



# Cisco Expressway-E and Expressway-C – Basic Configuration

Deployment Guide

**First Published: December 2013**

**Last Updated: July 2016**

Cisco Expressway X8.8



## Preface

### Change History

**Table 1 Deployment Guide Change History**

Date	Change
July 2016	Republished for X8.8.
November 2015	New template applied. Advanced Network Deployments appendix revised. Republished for X8.7.
April 2015	Menu path changes for X8.5. Republished with X8.5.2.
December 2014	Republished for X8.5.
August 2014	Correction in firewall appendix.
June 2014	Republished for X8.2.
December 2013	Initial release.

# Contents

Preface .....	3
Change History .....	3
Introduction .....	7
Example Network Deployment .....	9
Network Elements .....	10
Process Summary .....	12
Prerequisites .....	13
Run the Service Setup Wizard .....	14
Overview .....	14
Task 1: Accessing and Navigating the Wizard .....	14
Task 2: Running the Service Setup Wizard and Applying Licenses .....	16
Examples for Running the Service Setup Wizard .....	18
Expressway System Configuration .....	19
Task 3: Setting the System Name .....	19
Task 4: Configuring DNS .....	19
Task 5: Replacing the Default Server Certificate .....	20
Task 6: Configuring NTP Servers .....	21
Task 7: Configuring SIP Domains .....	22
Routing Configuration .....	23
Pre-search Transforms .....	23
Search Rules .....	23
Task 8: Configuring Transforms .....	23
Task 9: Configuring Local Zone Search Rules .....	24
Task 10: Configuring the Traversal Zone .....	25
Neighboring Between Expressway Clusters .....	27
Task 11: Configuring Traversal Zone Search Rules .....	27
Task 12: Configuring the DNS Zone .....	30
Task 13: Configuring DNS Zone Search Rules .....	30
Task 14: Configuring External (Unknown) IP Address Routing .....	32
Endpoint Registration .....	34
System Checks .....	35

Zone Status .....	35
Registration Status .....	35
Call Signaling .....	35
Maintenance Routine .....	36
Creating a System Backup .....	36
Optional Configuration Tasks .....	37
Task 15: Configuring Routes to a Neighbor Zone (Optional) .....	37
Task 16: Configuring Cisco TMS (Optional) .....	38
Task 17: Configuring Logging (Optional) .....	40
Task 18: Configuring Registration Restriction Policy (Optional) .....	41
Task 19: Configuring Device Authentication Policy (Optional) .....	42
Task 20: Restricting Access to ISDN Gateways (Optional) .....	42
Appendix 1: Configuration Details .....	50
Expressway-C Configuration Details .....	50
Expressway-E Configuration Details .....	51
Expressway-C and Expressway-E Configuration Details .....	52
Appendix 2: DNS Records .....	54
DNS Configuration on Host Server .....	54
DNS Configuration (internal DNS server) .....	54
Appendix 3: Firewall and NAT Settings .....	56
Internal Firewall Configuration .....	56
External Firewall Configuration Requirement .....	57
Appendix 4: Advanced Network Deployments .....	59
Prerequisites .....	59
Recommended: Dual NIC Static NAT Deployment .....	59
Background Information .....	61
Other Deployment Examples .....	62
Obtaining Documentation and Submitting a Service Request .....	67
Cisco Legal Information .....	68
Cisco Trademark .....	68



## Introduction

Cisco Expressway is designed specifically for comprehensive collaboration services. 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 you through the following tasks:

1. Using the Service Setup Wizard to select the services you want to use and to apply the corresponding keys (licenses).
2. Configuring system parameters and routing information.
3. Checking that the system is working as expected.
4. Configuring optional items such as Cisco TMS, system logging, and access restrictions.

### Advanced configuration

This document also provides detailed DNS, NAT, and firewall configuration information. In each case we assume that you have a working knowledge of how to configure these systems. The appendices to the document provide detailed reference information, as follows:

- Expressway configuration details used in this document are listed in [Appendix 1: Configuration Details, page 50](#).
- DNS records required for the example deployment used in this document are in [Appendix 2: DNS Records, page 54](#).
- Details of required NAT and firewall configurations are in [Appendix 3: Firewall and NAT Settings, page 56](#). 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.
- How to deploy your system with a static NAT and Dual Network Interface architecture is explained in [Appendix 4: Advanced Network Deployments, page 59](#).

For descriptions of all system configuration parameters, see the [Expressway Administrator Guide](#) and the Expressway web application's online field help  and page help .

### Example configuration values used in this guide

For ease of reading this guide is based around an example deployment, which uses the following assumed configuration values throughout:

	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
Domain name	<i>internal-domain.net</i>	<i>example.com</i>

### Information in other deployment guides

This document does not describe how to deploy a clustered system, or systems running device provisioning, device authentication, or FindMe applications, or how to configure the Expressway system for Unified Communications services. For more details about these features, see the following documents:

- *Mobile and Remote Access via Cisco Expressway Deployment Guide* on the [Expressway configuration guides page](#) (for how to configure Unified Communications services)

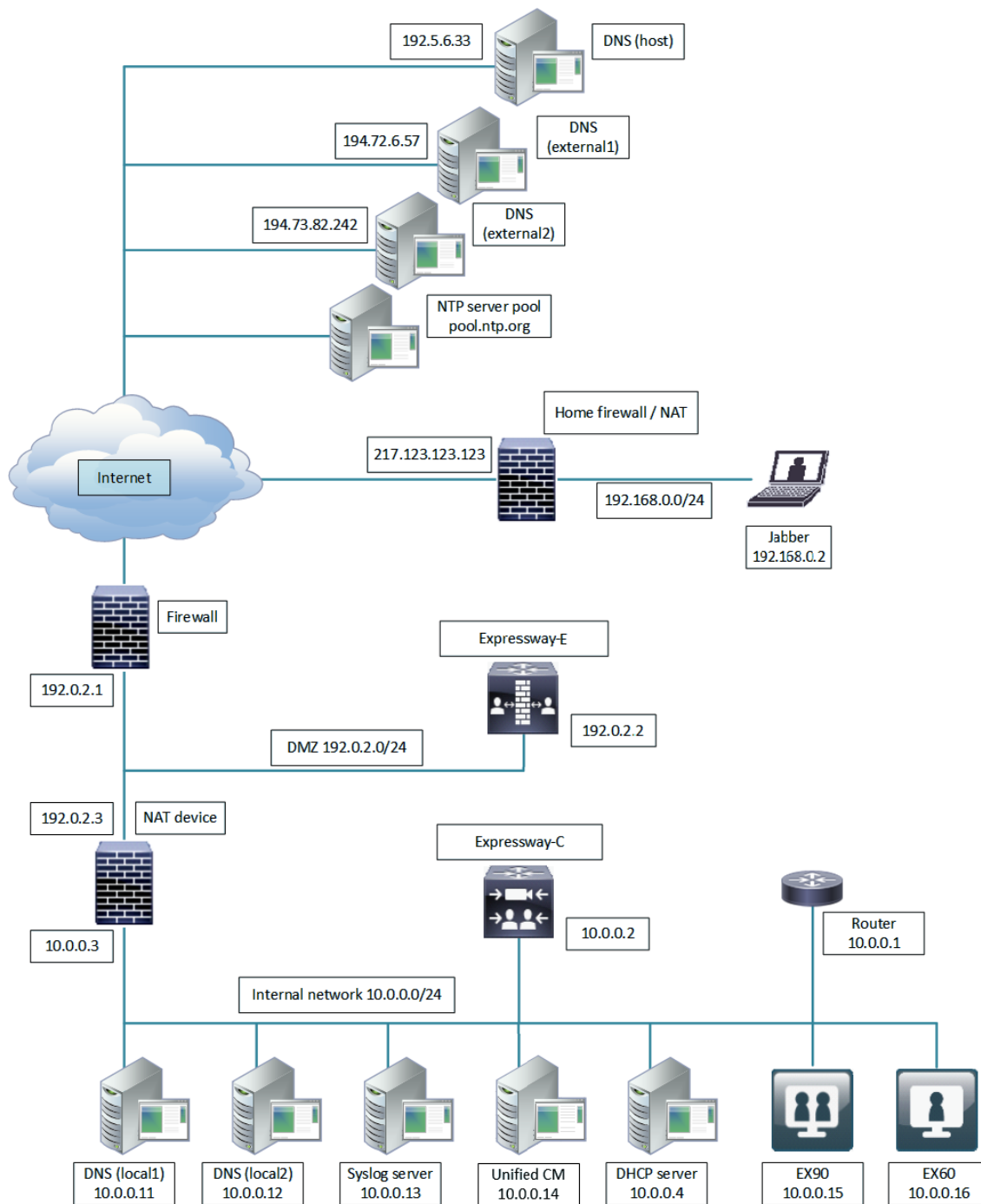
## Introduction

- *Expressway Cluster Creation and Maintenance Deployment Guide* on the [Expressway configuration guides page](#)
- *Cisco TMS Provisioning Extension Deployment Guide* on the [VCS configuration guides page](#) (includes instructions for deploying FindMe – note that this guide is on the VCS page and not on the Expressway page)
- *Expressway IP Port Usage for Firewall Traversal* on the [Expressway configuration guides page](#)
- *Cisco VCS Authenticating Devices* on the [VCS configuration guides page](#) (note that this guide is on the VCS page and not on the Expressway page)



## Example Network Deployment

**Figure 1 Example Network for the Deployment Described in this Document**



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

## Introduction

## Network Elements

### Internal Network Elements

The internal network elements are devices which are hosted on your local area network. Elements on the internal network have an internal network domain name. This 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).

Element	Role
Expressway-C	SIP Registrar & Proxy and communications gateway for Unified CM.
EX90 and EX60	Example endpoints hosted on the internal network which register to the Expressway-C or to the Unified CM.
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	Provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.
Router	Acts as the gateway for all internal network devices to route towards the DMZ (to the NAT device internal address).
Cisco TMS Server	Management and scheduling server. See <a href="#">Task 16: Configuring Cisco TMS (Optional)</a> , page 38.
Unified CM	Endpoint devices can register to Unified CM. The Expressway acts as a Unified Communications gateway for third-party devices and for mobile and remote access. Or you can register directly to the Cisco Expressway-C.  To configure the Expressway for Unified Communications services, see <i>Mobile and Remote Access via Cisco Expressway Deployment Guide</i> on the <a href="#">Expressway configuration guides page</a> .
Syslog Server	Logging server for Syslog messages. See <a href="#">Task 17: Configuring Logging (Optional)</a> , page 40.

### 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 3<sup>rd</sup> 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

Element	Role
Jabber	An example remote endpoint, which is registering over the internet to Unified CM via the Expressway-E and Expressway-C.
EX60	An example remote endpoint, which is registering to the Expressway-E via the internet.
DNS (Host)	The DNS owned by the 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, page 56](#).
- 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, page 59](#) 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 internal-domain.net. The DNS SRV configurations are described in [Appendix 2: DNS Records, page 54](#).

- 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 Expressway-C.

## Process Summary

### Before You Begin

- [Prerequisites, page 13](#)

### Run the Service Setup Wizard

- [Task 1: Accessing and Navigating the Wizard, page 14](#)
- [Task 2: Running the Service Setup Wizard and Applying Licenses, page 16](#)
- [Examples for Running the Service Setup Wizard, page 18](#)

### Expressway system configuration tasks

- [Task 3: Setting the System Name, page 19](#)
- [Task 4: Configuring DNS, page 19](#)
- [Task 5: Replacing the Default Server Certificate, page 20](#)
- [Task 6: Configuring NTP Servers, page 21](#)
- [Task 7: Configuring SIP Domains, page 22](#)

### Routing configuration tasks

- [Task 8: Configuring Transforms, page 23](#)
- [Task 9: Configuring Local Zone Search Rules, page 24](#)
- [Task 10: Configuring the Traversal Zone, page 25](#)
- [Task 11: Configuring Traversal Zone Search Rules, page 27](#)
- [Task 12: Configuring the DNS Zone, page 30](#)
- [Task 13: Configuring DNS Zone Search Rules, page 30](#)
- [Task 14: Configuring External \(Unknown\) IP Address Routing, page 32](#)

### Optional configuration tasks

- [Task 15: Configuring Routes to a Neighbor Zone \(Optional\), page 37](#)
- [Task 16: Configuring Cisco TMS \(Optional\), page 38](#)
- [Task 17: Configuring Logging \(Optional\), page 40](#)
- [Task 18: Configuring Registration Restriction Policy \(Optional\), page 41](#)
- [Task 20: Restricting Access to ISDN Gateways \(Optional\), page 42](#)

## Prerequisites

## Prerequisites

Before you begin any of the tasks in this guide, make sure that the following prerequisites are complete.

### General prerequisites

- We recommend that you use the Expressway web user interface to do the system configuration. This guide assumes that you are using a web browser running on a PC. The PC needs an Ethernet connection to a LAN which can route HTTP(S) traffic to the Expressway.
- Review the relevant release notes on the [Expressway release notes page](#).
- Have the *Expressway Administrator Guide* on the [Expressway maintenance and operation guides page](#) available for reference before you start.

### IP address and password prerequisites

This guide also assumes that you have already configured a static IP address and changed the default passwords, as described in the appropriate installation guide:

- *Cisco Expressway Virtual Machine Installation Guide* on the [Expressway installation guides page](#).
- *Cisco Expressway CE1100 Appliance Installation Guide* on the [Expressway installation guides page](#).

**Note:** Expressway requires a static IP address. It doesn't use DHCP/SLAAC to get an IP address.

### DNS, NAT/firewall, and DHCP prerequisites

The following non-Expressway system configuration needs to be in place before you start:

- Internal and external DNS records. See [Appendix 2: DNS Records, page 54](#).
- NAT & firewall configuration. See [Appendix 3: Firewall and NAT Settings, page 56](#).
- DHCP server configuration (not described in this document).

## Run the Service Setup Wizard

### Overview

The Service Setup Wizard makes it easier to configure and license the Expressway for its chosen purpose in your environment. It also simplifies the user interface. You select from a list of popular Expressway services and the wizard then prompts you with the licensing requirements for those services. You can also use the wizard to review and edit the Expressway basic network settings (typically already configured during initial installation).

When you restart the Expressway, the user interface is tailored to match your service selections. You only see menus and pages for the services you chose.

**Note:** Some services are incompatible and cannot be selected together. The [Expressway Administrator Guide](#) and the online help provide a matrix of compatible services. The matrix specifies which services you can use together on the same system or cluster.

### What If I Don't Want to Use the Wizard?

A skip option exists if you don't want to use the wizard. If you change your mind later, you can go back and run it at any time (**Status > Overview** page; click **Run service setup**).

If you opt to skip the wizard, you need to deal with the Expressway licensing setup requirements manually before you start the configuration tasks in this guide. Also, the user interface isn't customized to reflect your specific service selections.

## Task 1: Accessing and Navigating the Wizard

There are multiple ways to access the wizard:

- As of X8.8, you'll automatically see the Service Setup Wizard when you first log in to the Expressway user interface. You don't need to launch it.
- If you previously logged in or have upgraded, you'll see the **Status > Overview** page as usual. Click **Run service setup** to launch the wizard.
- If you've already run the wizard you can rerun it at any time. From the **Status > Overview** page, click **Return to service setup**.

To navigate the wizard:

- Click **Skip Service Setup Wizard** if you want to back out of the wizard completely, or **Back** to return to the previous page.
- Click **Continue** to save and move to the next wizard page.

## Run the Service Setup Wizard

**Figure 2 Service Setup Wizard Example - Selection Page**

Welcome to Cisco Collaboration services [Help](#) [Logout](#)

**Select Series**

Expressway series ☒ ⓘ

VCS series ☐

**Select Type**

Expressway-C ☒ ⓘ

Expressway-E ☐

**Select Services**

After you select services, you get a simplified menu that is relevant to your selection. ⓘ

Cisco Spark Hybrid Services ☐

Mobile and remote access ☐

Jabber Guest services ☐

Microsoft Interoperability ☐

Registrar ☐

Collaboration Meeting Rooms (CMR) Cloud ☐

Business to business calls ☐

If you proceed without selecting services, you will get the full menu.

Proceed without selecting services ☐

[Cancel](#) [Continue](#)

## Task 2: Running the Service Setup Wizard and Applying Licenses

### Process

1. Choose *Expressway series*.
2. Choose *Expressway-C* or *Expressway-E*. We recommend that you select Expressway-C first and run the wizard for it. Then run the wizard on the Expressway-E.  
The list of services changes to match what's available on your chosen Series and Type.
3. Select Services. Check the boxes next to the services you want to use on this system. (The matrix of compatible services is in the [Expressway Administrator Guide](#) and the online help.)  
If you want to keep all the menu options, or if you want to use the wizard for applying licenses but don't want to choose services yet, check *Proceed without selecting services*.
4. Click **Continue** to move to the **Option keys** page of the wizard. This page helps you to identify and acquire the appropriate licenses for your chosen selections. (Worked examples are provided in [Examples for Running the Service Setup Wizard](#), page 18.)

The [Licensing help](#) section (top of page) explains how to use your Product Authorization Key (PAK) in Cisco's Product License Registration Portal. The [License status](#) section (bottom of page) lists the actual licenses that you need and their status (loaded / not loaded).

The exact entries vary by deployment – this example is for the Cisco Expressway-C Registrar service:

Figure 3 Service Setup Wizard Example – Option Keys Page

Option keys

Licensing help

Serial number

How to get licenses

Licenses are still required for the services you selected. You may need to paste more text from your email, or return to the ordering portal.

You need this system's serial number to order keys. Go to the [Product License Registration Portal](#), and load your PAK (Product Authorization Key). Inside your PAK you have one or more Product Identifiers (PDIs) that are named like the examples shown in the License status section further down this page. Select the PDIs that you need from the ones in the PAK, by looking at the examples shown in the Required section of the License status below. When you've selected PDIs, click Assign to device and enter the serial number from this page. When you click Finish, you'll get an email with the keys you need. Paste all the email text into this page so the system can read the keys for you. If you generate more than one email from the licensing portal, you can add new paste areas.

Apply keys

Paste the text from your release key email here

Paste the text from your option keys email here

New paste area

Add keys

License status

Based on the services you have selected:

Required	License PID example	Status
Description	LC-SW-EXP-K9	Loaded
Release key	LC-EXP-SERIES	Needed

Optional	License PID example	Status
Description	LC-EXP-RMS	Not loaded
Rich Media Sessions	LC-EXP-AN	Not loaded
Advanced Networking	LC-EXP-QW	Not loaded
K323-SP Interworking Gateway	LC-EXP-ROOM	Not loaded
Room Systems	LC-EXP-DSK	Loaded
Desktop Systems		



5. On the **Option Keys** page, click the [Product License Registration Portal](#) link to go to the licensing portal. (For this step you need to work away from the wizard to obtain the necessary licenses, and you need the serial number of the system.) In the licensing portal, enter the necessary details for the required licenses. For example, to register desktop systems like the EX90, you'll need to add Desktop System registration licenses. Detailed information about using the licensing portal is in the online help or the [Expressway Administrator Guide](#). An ordering guide for our products is available on the Cisco [Collaboration Ordering Guides](#) page.
6. Wait for system-generated emails from the licensing portal with the release key and option keys for your selected services.
7. Back in the wizard, paste the text from the release key email into the first text area. The system reads the release key out of the pasted text and displays it next to the text area.
8. Paste the text from the option keys email into the second text area. The system reads the option keys out of the pasted text and displays them next to the text area.
9. Add new text areas if you have more email text to paste in, such as your room or desktop system registration license keys.
10. Click **Add Keys**.

The **License status** table groups the keys that are possible on this system, and indicates whether they are loaded or not loaded. The keys are grouped as follows:

  - **Required:** If any keys in this section are not yet loaded, you see status **Required** and will not be able to continue through the wizard.
  - **Optional:** Shows keys that may or may not be useful, but are not strictly required for the services you chose.
  - **Unrelated:** These keys won't harm the system if they are loaded, but will not provide any benefit for the services you chose.
  - **Incompatible:** These keys cannot work with the selected services. You must remove them or choose different services before you can continue.
11. Click **Continue**.
12. Review the network configuration and modify the settings if necessary. Save any changes before you continue the wizard.
13. Click **Finish**.
14. Restart the system when prompted.

**Result:** When you log in, the user interface is tailored to match your service selections. You only see menus and pages for the services you chose.

## What to do next

The wizard is complete for the Expressway-C element. Now you need to run it on the Expressway-E. For typical deployments with the Expressway-E the services you are most likely to select with the wizard include *Mobile and remote access* and *Business to business calls*. When the Expressway-E is done, go to the next section in this guide, "*Expressway System Configuration*."

## Examples for Running the Service Setup Wizard

### Example for Expressway Registrar

1. Click *Expressway Series*.
2. Click *Expressway-C*.
3. Check *Registrar*.
4. Check any other compatible services that you have bought for this system. For this example, let's assume *Business to business calls*. (The matrix of compatible services is in the online help and the [Expressway Administrator Guide](#).)
5. Click **Continue**.  
The wizard takes you to the licensing and options page.
6. Paste the release key into the first text area (eg. LIC-SW-AAA-A0)
7. Paste the Expressway Series key into the second text area (eg. 116341E00-1-AAAAAAA).
8. Create a new paste area and paste in your room or desktop system registration license keys.
9. Click **Add Keys**.
10. Click **Continue**.
11. Review the networking configuration and click **Finish**.
12. Restart the system when prompted.

This completes the service setup and licensing for the Expressway-C part of your desired outcome. However, since we chose *Business to business calls*, we would have to run the wizard again to set up and license an Expressway-E, because the business to business calling deployment requires firewall traversal.

### Example for Hybrid Services

1. Click *Expressway Series*.
2. Click *Expressway-C*.
3. Check *Spark Hybrid Services*.
4. Click **Continue**.  
The wizard asks you to review your network configuration. It skipped the licensing page because you don't need a release key, or licenses, or option keys, to register for Hybrid Services.
5. Review the network configuration and modify the settings if necessary. Save any changes before you continue the wizard.
6. Click **Finish**.  
The wizard opens the **Connector Management** page where you can register the Expressway for Hybrid Services.

## Expressway System Configuration

### Task 3: Setting the System Name

The **System name** defines the name of the Expressway. It appears in various places in the web interface and is also used by Cisco TMS. We recommend using a name that lets you easily and uniquely identify the Expressway.

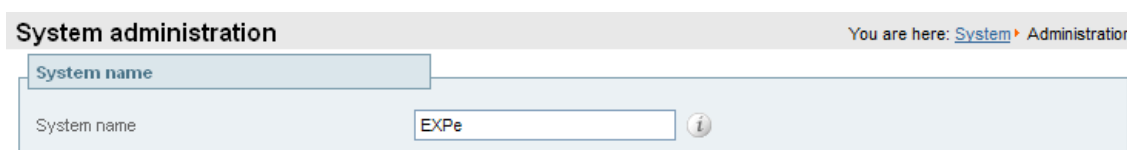
To configure the **System name**:

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

	Expressway-C	Expressway-E
<b>System name</b>	Enter <b>EXPC</b>	Enter <b>EXPE</b>

3. Click **Save**.

**Figure 4 Expressway-E**



### Task 4: 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
<b>System host name</b>	Enter <b>expc</b>	Enter <b>expe</b>

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**:

## Expressway System Configuration

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

	Expressway-C	Expressway-E
<b>Domain name</b>	Enter <code>internal-domain.net</code>	Enter <code>example.com</code>

3. Click **Save**.

The fully qualified domain name for the Expressway-C is now `expc.internal-domain.net`

The fully qualified domain name for the Expressway-E is now `expe.example.com`

## DNS Servers

The DNS server addresses specify the IP addresses of up to five domain name servers to be used for resolving domain names. In either of the following cases you must specify at least one default DNS server for address resolution:

- To use fully qualified domain names instead of IP addresses when specifying external addresses. For example, for LDAP and NTP servers, neighbor zones and peers.
- To use features such as URI dialing or ENUM dialing.

The Expressway queries one server at a time. If that server is unavailable the Expressway tries another server from the list.

In the example deployment two 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
<b>Address 1</b>	Enter <code>10.0.0.11</code>	Enter <code>194.72.6.57</code>
<b>Address 2</b>	Enter <code>10.0.0.12</code>	Enter <code>194.73.82.242</code>

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 5: 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 a certificate that can represent the Expressway as either a client or a server in connections using TLS. The Expressway can also authenticate client connections (typically from a web browser) over

## Expressway System Configuration

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 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 the system is working correctly over TCP before attempting to secure the connection with TLS. We also recommend using a third party LDAP browser to verify that your LDAP server is correctly configured for TLS.

**Note:** Be careful not to allow your CA certificates or CRLs to expire. 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* on the [Expressway configuration guides page](#).

## Task 6: 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
<b>NTP server 1</b>	Enter pool.ntp.org	Enter pool.ntp.org
<b>Time zone</b>	GMT in this example	GMT in this example

3. Click **Save**.

## Expressway System Configuration

**Time** You are here: [System](#) > Time

**NTP servers**

NTP server 1	Address	pool.ntp.org	Authentication	Disabled
NTP server 2	Address		Authentication	Disabled
NTP server 3	Address		Authentication	Disabled
NTP server 4	Address		Authentication	Disabled
NTP server 5	Address		Authentication	Disabled

**Time zone**

Time zone: GMT

## Task 7: Configuring SIP Domains

The Expressway acts as a SIP Registrar for configured SIP domains, accepting registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See [Task 18: Configuring Registration Restriction Policy \(Optional\)](#), page 41.
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

- Go to **Configuration > Domains**.
- Click **New**.
- Enter the domain name into the **Name** field (on both Expressway-C and Expressway-E):

	Expressway-C	Expressway-E
<b>Name</b>	Enter example.com	Enter example.com

- Click **Create domain**.
- The **Domains** page displays all configured SIP domain names.

**Domains** You are here: [Configuration](#) > [Domains](#) > New

**Configuration**

Domain name: ★ example.com

## What To Do Next

The Expressway system configuration is now complete. Go to the next section, "[Routing Configuration](#)."

## Routing Configuration

### Pre-search Transforms

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The Expressway applies the transformation 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 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 automatically appends 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.

- Use pre-search transforms 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's 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 search rules described here are used to enable the following routing combinations:

Calling party	Called party
Registered devices (Expressway-C)	Registered devices (Expressway-C)
Registered devices (Expressway-C)	External domains and un-registered devices (via Expressway-E using DNS zone)
Registered devices (Expressway-C)	Public external IP addresses (via Expressway-E)
External domains and un-registered devices	Registered devices (Expressway-C)

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* with target Local Zone. 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 8: 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.

## Routing Configuration

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

4. Click **Create transform**.

**Create transform** You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority

1

Description

Transform destination aliases to URI format

Pattern type

Regex

Pattern string

\*([^\@]\*)

Pattern behavior

Replace

Replace string

\1@example.com

State

Enabled

Create transform

Cancel

## Task 9: Configuring Local Zone Search Rules

To configure the search rules to route calls to the Local Zone (to locally registered endpoint aliases):

1. Go to **Configuration > Dial plan > Search rules**.
2. Select the check box next to the default search rule (**LocalZoneMatch**).
3. Click **Delete**.  
(The default search rule is being deleted and replaced with a more specific configuration.)
4. Click **OK**.
5. Click **New**.



## 6. Configure the search rule fields as follows:

	Expressway-C	Expressway-E
<b>Rule name</b>	Enter <code>Local zone - full URI</code>	Same as Expressway-C
<b>Description</b>	Enter <code>Search local zone for SIP devices with a domain</code>	
<b>Priority</b>	Enter <code>50</code>	
<b>Protocol</b>	<i>Any</i>	
<b>Source</b>	<i>Any</i>	
<b>Request must be authenticated</b>	<i>No</i>	
<b>Mode</b>	<i>Alias pattern match</i>	
<b>Pattern type</b>	<i>Regex</i>	
<b>Pattern string</b>	Enter <code>(.+ )@example.com.*</code>	
<b>Pattern behavior</b>	<i>Leave</i>	
<b>On successful match</b>	<i>Continue</i>	
<b>Target</b>	<i>LocalZone</i>	
<b>State</b>	<i>Enabled</i>	

7. Click **Create search rule**.

## Task 10: 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. Expressway-C is configured with a traversal client zone. Expressway-E is configured with a traversal server zone.

### Which type of traversal zone?

- If your deployment is for business to business calling, use a traversal zone.
- If your deployment is for mobile and remote access, use a Unified Communications traversal zone (see next section).

### Traversal zones for Unified Communications

If you need Unified Communications features like mobile and remote access or Jabber Guest, a secure traversal zone connection must exist between Expressway-C and Expressway-E:

- The Expressway-C and Expressway-E must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on Expressway-C or a traversal server zone when selected on Expressway-E) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *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.

## Routing Configuration

- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

**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
<b>Name</b>	Enter TraversalZone	Enter TraversalZone
<b>Type</b>	Traversal client	Traversal server
<b>Username</b>	Enter exampleauth	Enter exampleauth
<b>Password</b>	Enter ex4mpl3.c0m	Not applicable
<b>H.323 Mode</b>	On	On
<b>H.323 Protocol</b>	Assent	Assent
<b>H.323 Port</b>	Enter 6001	Enter 6001
<b>H.323 H.460.19 demultiplexing mode</b>	Not applicable	Off
<b>SIP Mode</b>	On	On
<b>SIP Port</b>	Enter 7001	Enter 7001
<b>SIP Transport</b>	TLS	TLS
<b>SIP TLS verify mode</b>	Off	Off
<b>SIP Accept proxied registrations</b>	Allow	Off
<b>Location Peer 1 address</b>	Enter 192.0.2.2	Not applicable

4. Click **Create zone**.

**Configuring authentication credentials in Expressway-E**

To configure the authentication credentials in the **Local authentication database** (configured in the Expressway-E only), do the following:

1. Go to **Configuration > Authentication > Devices > Local database**.
2. Click **New**.
3. Configure the fields as follows:

	Expressway-C	Expressway-E
<b>Name</b>	Not applicable	Enter exampleauth
<b>Password</b>	Not applicable	Enter ex4mpl3.c0m

4. Click **Create credential**.

**Local authentication database** You are here: [Configuration](#) > [Authentication](#) > [Devices](#) > [Local database](#)

**Configuration**

Name  ⓘ

Password  ⓘ

## Neighboring Between Expressway Clusters

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

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

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

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

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

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

### Neighboring your clusters

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

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

Note that:

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

## Task 11: Configuring Traversal Zone Search Rules

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

## Routing Configuration

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

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

\* This example routes any alias across the traversal zone towards the Expressway-C. You can be more selective by adding search rules or configuring call policy.

4. Click **Create search rule**.

**Figure 5 Traversal Zone Search Rule on Expressway-C**

**Create search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name

★ Traversal zone search rule ⓘ

Description

Search traversal zone - EXPe ⓘ

Priority

★ 100 ⓘ

Protocol

Any ⓘ

Source

Any ⓘ

Request must be authenticated

No ⓘ

Mode

Any alias ⓘ

On successful match

Continue ⓘ

Target

★ TraversalZone ⓘ

State

Enabled ⓘ











Create search rule

Cancel

**Figure 6 Traversal Zone Search Rule on Expressway-E**

**Create search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

**Configuration**

Rule name	★ Traversal zone search rule 
Description	Search traversal zone - EXPc 
Priority	★ 100 
Protocol	Any 
Source	Any 
Request must be authenticated	No 
Mode	Any alias 
On successful match	Continue 
Target	★ TraversalZone 
State	Enabled 

## Task 12: 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. Sign in to the Expressway-E.
2. Go to **Configuration > Zones > Zones**.
3. Click **New**.
4. Configure the fields as follows (leave all other fields with default values):

Field name	Value
<b>Name</b>	Enter DNSZone for example
<b>Type</b>	<i>DNS</i>
<b>H.323 Mode</b>	<i>On</i>
<b>SIP Mode</b>	<i>On</i>
<b>Fallback transport protocol</b>	<i>TCP</i>
<b>Include address record</b>	<i>Off</i>

5. Click **Create zone**.

## Task 13: 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. Sign in to the Expressway-E.
2. Go to **Configuration > Dial plan > Search rules**.
3. Click **New**.

## Routing Configuration

## 4. Configure the fields as follows:

Field name	Value
<b>Rule name</b>	Enter DNS zone search rule for example
<b>Description</b>	Enter Search DNS zone (external calling) for example
<b>Priority</b>	150
<b>Protocol</b>	Any
<b>Source</b>	All zones
<b>Request must be authenticated</b>	No
<b>Mode</b>	Alias pattern match
<b>Pattern type</b>	Regex
<b>Pattern string</b>	Enter (?!.*@example\.com.*\$).*
<b>Pattern behavior</b>	Leave
<b>On successful match</b>	Continue
<b>Target</b>	DNSZone
<b>State</b>	Enabled

5. Click **Create search rule**.

**Create search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name

★ DNS zone search rule ⓘ

Description

Search DNS zone (external calling) ⓘ

Priority

★ 150 ⓘ

Protocol

Any ⓘ

Source

AllZones ⓘ

Request must be authenticated

No ⓘ

Mode

Alias pattern match ⓘ

Pattern type

Regex ⓘ

Pattern string

★ (?!.\*@%localdomains%.\*\$).\* ⓘ

Pattern behavior

Leave ⓘ

On successful match

Continue ⓘ

Target

★ DNSZone ⓘ

State

Enabled ⓘ

Create search rule

Cancel

## Routing Configuration

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

(?!.\*@example\.com.\*\$).\* = do not match any pattern strings ending in @example.com

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 14: 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.

Known IP addresses are addresses defined in a subzone (using a subzone membership subnet rule).

- 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 handles calls to unknown IP addresses:

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

	Expressway-C	Expressway-E
<b>Calls to unknown IP addresses</b>	<i>Indirect</i>	<i>Direct</i>

### Expressway-C

**Dial plan configuration** You are here: [Configuration](#) > [Dial plan](#) > [Configuration](#)

**Configuration**

Calls to unknown IP addresses Indirect ⓘ

Fallback alias  ⓘ

**Save**

### Expressway-E

**Dial plan configuration** You are here: [Configuration](#) > [Dial plan](#) > [Configuration](#)

**Configuration**

Calls to unknown IP addresses Direct ⓘ

Fallback alias  ⓘ

**Save**

3. Click **Save**.

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
<b>Rule name</b>	Enter External IP address search rule	Not applicable
<b>Description</b>	Enter Route external IP address	Not applicable
<b>Priority</b>	Enter 100	Not applicable
<b>Protocol</b>	Any	Not applicable
<b>Source</b>	Any	Not applicable
<b>Request must be authenticated</b>	No	Not applicable
<b>Mode</b>	Any IP address	Not applicable
<b>On successful match</b>	Continue	Not applicable
<b>Target</b>	TraversalZone	Not applicable
<b>State</b>	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 i

Description Route external IP address i

Priority ★ 100 i

Protocol Any i

Source Any i

Request must be authenticated No i

Mode Any IP address i

On successful match Continue i

Target ★ TraversalZone i

State Enabled i

Create search rule

Cancel

## Endpoint Registration

The example network configuration diagram shows three endpoints.

Endpoint	IP address	Network
EX90	10.0.0.15	Internal network
EX60	10.0.0.16	Internal network
EX60	192.168.0.2	Home user network

After system configuration, endpoint registration should be possible using these endpoint configuration details:

EX90 (uses SIP protocol)	
SIP URI	user.one.ex90@example.com
SIP Proxy1	expc.internal-domain.net
EX60 (uses SIP protocol)	
SIP URI	user.two.mxp@example.com
SIP Proxy1	expc.internal-domain.net
EX60 at home (uses SIP protocol)	
SIP URI	user.three.mxp@example.com
SIP Proxy1	expe.example.com

## What To Do Next

The Expressway routing configuration is now complete. Go to the next section, "*System Checks*."

## 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 in **Configuration > Zones > Zones**.

If the traversal zone is not active, do the following:

- Review the traversal zone configuration.
- Check 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, page 56](#).
- Check 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.

### Registration Status

Check that all endpoints which are expected to be registered are actually registered to the relevant Expressway. And that they are registering the expected aliases. All successfully registered endpoints are listed on **Status > Registrations > By device**.

If the expected endpoints are not registered, review the following items:

- The endpoint's registration configuration.
- The SIP domains ([Task 7: Configuring SIP Domains, page 22](#)).
- Any registration restriction configuration applied to the Expressway (optional, [Task 18: Configuring Registration Restriction Policy \(Optional\), page 41](#)).

In some cases, home endpoints may fail to register when using SRV records. This can happen if the endpoint uses the home router for its DNS server, and the router's DNS server software doesn't support SRV records lookup. (Also applies to the DNS server being used by a PC when Jabber Video is running on it.) If registration failure occurs, do either of the following:

- Change the DNS server on the endpoint to use a publicly available DNS server which can resolve SRV record lookups. For example, Google – 8.8.8.8
- Change the SIP server address on the endpoint to use the FQDN of a node in the Expressway cluster and not the cluster SRV record. So that the device performs an AAAA or A record lookup.

### 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**).

### What To Do Next

When you've completed the system checks and are satisfied that the system is working as expected, [create a system backup](#) and then go on to "Optional Configuration Tasks".

## 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 15: Configuring Routes to a Neighbor Zone (Optional)

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

#### Example: Cisco VCS Neighbor Zone

This example assumes that you want to route calls toward devices (typically H.323 devices) that are registered to a Cisco VCS. The devices that are registered to the Cisco VCS have an address (destination alias) in the format `<alias>@vcs.domain`. (You may need more 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, and leave all other fields with their default values:

	Expressway-C	Expressway-E
<b>Name</b>	Enter Neighbor zone to VCS	Not applicable
<b>Type</b>	Neighbor	
<b>H.323 Mode</b>	On	
<b>H.323 Port</b>	Enter 1719	
<b>SIP Mode</b>	On	
<b>SIP Port</b>	Enter 5061	
<b>SIP Transport</b>	TCP	
<b>Location Peer 1 address</b>	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**.

## Optional Configuration Tasks

## 3. Configure the search rule fields as follows:

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

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 16: Configuring Cisco TMS (Optional)

The following configuration enables the Expressway system to be integrated to a Cisco TelePresence Management Suite (Cisco TMS).

Points to note:

- Further configuration tasks are also required on Cisco TMS to fully integrate the Expressway with the TMS server. For details, see *Cisco TMS Administrator Guide* on the [TMS Maintain and Operate Guides page](#).
- Enabling SNMP speeds up the Expressway – TMS integration process, but is not essential.
- Expressway-E integration with TMS requires additional firewall / NAT configuration. Expressway-E needs to access port 80/443 on Cisco TMS from outside the firewall. See [Appendix 3: Firewall and NAT Settings, page 56](#).

To enable and configure SNMP:

## Optional Configuration Tasks

1. Go to **System > SNMP**.
2. Configure the SNMP fields as follows:

	Expressway-C	Expressway-E
<b>SNMP mode</b>	<i>v3 plus TMS support</i>	Same as Expressway-C
<b>Community name</b>	Check that it is <code>public</code>	
<b>System contact</b>	Enter <code>IT administrator</code>	
<b>Location</b>	Enter <code>example.com head office</code>	
<b>Username</b>	Enter <code>VCS</code>	
<b>Authentication mode</b>	<i>On</i>	
<b>Type</b>	<i>SHA</i>	
<b>Password</b>	Enter <code>ex4mpl3.c0m</code>	
<b>Privacy mode</b>	<i>On</i>	
<b>Type</b>	<i>AES</i>	
<b>Password</b>	Enter <code>ex4mpl3.c0m</code>	

3. Click **Save**.

**SNMP** You are here: [System](#) > [SNMP](#)

**Configuration**

SNMP mode: v3 plus TMS support ⓘ

Community name: public ⓘ

System contact: IT administrator ⓘ

Location: example.com head office ⓘ

Username: VCS ⓘ

**Authentication**

Authentication mode: On ⓘ

Type: SHA ⓘ

Password: ..... ⓘ

**Privacy**

Privacy mode: On ⓘ

Type: AES ⓘ

Password: ..... ⓘ

**Save**

To configure the necessary external manager (Cisco TMS) parameters:

## Optional Configuration Tasks

1. Go to **System > External manager**.
2. Configure the fields as follows:

	Expressway-C	Expressway-E
<b>Address</b>	Enter 10.0.0.14	Same as Expressway-C
<b>Path</b>	Enter tms/public/external/management/SystemManagementService.asmx	
<b>Protocol</b>	Select <i>HTTP</i> or <i>HTTPS</i>	
<b>Certificate verification mode</b>	Select <i>On</i> or <i>Off</i>  The certificate is only verified if the value is <i>On</i> and the protocol is set to <i>HTTPS</i> . If you switch this on then Cisco TMS and Expressway must have appropriate certificates.	

3. Click **Save**.

**External manager** You are here: [System](#) > External manager

**Configuration**

Address	<input type="text" value="10.0.0.14"/>	
Path	<input type="text" value="tms/public/external/management/SystemManagementService.asmx"/>	
Protocol	<input type="button" value="HTTP"/>	
Certificate verification mode	<input type="button" value="On"/>	

## Task 17: Configuring Logging (Optional)

The following configuration enables event logs to be sent to an external logging server using the SYSLOG protocol.

- The **Local event log verbosity** setting controls the granularity of event logging. 1 is the least verbose, 4 the most.
- We recommend a minimum level of 2. This provides both system and basic signaling message logging.

The Expressway-E needs further firewall / NAT configuration for external logging. See [Appendix 3: Firewall and NAT Settings, page 56](#) for details.

To configure a logging server:



## Optional Configuration Tasks

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

	Expressway-C	Expressway-E
<b>Local event log verbosity</b>	2	2
<b>Remote syslog server 1: Address</b>	Enter 10.0.0.13	Enter 10.0.0.13
<b>Remote syslog server 1: Message Format</b>	IETF syslog format	IETF syslog format

3. Click **Save**.

## Task 18: Configuring Registration Restriction Policy (Optional)

You can limit the aliases that endpoints can register, using either an Allow list or a Deny list. This is an example of how to configure Allow list registration restrictions:

1. Go to **Configuration > Registration > Allow List**.
2. Click **New**.
3. Create an allow pattern by configuring the following fields. This example limits registrations to endpoints which register with an identity that contains "@example.com".

	Expressway-C
<b>Description</b>	Enter Only allow registrations containing "@example.com"
<b>Pattern type</b>	Regex
<b>Pattern string</b>	Enter .*@example\.com

4. Click **Add Allow List pattern**.

**Create allow pattern** You are here: [Configuration](#) > [Registration](#) > [Allow List](#) > Create allow pattern

Configuration

Description

Only allow registrations containing "@example.com" ⓘ

Pattern type

Regex ⓘ

Pattern string

.\*@example.com ⓘ

Add Allow List pattern

Cancel

To activate the registration restriction:

1. Go to **Configuration > Registration > Configuration**.
2. Configure the **Restriction policy** as follows:

	Expressway-C
<b>Restriction policy</b>	Allow List

## Optional Configuration Tasks

3. Click **Save**.

## Task 19: Configuring Device Authentication Policy (Optional)

Authentication policy is applied by the Expressway at the zone and subzone levels. It controls how the Expressway challenges incoming messages (for provisioning, registration, phone books, and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the Expressway.

Each zone and subzone can set its **Authentication policy** to *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone configuration (or the relevant alternative subzone).
- Initial provisioning subscription request authentication is controlled by the Default Zone configuration.
- Call and phone book request authentication is controlled by the Default Subzone (or relevant alternative subzone) if the endpoint is registered, or by the Default Zone if the endpoint is not registered.

By default, zones and subzones are configured as *Do not check credentials*.

## Using Delegated Credential Checking

If you have enabled device authentication in your network (by using an **Authentication policy** of *Check credentials*) and you have remote workers (outside the enterprise) with SIP devices, you should consider enabling delegated credential checking. In summary, this would require you to:

- Set up a secure traversal zone between the Expressway-E and the Expressway-C.
- Enable the Expressway-E and the Expressway-C's SIP settings, traversal zones and required SIP domains for delegated credential checking.
- Configure the Expressway-C with the relevant authentication mechanisms.

This means that remote workers can now register to the Expressway-E (assuming it has its **SIP registration proxy mode** set to *Off*) and be authenticated securely via the Expressway-C against an authentication mechanism inside the enterprise.

See [Device Authentication on Expressway Deployment Guide](#) for full information on configuring device authentication and delegated credential checking.

## Task 20: Restricting Access to ISDN Gateways (Optional)

We recommend that you restrict unauthorized access to any ISDN gateway resources (also known as toll-fraud prevention). Some methods to achieve this are described here.

In these examples, an ISDN gateway is registered to the Expressway-C with a prefix of 9. And / or it has a neighbor zone specified that routes calls starting with a 9.

## Expressway-E

Two search rules are created on the Expressway-E:

## Optional Configuration Tasks

- Both rules have a pattern string that matches calls directed at the ISDN gateway. (In this example calls prefixed with a 9.)
- The first rule has a **Source** of *All zones*. This allows calls from registered endpoints and neighbor zones to pass through to the traversal zone.
- The second rule is similar to the first rule but has a **Source** of *All*. So it includes nonregistered endpoints (which are excluded from the previous rule). They 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**.

## Optional Configuration Tasks

## 3. Configure the fields as follows:

	<a href="#">Expressway-E</a>
<b>Rule name</b>	Enter <code>Allow ISDN call</code> for example
<b>Description</b>	Enter <code>Allow ISDN calls for registered devices and neighbors</code>
<b>Priority</b>	Enter <code>40</code> (these rules must be the highest priority in the search rule configuration)
<b>Protocol</b>	<i>Any</i>
<b>Source</b>	<i>All zones</i>
<b>Request must be authenticated</b>	<i>No</i>
<b>Mode</b>	<i>Alias pattern match</i>
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter <code>(9\d+) (@example.com)</code>
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	Enter <code>\1</code>
<b>On successful match</b>	<i>Stop</i>
<b>Target</b>	<i>TraversalZone</i>
<b>State</b>	<i>Enabled</i>

## Optional Configuration Tasks

**Create search rule** You are here: [Configuration](#) ▶ [Dial plan](#) ▶ [Search rules](#) ▶ Create search rule

**Configuration**

Rule name	★ Allow ISDN call ⓘ
Description	Allow ISDN calls for neighbors ⓘ
Priority	★ 40 ⓘ
Protocol	Any ⓘ
Source	AllZones ⓘ
Request must be authenticated	No ⓘ
Mode	Alias pattern match ⓘ
Pattern type	Regex ⓘ
Pattern string	★ (9ld+)(@example.com) ⓘ
Pattern behavior	Replace ⓘ
Replace string	\1 ⓘ
On successful match	Stop ⓘ
Target	★ TraversalZone ⓘ
State	Enabled ⓘ

4. Click **Create search rule**.

5. Click **New**.

## Optional Configuration Tasks

## 6. Configure the fields as follows:

	Expressway-E
<b>Rule name</b>	Enter <code>Block ISDN call</code> for example
<b>Description</b>	Enter <code>Blocks everything (including nonregistered endpoints)</code>
<b>Priority</b>	Enter <code>41</code>
<b>Protocol</b>	<i>Any</i>
<b>Source</b>	<i>Any</i>
<b>Request must be authenticated</b>	<i>No</i>
<b>Mode</b>	<i>Alias pattern match</i>
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter <code>(9\d+) (.*) (@example.com)</code>
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	Enter <code>do-not-route-this-call</code> for example
<b>On successful match</b>	<i>Stop</i>
<b>Target</b>	<i>TraversalZone</i>
<b>State</b>	<i>Enabled</i>

## Optional Configuration Tasks

**Create search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

**Configuration**

Rule name  ⓘ

Description  ⓘ

Priority  ⓘ

Protocol  ⓘ

Source  ⓘ

Request must be authenticated  ⓘ

Mode  ⓘ

Pattern type  ⓘ

Pattern string  ⓘ

Pattern behavior  ⓘ

Replace string  ⓘ

On successful match  ⓘ

Target  ⓘ

State  ⓘ

7. Click **Create search rule**.

**Search rules** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#)

Priority	State	Rule name	Protocol	Source	Authentication required	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	Actions
<input type="checkbox"/> 40	✓ Enabled	<a href="#">Allow ISDN call</a>	Any	AllZones	No	Alias pattern match	Regex	(9ld+)(@example.com)	Replace	Stop	<a href="#">TraversalZone</a>	<a href="#">ViewEdit</a>
<input type="checkbox"/> 41	✓ Enabled	<a href="#">Block ISDN call</a>	Any	Any	No	Alias pattern match	Regex	(9ld+)(@example.com)	Replace	Stop	<a href="#">TraversalZone</a>	<a href="#">ViewEdit</a>
<input type="checkbox"/> 50	✓ Enabled	<a href="#">LocalZoneMatch</a>	Any	Any	No	Any alias				Continue	<a href="#">LocalZone</a>	<a href="#">ViewEdit</a>

## Expressway-C

This example describes how to configure the Expressway-C to stop calls that come in through the gateway, from being able to route calls back out of the gateway.

To do this, you load some specially constructed CPL onto the Expressway-C and configure its **Call policy mode** to use *Local CPL*.

## Creating a CPL File

The CPL file can be created in a text editor.

Here are two example sets of CPL. In these examples:

- “GatewayZone” is the neighbor zone to the ISDN gateway.
- “GatewaySubZone” is the subzone to the ISDN gateway (required if the gateway registers the 9 prefix to the Expressway).
- Calls coming into the ISDN gateway and hitting a FindMe do not ring devices that use the gateway. So for example, calls forwarded to a mobile phone are disallowed.

This example CPL excludes any checking of whether 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"
```

## Optional Configuration Tasks

```

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>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" 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>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" 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:




## Optional Configuration Tasks

1. Go to **Configuration > Call Policy > Configuration**.
2. Click **Browse....** Select the CPL file you created in the previous step from your file system.
3. Click **Upload file**.
  - If the file upload succeeds, you see a "File upload successful" message.
  - If you receive an "XML invalid" message, correct the problems with the CPL file and upload it again.
4. Select a **Call policy mode** of *Local CPL*.
5. Click **Save**.





**Call Policy configuration** You are here: [Configuration](#) > [Call Policy](#) > Configuration

**Configuration**

Call Policy mode Local CPL 

**Save**

**Policy files**

Call policy file	CPL File	<span>Show Call Policy file</span> 
CPL XSD file	XSD File	<span>Show CPL XSD file</span> 
CPL extensions xsd file	XSD File	<span>Show CPL extensions XSD file</span> 
Select the new Call Policy file		<input type="text"/> <span>Browse...</span> 

**Upload file**

## 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 > Network interfaces > IP
IPv4 gateway	10.0.0.1	System > Network interfaces > IP
LAN1 subnet mask	255.255.255.0	System > Network interfaces > 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

## Appendix 1: Configuration Details

Configuration item	Value	Expressway page
Mode	Any alias	Configuration > Dial plan > Search rules
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 > Network interfaces > IP
IPv4 gateway	192.0.2.1	System > Network interfaces > IP
LAN1 subnet mask	255.255.255.0	System > Network interfaces > 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

## Appendix 1: Configuration Details

Configuration item	Value	Expressway page
Protocol H.323 port	6001	Configuration > Zones > Zones
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	(?!.*@example\.com.*\$).*	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		

## Appendix 1: Configuration Details

Configuration item	Value	Expressway page
Pattern string	([^\@]*)	Configuration > Dial plan > Transforms
Pattern type	Regex	Configuration > Dial plan > Transforms
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*). This allows:

- External endpoints registration messages to be routed to the Expressway-E.
- Calls 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 Expressway 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

## Appendix 2: DNS Records

## 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
<b>H.323 traversal calls using Assent</b>							
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 *
<b>SIP traversal calls</b>							
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 *
<b>When ICE is enabled on Expressway-C zones and the Expressway-E is used as the TURN server</b>							
TURN server control	EXPc	EXPe	Any	>=1024	UDP	192.0.2.2	3478 **
TURN server media	EXPc	EXPe	Any	>=1024	UDP	192.0.2.2	24000 to 29999

\* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > 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).



## Appendix 3: Firewall and NAT Settings

## Inbound (DMZ &gt; 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 &gt; 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

## Appendix 3: Firewall and NAT Settings

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
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
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 systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

## Outbound (DMZ &gt; 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

### Prerequisites

- Apply an **Advanced Networking** option key on any Expressway-E that needs static NAT or two LAN interfaces.  
The **Advanced Networking** option is available only on the Expressway-E.
- Disable SIP and H.323 ALGs (SIP / H.323 awareness) on routers/firewalls carrying network traffic to or from the Expressway-E.  
We strongly recommend disabling this functionality on the firewall/s when deploying an Expressway-E behind a NAT, because our experience shows that they do not handle video traffic properly. You must use the Expressway to perform the static network address translation on its own interface. Read more in [What About Routers/Firewalls with SIP/H.323 ALG?](#), page 62.

### Planning Your Deployment

#### Do Not Overlap Subnets

The recommended deployment of the Expressway-E configures 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 the peers have the **Advanced Networking** option installed, you must use the LAN1 interface address of each peer to create the cluster.
- The LAN interface that you use for clustering must not have **Static NAT mode** enabled.

For these reasons, we recommend that you use LAN2 as the externally facing interface, and also enable static NAT on LAN2 when it's required.

#### External LAN Interface Setting

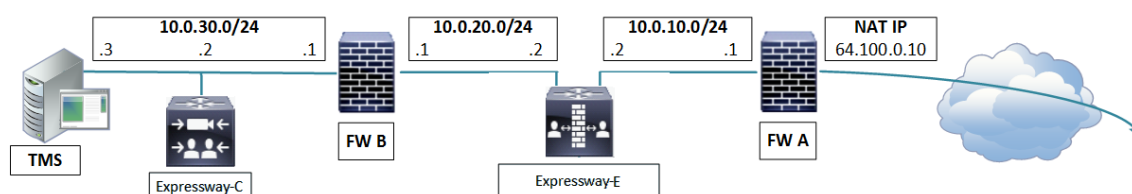
The **External LAN interface** configuration setting, on the **IP** configuration page, controls where the Expressway-E's TURN server allocates TURN relays. In the recommended dual NIC deployment, you should select the externally-facing LAN interface (LAN2) on the Expressway-E.

### Recommended: Dual NIC Static NAT Deployment

The following example illustrates the recommended deployment. It shows the typical DMZ configuration where the internal and external firewalls cannot route directly to each other, and dual NIC devices such as Expressway-E are required to validate and forward the traffic between the isolated subnets.

The Expressway-E has both NICs enabled, and it has static NAT enabled on its outward-facing LAN interface. The Expressway-C inside the network is a traversal client of the Expressway-E in the DMZ.

**Figure 7 Dual Network Interfaces Deployment**



## Appendix 4: Advanced Network Deployments

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
- Firewall A is the outward-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)

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 Towards the Internal Network

With a deployment like [Figure 7 Dual Network Interfaces Deployment, page 59](#), you would typically configure the private address of the external firewall (10.0.10.1 in the diagram) as the default gateway of the Expressway-E. Traffic that has no more specific route is sent out from either Expressway-E interface to 10.0.10.1.

- **If the internal firewall (B) is doing NAT** for traffic from the internal network (subnet 10.0.30.0 in diagram) to LAN1 of the Expressway-E (for example traversal client traffic from Expressway-C), that traffic is recognized as being from the same subnet (10.0.20.0 in diagram) as it reaches LAN1 of the Expressway-E. The Expressway-E will therefore be able to reply to this traffic through its LAN1 interface.
- **If the internal firewall (B) is not doing NAT** for traffic from the internal network (subnet 10.0.30.0 in diagram) to LAN1 of the Expressway-E (for example traversal client traffic from Expressway-C), that traffic still has the originating IP address (for example, 10.0.30.2 for traffic from Expressway-C in the diagram). You must create a static route towards that source from LAN1 on the Expressway-E, or the return traffic will go to the default gateway (10.0.10.1). You can do this on the web UI (**System > Network interfaces > Static routes**) or using `xCommand RouteAdd` at the CLI.

If the Expressway-E needs to communicate with other devices behind the internal firewall (eg. for reaching network services such as NTP, DNS, LDAP/AD and syslog servers), you also need to add static routes from Expressway-E LAN1 to those devices/subnets.

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.

**Figure 8 The Web UI for Creating a Static Route**

The `xCommand RouteAdd` command and the equivalent web UI, are detailed in the Expressway help and the *Expressway Administrator Guide*.

## Background Information

### The Challenge of NAT for SIP and H.323 Applications

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.

### How Does Expressway-E Address This Challenge?

To ensure that call signaling and media connectivity remains functional in scenarios where the Expressway-E is deployed behind a NAT, 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 and replace these with the public NAT address of the NAT router.

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. You do not have to use both interfaces, but we recommend that you do. If you choose to use a single interface, and enable static NAT on that interface, read [Why We Advise Against Using These Types of Deployment](#), page 64.

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 > Network interfaces > IP**) has additional options, allowing the user to decide whether to **Use dual network interfaces**, to

## Appendix 4: Advanced Network Deployments

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.

When enabling **IPv4 static NAT mode** on an interface, 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 are replaced with the IPv4 static NAT address configured for this interface. 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 a public IP address.

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.

### What About 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.

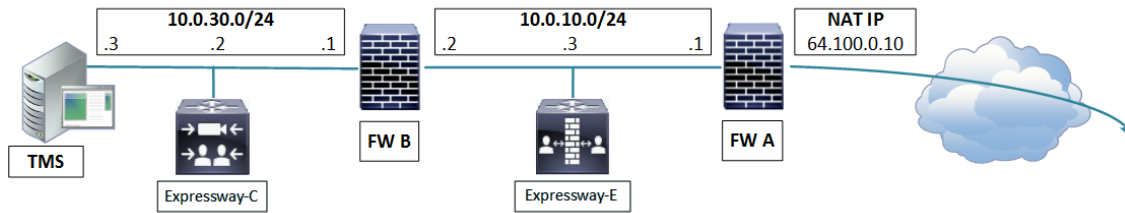
As per the recommendations in the Introduction section of this appendix, it is highly recommended to disable SIP and H.323 ALGs on routers/firewalls carrying network traffic to or from a Expressway-E, as, when enabled this is frequently found to negatively affect the built-in firewall/NAT traversal functionality of the Expressway-E itself. This is also mentioned in [Appendix 3: Firewall and NAT Settings, page 56](#).

### Other Deployment Examples

**Note:** Using the Expressway-E as shown in these examples could have a serious impact on your network bandwidth, and may contravene your security policy. We strongly recommend that you use the [Recommended: Dual NIC Static NAT Deployment, page 59](#). Read [Why We Advise Against Using These Types of Deployment, page 64](#).

#### Single Subnet DMZ Using Single Expressway-E LAN Interface and Static NAT

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.

**Figure 9 Single Subnet DMZ – Single LAN Interface and Static NAT**

This deployment consists of the following elements:

- Single subnet DMZ (10.0.10.0/24) with the following interfaces:
  - Internal interface of firewall A – 10.0.10.1
  - External interface of firewall B – 10.0.10.2
  - LAN1 interface of Expressway-E – 10.0.10.3
- LAN subnet (10.0.30.0/24) with the following interfaces:
  - Internal interface of firewall B – 10.0.30.1
  - LAN1 interface of Expressway-C – 10.0.30.2

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** is enabled for LAN1 on the Expressway-E, with a static NAT address of 64.100.0.10.

---

#### Note:

You must enter the FQDN of the Expressway-E, as it is seen from outside the network, as the peer address on the Expressway-C's secure traversal zone. The reason for this is that in static NAT mode, the Expressway-E requests that incoming signaling and media traffic should be sent to its external FQDN, rather than its private name.

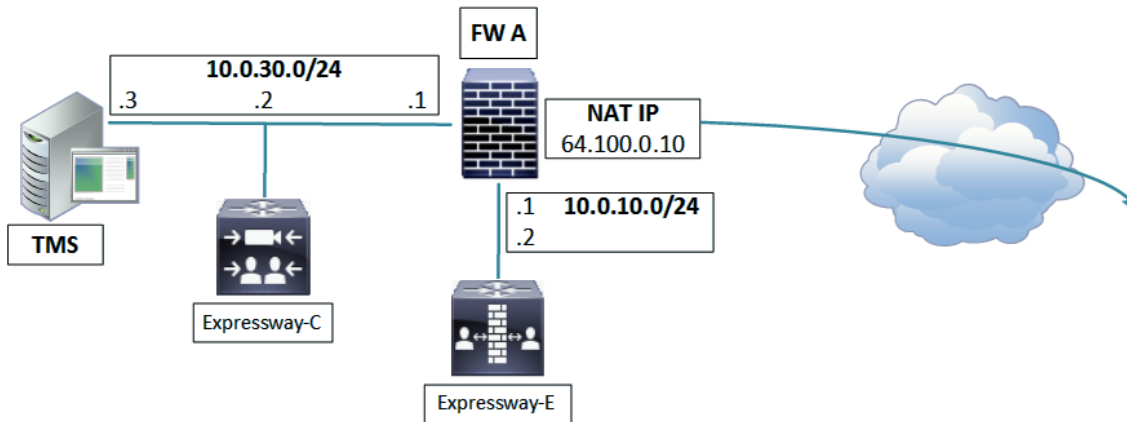
**This also means that the external firewall must allow traffic from the Expressway-C to the Expressway-E's external FQDN. This is known as NAT reflection, and may not be supported by all types of firewalls.**

---

So, in this example, firewall A must allow NAT reflection of traffic coming from the Expressway-C that is destined for the external address, that is 64.100.0.10, of the Expressway-E. The traversal zone on the Expressway-C must have 64.100.0.10 as the peer address.

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 through 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, asymmetric routing occurs. Which may or may not work, depending on the firewall capabilities.

### 3-port Firewall DMZ Using Single Expressway-E LAN Interface



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

- DMZ subnet (10.0.10.0/24) with the following interfaces:
  - DMZ interface of firewall A – 10.0.10.1
  - LAN1 interface of Expressway-E – 10.0.10.2
- LAN subnet (10.0.30.0/24) with the following interfaces:
  - LAN interface of firewall A – 10.0.30.1
  - LAN1 interface of Expressway-C – 10.0.30.2
  - 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 is enabled for LAN1 on the Expressway-E, with a static NAT address of 64.100.0.10.

The Expressway-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.

---

**Note:** 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 described in [Single Subnet DMZ Using Single Expressway-E LAN Interface and Static NAT](#), page 62.

**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.**

---

### Why We Advise Against Using These Types of Deployment

For deployments that use only one NIC on the Expressway-E, but also require static NAT for the public address, the media must "hairpin" or reflect on the external firewall whenever media is handled by the Expressway-E's back to back user agent (B2BUA).

For all calls coming in on a Unified Communications Traversal Server zone, or another zone where SIP **Media encryption mode** is not *Auto*, the Expressway-E's B2BUA could be engaged to decrypt or encrypt the media packets. In these deployments, the B2BUA sees the public IP address of the Expressway-E instead of its private IP address, so the media stream must go through the network address translator to get to the private IP address.



## Appendix 4: Advanced Network Deployments

- Not all firewalls will allow this reflection, and it is considered by some to be a security risk.
- Each call where the B2BUA is engaged will consume three times as much bandwidth as it would using the recommended dual NIC deployment. This could adversely affect call quality.

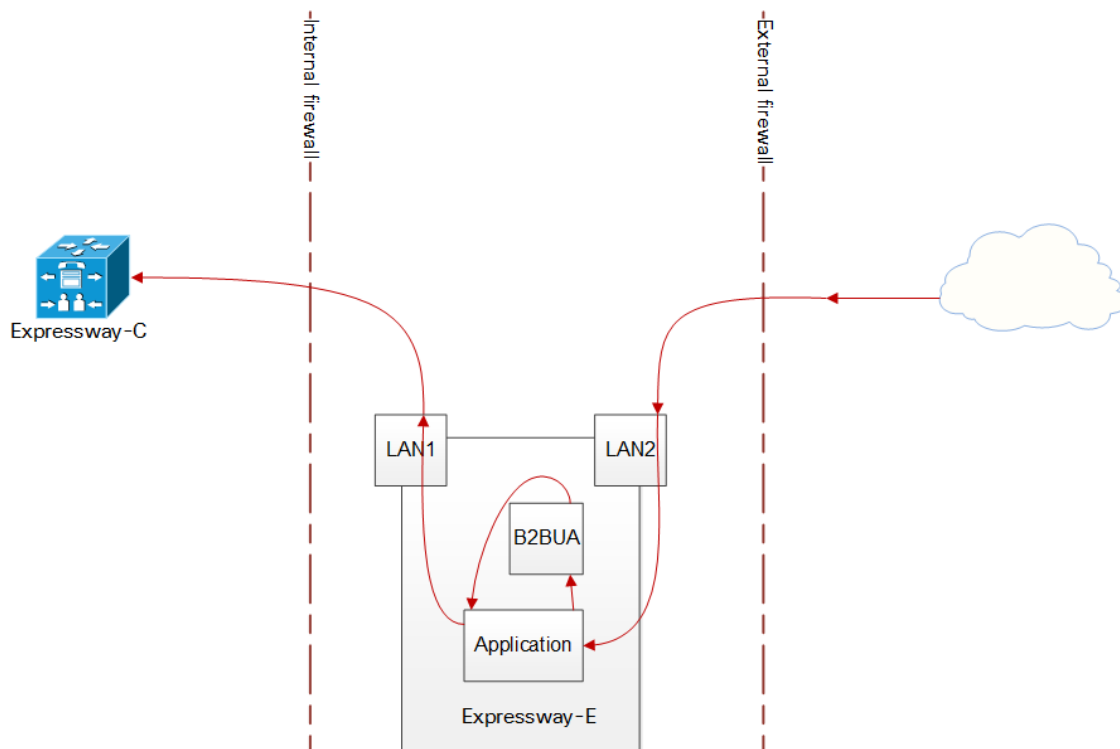
**Figure 10 Media Path in Dual NIC Static NAT Example (Recommended)**

Figure 11 Media Path in Single NIC Static NAT Example

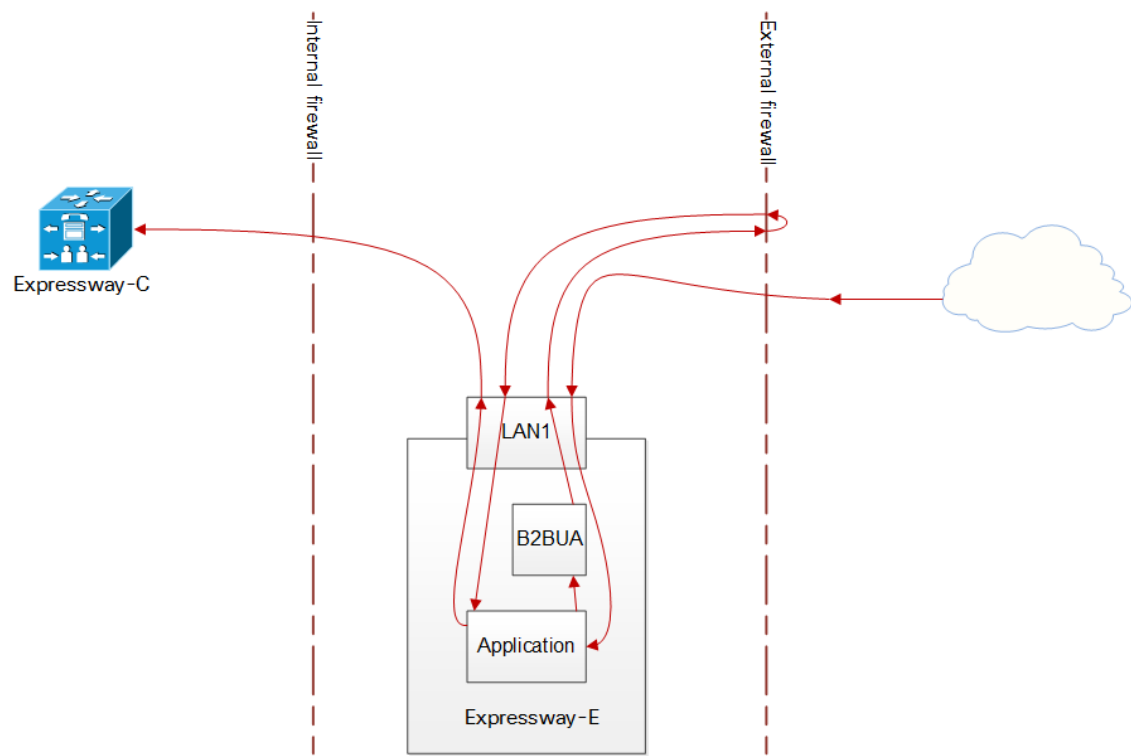
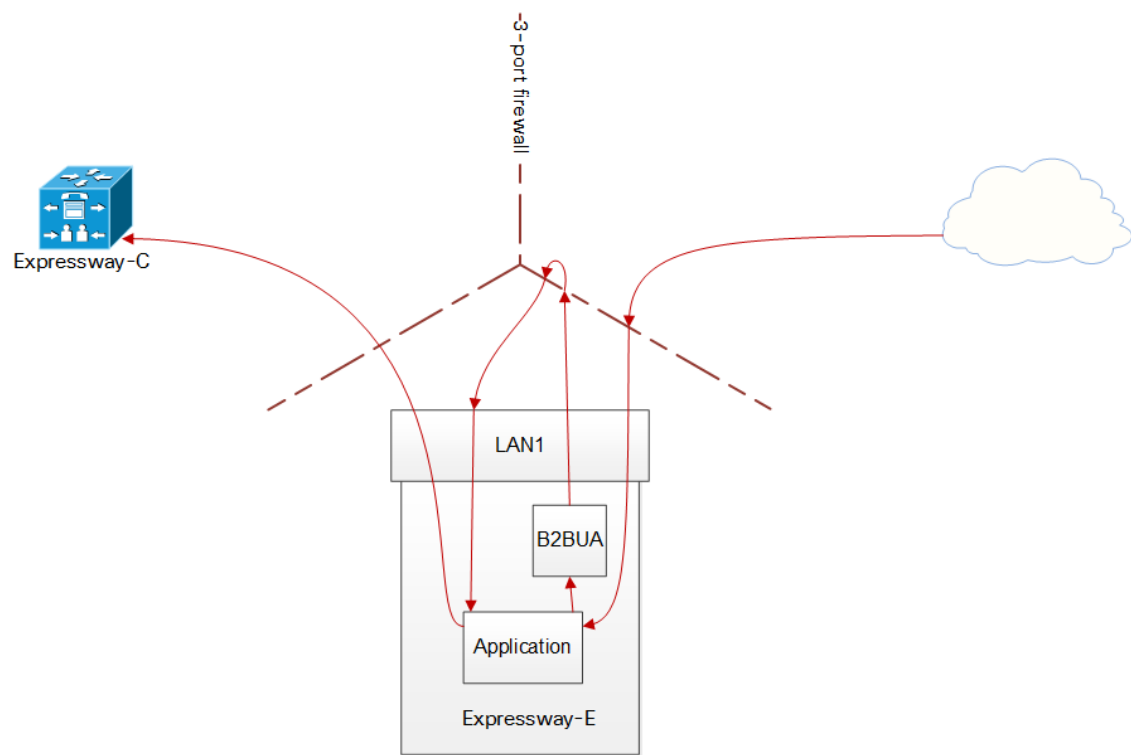


Figure 12 Media Path in 3-port Firewall Static NAT Example



## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

## Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

© 2016 Cisco Systems, Inc. All rights reserved.

## Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)