate the IP addresses and port numbers of the headers, but leave the IP address and port references within the SIP and H.323 message payloads unchanged.

To provide an example of this, assume you have an Expressway-E deployed behind a NAT router and two endpoints. The Expressway-E has static NAT disabled on LAN2, but the NAT router is configured with a static 1:1 NAT, NATing the public address 64.100.0.10 to the Expressway-E LAN2 IP address 10.0.10.2:



- NAT router with local IP address 10.0.10.1 and NAT IP address 64.100.0.10, statically NATed to 10.0.10.2
- Expressway-E LAN1 (internally-facing interface) with IP address 10.0.20.2
- Expressway-E LAN2 (externally-facing interface) with IP address 10.0.10.2 (and with static NAT disabled)
- Expressway-E default gateway set to 10.0.10.1 (inside address of NAT firewall, reachable via LAN2)

- Endpoint A with IP address 10.0.20.3
- Endpoint B with IP address 64.100.0.20, located on the Internet

Assume that endpoint A places a SIP call towards endpoint B. The call will arrive at the Expressway-E, which will proxy the SIP INVITE towards endpoint B. The Expressway-E to Endpoint B will then be a traversal call, which means that the Expressway-E will take both signaling and media, and the packet carrying the SIP INVITE message will have the following contents as it arrives at the NAT router (the actual INVITE contents have been simplified for ease of reading):

```
Packet header:
Source IP: 10.0.10.2
Destination IP: 64.100.0.20
SIP payload:
INVITE sip: 64.100.0.20 SIP/2.0
Via: SIP/2.0/TLS 10.0.10.2:5061
Via: SIP/2.0/TLS 10.0.20.3:55938
Call-ID: 20ec9fd084eb3dd2@127.0.0.1
CSeq: 100 INVITE
Contact: <sip:EndpointA@10.0.20.3:55938;transport=tls>
From: "Endpoint A" <sip:EndpointA@cisco.com>;tag=9a42af
To: <sip: 64.100.0.20>
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 2825

v=0
o=tandberg 1 2 IN IP4 10.0.10.2
s=-
c=IN IP4 10.0.10.2
b=AS:2048
…
…
…
```

Figure 3: SIP INVITE arriving at NAT router

In the example above, the SDP (session description protocol) within the SIP payload contains a reference to the Expressway-E IP address, marked in yellow: **`c=IN IP4 10.0.10.2`**.

Upon receiving the SIP INVITE packet, the NAT router will rewrite the layer 3 source IP address header (marked in green: **`10.0.10.2`**) and replace 10.0.10.2 (Expressway-E LAN2 IP address) with its own public NAT address (**`64.100.0.10`**) and route the packet out to the Internet, so that the SIP INVITE message will have the following contents as it arrives at endpoint B:

```
Packet header:
Source IP: 64.100.0.10
Destination IP: 64.100.0.20
SIP payload:
INVITE sip:64.100.0.20 SIP/2.0
Via: SIP/2.0/TLS 10.0.10.2:5061
Via: SIP/2.0/TLS 10.0.20.3:55938
Call-ID: 20ec9fd084eb3dd2@127.0.0.1
CSeq: 100 INVITE
Contact: <sip:EndpointA@10.0.20.3:55938;transport=tls>
From: "Endpoint A" <sip:EndpointA@cisco.com>;tag=9a42af
To: <sip:64.100.0.20>
```

```
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 2825

v=0
s=-
c=IN IP4 10.0.10.2

b=AS:2048
…
…
…
```

Figure 4: SIP INVITE arriving at Endpoint B

As can be seen from the example above, endpoint B will see that the SIP INVITE was received from IP 64.100.0.10 (NAT router), so the endpoint will know where to send its reply messages for the INVITE itself.

The c-line within the SDP of the SIP INVITE is however still set to c=IN IP4 10.0.10.2, which means that endpoint B will attempt to send RTP media to the IP address 10.0.10.2, an address which is not routable on the Internet.

The result in this scenario will therefore be that endpoint A will never receive media sent by endpoint B (while endpoint B will normally receive media from endpoint A, since endpoint B is assigned with a publicly routable IP address).

Similar behavior will be seen in H.323 calls, since H.323 uses the same principles as SIP in terms of embedding IP address and port references within the message payload.

Solution

To ensure that call signaling and media connectivity remains functional in scenarios where the Expressway-E is deployed behind a NAT (as in the example above), the Expressway-E will have to modify the parts of SIP and H.323 messages which contain references to its actual LAN2 network interface IP address (10.0.10.2) and replace these with the public NAT address of the NAT router (64.100.0.10).

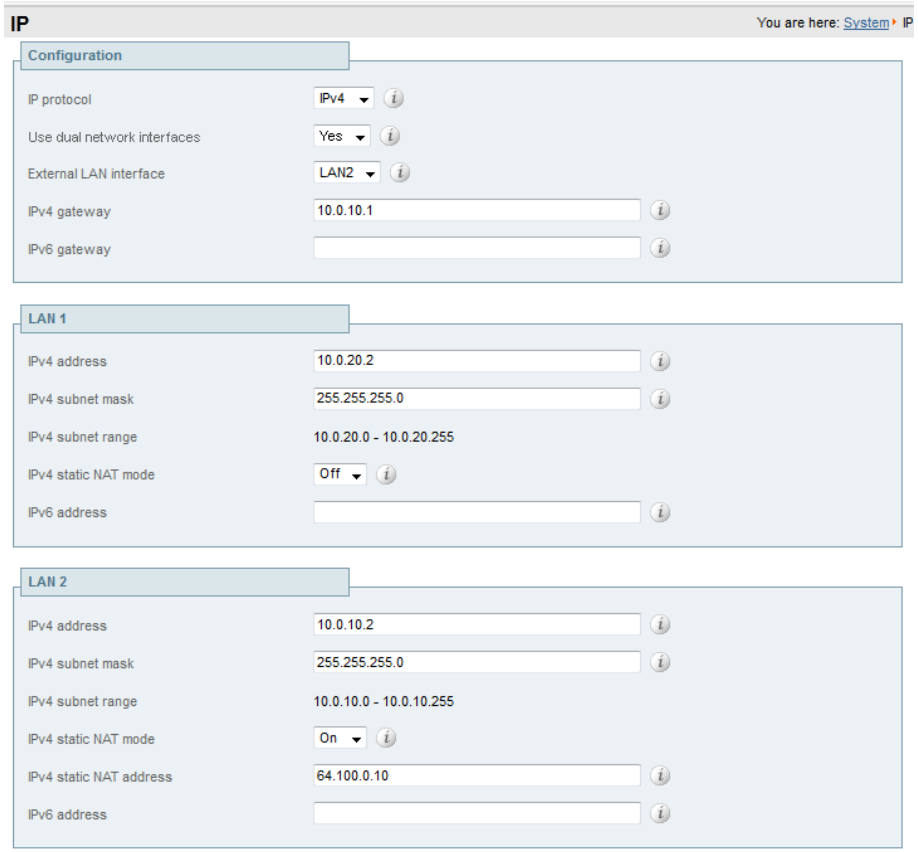
This can be achieved by enabling **Static NAT mode** on selected network interfaces on the Expressway-E. The Static NAT mode feature on the Expressway-E is made available with the **Advanced Networking** option key.

This option key allows the use of two network interfaces (LAN1 and LAN2) and for Static NAT mode to be enabled on one or both of these interfaces. It is not compulsory to use both interfaces; you may use only a single interface and have Static NAT mode enabled on that.

When static NAT has been enabled on an interface, the Expressway will apply static NAT for all outbound SIP and H.323 traffic for this interface, which means that H.323 and SIP devices have to communicate with this interface using the static NAT address rather than the local interface address.

When the **Advanced Networking** key is installed on the Expressway-E, the **IP** configuration page (**System > IP**) has additional options, allowing the user to decide whether to **Use dual network interfaces**, to nominate which interface is the **External LAN interface**, to enable **Static NAT mode** on selected interfaces and configure an **IPv4 static NAT address** for each interface.

Using the example deployment above, the Expressway-E would be configured as follows:



- Dual interfaces are selected and the external LAN interface is set to *LAN2*
- Configuration > IPv4 gateway is set to 10.0.10.1, the local IP address of the NAT router
- LAN1 > IPv4 address is set to 10.0.20.2
- LAN1 > IPv4 static NAT mode is set to *Off*
- LAN2 > IPv4 address is set to 10.0.10.2
- LAN2 > IPv4 static NAT mode is set to *On*
- LAN2 > IPv4 static NAT address is set to 64.100.0.10, the public NAT address of the NAT router

When enabling **IPv4 static NAT mode** on an interface (LAN2 in our example), the Expressway-E will modify the payload of H.323 and SIP messages sent out via this interface, so that references to the LAN2 interface address (10.0.10.2) are replaced with the IPv4 static NAT address configured for this interface (64.100.0.10). This means that when looking at the payload of SIP and H.323 messages sent out via this interface, it will appear as if the LAN2 interface has an IP address of 64.100.0.10.

It is important to note that the Expressway-E will not modify the layer 3 source address of outgoing H.323 and SIP packets sent out of this interface, as this will be done by the NAT router.

With this configuration in place, the SIP INVITE shown in Figure 4 will now look as follows as it arrives at endpoint B:

```
Packet header:
Source IP: 64.100.0.10
Destination IP: 64.100.0.20
SIP payload:
INVITE sip: 64.100.0.20 SIP/2.0
```

```
Via: SIP/2.0/TLS 10.0.10.2:5061
Via: SIP/2.0/TLS 10.0.20.3:55938
Call-ID: 20ec9fd084eb3dd2@127.0.0.1
CSeq: 100 INVITE
Contact: <sip:EndpointA@10.0.20.3:55938;transport=tls>
From: "Endpoint A" <sip:EndpointA@cisco.com>;tag=9a42af
To: <sip: 64.100.0.20>
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 2825

v=0
s=-
c=IN IP4 64.100.0.10

b=AS:2048
…
…
…
```

Figure 5: SIP INVITE arriving at Endpoint B - Static NAT mode enabled

With static NAT enabled on LAN2 of the Expressway-E, the c-line of the SIP INVITE has now been rewritten to c=IN IP4 64.100.0.10, and this means that when endpoint B sends outbound RTP media to endpoint A, this will be sent to IP address 64.100.0.10, the public NAT address of the NAT router, which is 1:1 NATed to the LAN2 IP address of the Expressway-E, 10.0.10.2. As RTP media from endpoint B arrives at the NAT router with a destination IP address of 64.100.0.10, the NAT router will forward these packets to the Expressway-E at 10.0.10.2 and two-way media is achieved.

Routers/firewalls with SIP/H.323 ALG

Some routers and firewalls have SIP and H.323 ALG capabilities. ALG is also referred to as Fixup, Inspection, Application Awareness, Stateful Packet Inspection, Deep Packet Inspection and so forth. This means that the router/firewall is able to identify SIP and H.323 traffic as it passes through and inspect, and in some cases modify, the payload of the SIP and H.323 messages. The purpose of modifying the payload is to help the H.323 or SIP application from which the message originated to traverse NAT, i.e. to perform a similar process to what the Expressway-E does.

The challenge with router/firewall-based SIP and H.323 ALGs is that these were originally intended to aid relatively basic H.323 and SIP applications to traverse NAT, and these applications had, for the most part, very basic functionality and often only supported audio.

Over the years, many H.323 and SIP implementations have become more complex, supporting multiple video streams and application sharing (H.239, BFCP), encryption/security features (H.235, DES/AES), firewall traversal (Assent, H.460) and other extensions of the SIP and H.323 standards.

For a router/firewall to properly perform ALG functions for SIP and H.323 traffic, it is therefore of utmost importance that the router/firewall understands and properly interprets the full content of the payload it is inspecting. Since H.323 and SIP are standards/recommendations which are in constant development, it is not likely that the router/firewall will meet these requirements, resulting in unexpected behavior when using H.323 and SIP applications in combination with such routers/firewalls.

There are also scenarios where the router/firewall normally will not be able to inspect the traffic at all, for example when using SIP over TLS, where the communication is end-to-end secure and encrypted as it passes through the router/firewall.

As per the recommendations in the Introduction section of this appendix, it is highly recommended to disable SIP and H.323 ALGs on routers/firewalls carrying network traffic to or from a Expressway-E, as, when enabled this is frequently found to negatively affect the built-in firewall/NAT traversal functionality of the Expressway-E itself. This is also mentioned in Appendix 3: Firewall and NAT settings [p.42].

General guidelines and design principles

With Expressway-E deployments involving NAT and/or dual network interfaces, some general guidelines and principles apply, as described below.

Non-overlapping subnets

If the Expressway-E will be configured to use both LAN interfaces, the LAN1 and LAN2 interfaces **must** be located in non-overlapping subnets to ensure that traffic is sent out the correct interface.

Clustering

When clustering Expressways that have the **Advanced Networking** option installed, cluster peers have to be addressed with their LAN1 interface address. In addition, clustering must be configured on an interface that does not have **Static NAT mode** enabled.

We therefore recommend that you use LAN2 as the externally facing interface, and that LAN2 is used as the static NAT interface where applicable.

Static NAT restrictions when using SIP media encryption

You should not configure an Expressway for SIP media encryption if that same Expressway is also configured for static NAT. If you do so, the private IP address will be sent in the SDP rather than the static NAT address and this will cause calls to fail.

Note that the recommended configuration for Expressway-C with Expressway-E deployments is to:

- configure the same media encryption policy setting on the traversal client zone on Expressway-C, the traversal server zone on Expressway-E, and every zone on Expressway-E
- use static NAT on the Expressway-E only

With this configuration the encryption B2BUA will be enabled on the Expressway-C only.

External LAN interface setting

The **External LAN interface** configuration setting on the **IP** configuration page controls on which network interface TURN relays are allocated. In a dual network interfaces Expressway-E configuration, this should normally be set to the externally-facing LAN interface on the Expressway-E.

Dual network interfaces

The following diagram shows an example deployment involving the use of an Expressway-E with dual network interfaces and static NAT, an Expressway-C acting as a traversal client, and two firewalls/routers. Typically in this DMZ configuration, FW A cannot route traffic to FW B, and devices such as the dual interface Expressway-E are required to validate and forward traffic from FW A's subnet to FW B's subnet (and vice versa).

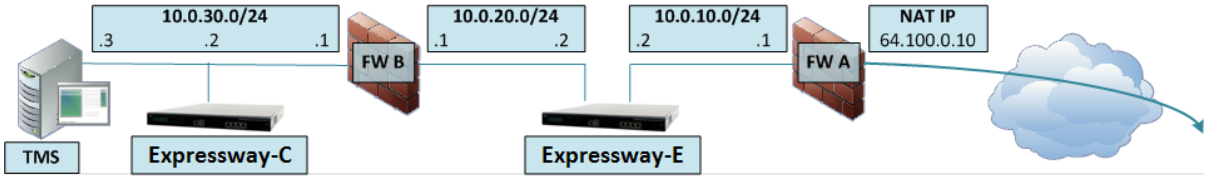


Figure 6: Dual network interfaces deployment

This deployment consists of:

- DMZ subnet 1 – 10.0.10.0/24, containing:
  - the internal interface of Firewall A – 10.0.10.1
  - the LAN2 interface of the Expressway-E – 10.0.10.2
- DMZ subnet 2 – 10.0.20.0/24, containing:
  - the external interface of Firewall B – 10.0.20.1
  - the LAN1 interface of the Expressway-E – 10.0.20.2
- LAN subnet – 10.0.30.0/24, containing:
  - the internal interface of Firewall B – 10.0.30.1
  - the LAN1 interface of the Expressway-C – 10.0.30.2
  - the network interface of the Cisco TMS server – 10.0.30.3
- Firewall A is the publicly-facing firewall; it is configured with a NAT IP (public IP) of 64.100.0.10 which is statically NATed to 10.0.10.2 (the LAN2 interface address of the Expressway-E)
- Firewall B is the internally-facing firewall
- Expressway-E LAN1 has static NAT mode disabled
- Expressway-E LAN2 has static NAT mode enabled with Static NAT address 64.100.0.10
- Expressway-C has a traversal client zone pointing to 10.0.20.2 (LAN1 of the Expressway-E)
- Cisco TMS has Expressway-E added with IP address 10.0.20.2

With the above deployment, there is no regular routing between the 10.0.20.0/24 and 10.0.10.0/24 subnets. The Expressway-E bridges these subnets and acts as a proxy for SIP/H.323 signaling and RTP /RTCP media.

Static routes

With a deployment such as that shown in Figure 6, the Expressway-E should be configured with a default gateway address of 10.0.10.1. This means that all traffic sent out via LAN2 will by default be sent to the IP address 10.0.10.1.

If Firewall B is doing NAT for traffic sent from the 10.0.30.0 subnet to the LAN1 interface of the Expressway-E (for example traversal client traffic from Expressway-C or management traffic from TMS), this means that this traffic will appear as coming from the external interface of firewall B (10.0.20.1) as it reaches LAN1 of the Expressway-E. The Expressway-E will therefore be able to reply to this traffic via its LAN1 interface, since the apparent source of that traffic is located on the same subnet.

If firewall B is not doing NAT however, traffic sent from the Expressway-C to LAN1 of the Expressway-E will appear as coming from 10.0.30.2. If the Expressway does not have a static route added for the 10.0.30.0/24 subnet, it will send replies for this traffic to its default gateway (10.0.10.1) out from LAN2, as it has not been told that the 10.0.30.0/24 subnet is located behind the 10.0.20.1 firewall. Therefore, a static route needs to be added, using the **`xCommand RouteAdd`** CLI command, which is run from an admin SSH shell on the Expressway.

In this particular example, we want to tell the Expressway-E that it can reach the 10.0.30.0/24 subnet behind the 10.0.20.1 firewall (router), which is reachable via the LAN1 interface. This is accomplished using the following **`xCommand RouteAdd`** syntax:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1
Interface: LAN1
```

In this example, the **`Interface`** parameter could also be set to **`Auto`** as the gateway address (10.0.20.1) is only reachable via LAN1.

If firewall B is not doing NAT and the Expressway-E needs to communicate with devices in subnets other than 10.0.30.0 which are also located behind firewall B (for example for communicating with management stations for HTTPS and SSH management or for reaching network services such as NTP, DNS, LDAP/AD and syslog servers), static routes will also have to be added for these devices/subnets.

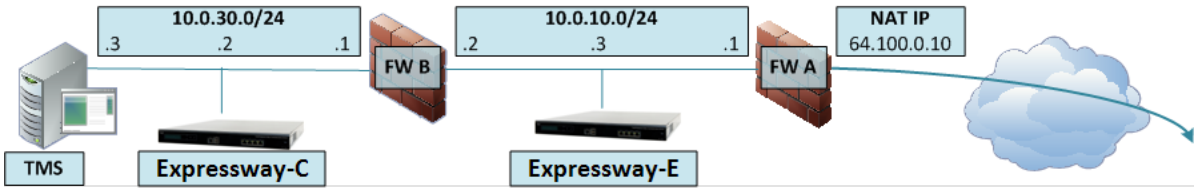
The **`xCommand RouteAdd`** command and syntax is described in full detail in *Expressway Administrator Guide*.

Example deployments

The following section contains additional reference designs which depict other possible deployment scenarios.

Single subnet DMZ using single Expressway-E LAN interface

In this case, FW A can route traffic to FW B (and vice versa). Expressway-E allows video traffic to be passed through FW B without pinholing FW B from outside to inside. Expressway-E also handles firewall traversal on its public side.



This deployment consists of:

- a single subnet DMZ – 10.0.10.0/24, containing:
  - the internal interface of firewall A – 10.0.10.1
  - the external interface of firewall B – 10.0.10.2
  - the LAN1 interface of the Expressway-E – 10.0.10.3
- a LAN subnet – 10.0.30.0/24, containing:
  - the internal interface of firewall B – 10.0.30.1
  - the LAN1 interface of the Expressway-C – 10.0.30.2
  - the network interface of Cisco TMS – 10.0.30.3

A static 1:1 NAT has been configured on firewall A, NATing the public address 64.100.0.10 to the LAN1 address of theExpressway-E. **Static NAT mode** has been enabled for LAN1 on the Expressway-E, with a static NAT address of 64.100.0.10.

The traversal client zone on the Expressway-C needs to be configured with a peer address which matches the static NAT address of the Expressway-E, in this case 64.100.0.10. This is because, since the Expressway-E has static NAT mode enabled, it will request that incoming signaling and media traffic should

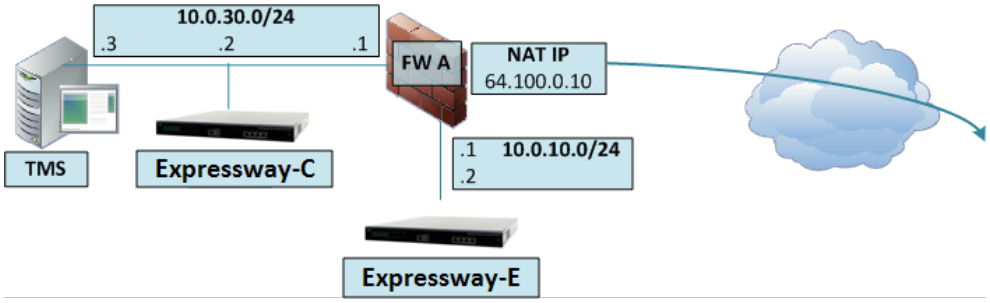
be sent to its static NAT address, which means that the traversal client zone has to be configured accordingly.

This means that firewall A must allow traffic from the Expressway-C with a destination address of 64.100.0.10. This is also known as NAT reflection, and it should be noted that this is not supported by all types of firewalls.

The Expressway-E should be configured with a default gateway of 10.0.10.1. Whether or not static routes are needed in this scenario depends on the capabilities and settings of FW A and FW B. Expressway-C to Expressway-E communications will be to the 64.100.0.10 address of the Expressway-E; the return traffic from the Expressway-E to Expressway-C might have to go via the default gateway. If a static route is added to the Expressway-E so that reply traffic goes from the Expressway-E and directly through FW B to the 10.0.30.0/24 subnet, this will mean that asymmetric routing will occur and this may or may not work, depending on the firewall capabilities.

The Expressway-E can be added to Cisco TMS with the IP address 10.0.10.3 (or with IP address 64.100.0.10 if FW A allows this), since Cisco TMS management communications are not affected by static NAT mode settings on the Expressway-E.

3-port firewall DMZ using single Expressway-E LAN interface



In this deployment, a 3-port firewall is used to create

- a DMZ subnet (10.0.10.0/24), containing:
  - the DMZ interface of firewall A - 10.0.10.1
  - the LAN1 interface of the Expressway-E - 10.0.10.2
- a LAN subnet (10.0.30.0/24), containing
  - the LAN interface of firewall A - 10.0.30.1
  - the LAN1 interface of the Expressway-C – 10.0.30.2
  - the network interface of Cisco TMS – 10.0.30.3

A static 1:1 NAT has been configured on firewall A, NATing the public address 64.100.0.10 to the LAN1 address of the Expressway-E. Static NAT mode has been enabled for LAN1 on the Expressway-E, with a static NAT address of 64.100.0.10.

TheExpressway-E should be configured with a default gateway of 10.0.10.1. Since this gateway must be used for all traffic leaving the Expressway-E, no static routes are needed in this type of deployment.

The traversal client zone on the Expressway-C needs to be configured with a peer address which matches the static NAT address of the Expressway-E, in this case 64.100.0.10, for the same reasons as those described in the previous example deployment, "Single subnet DMZ using single Expressway-E LAN interface".

This means that firewall A must allow traffic from the Expressway-C with a destination address of 64.100.0.10. This is also known as NAT reflection, and it should be noted that this is not supported by all types of firewalls.

The Expressway-E can be added to Cisco TMS with the IP address 10.0.10.2 (or with IP address 64.100.0.10 if FW A allows this), since Cisco TMS management communications are not affected by static NAT mode settings on the Expressway-E.

Checking for updates and getting help

If you experience any problems when configuring or using the product, consult the online help available from the user interface. The online help explains how the individual features and settings work.

If you cannot find the answer you need, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- make sure that you are running the most up-to-date software,
- find further relevant documentation, for example product user guides, printable versions of the online help, reference guides, and articles that cover many frequently asked questions,
- get help from the Cisco Technical Support team. Click on Technical Support Overview for information on Accessing Cisco Technical Services. Make sure you have the following information ready before raising a case:
  - the serial number and product model number of the unit (if applicable)
  - the software build number which can be found on the product user interface (if applicable)
  - your contact email address or telephone number
  - a full description of the problem

Document revision history

Revision	Date	Description
03	August 2014	Correction in firewall configuration appendix.
01	December 2013	Initial release.