Introduction

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 licenses and any optional feature keys.

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.

• DNS records required for the example deployment used in this document are in Appendix 2: DNS Records.

• Details of required NAT and firewall configurations are in Appendix 3: Firewall and NAT Settings.

  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 Networking Deployments.

For descriptions of all system configuration parameters, see the Expressway Administrator Guide and the online help.

Example configuration values in this guide

For ease of reading this guide is based around an example deployment with the following assumed configuration values:

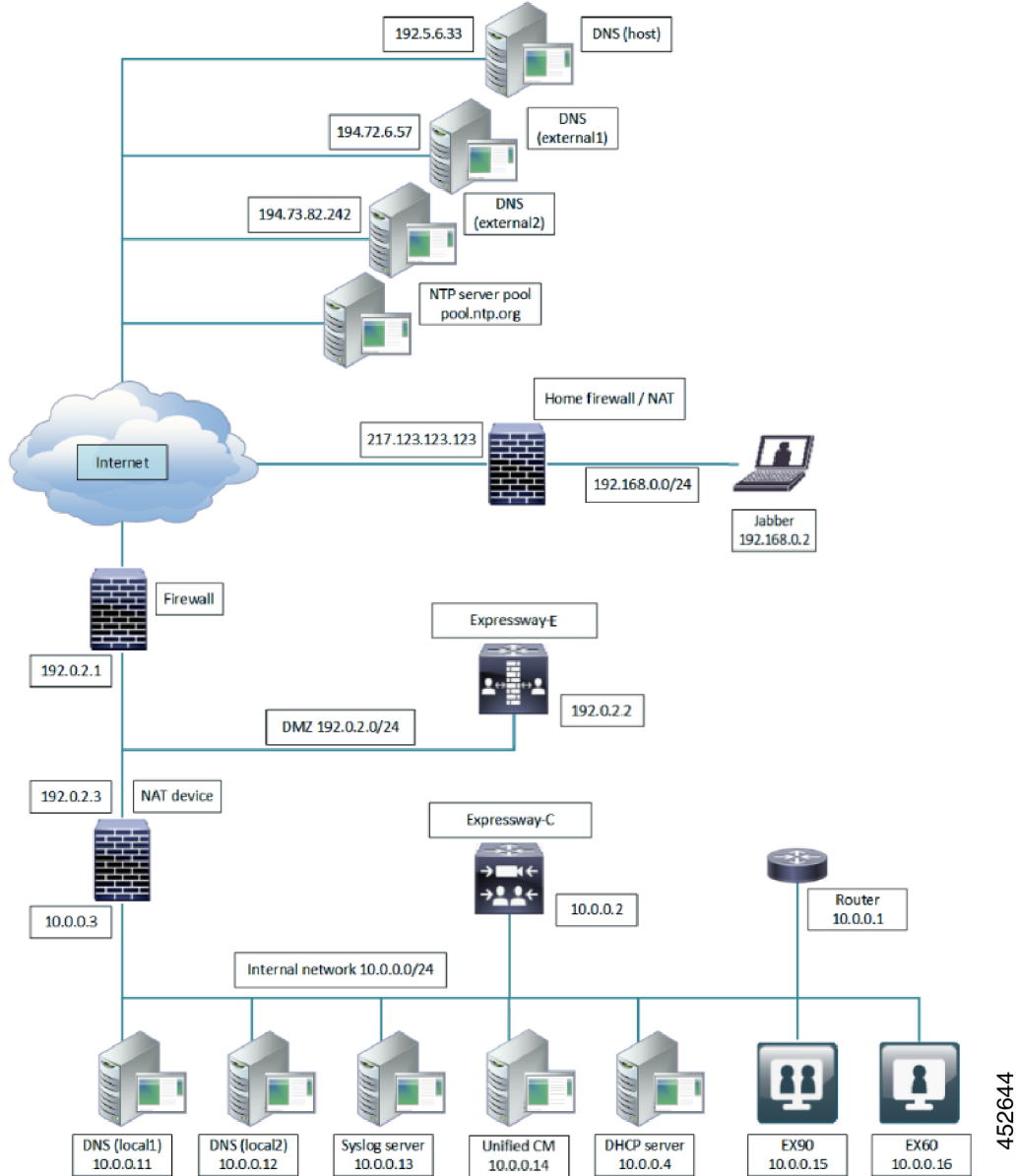|	**Expressway-C**	**Expressway-E**
LAN1 IPv4 address	10.0.0.2	192.0.2.2
IPv4 gateway	10.0.0.1	192.0.2.1
LAN1 subnet mask	255.255.255.0	255.255.255.0
Domain name	*internal-domain.net*	*example.com*

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).

- *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.

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, H.323 Gatekeeper for devices located on the internal network, 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 Task 16: Configuring Cisco TMS (Optional).
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 *Mobile and Remote Access via Cisco Expressway Deployment Guide* on the Expressway Configuration Guides page.
Syslog Server	Logging server for Syslog messages. See Task 17: Configuring Logging (Optional).
NTP Server	Provides the clock source used to synchronize devices.

DMZ Network Element

Expressway-E

The Expressway-E is a SIP Registrar & Proxy and H.323 Gatekeeper for devices which are located outside the internal network (for example, home users and mobile workers registering to Unified CM across the internet and 3 rd 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.

- Home firewall NAT (PAT) device which performs port address and firewall functions for network traffic originating from the EX60 device.

- See Appendix 4: Advanced Networking Deployments for information about how to deploy your system with a static NAT and Dual Network Interface architecture.

SIP and H.323 Domain

The example deployment is configured to route SIP (and H.323) signaling messages for calls made to URIs which use the domain example.com. The DNS SRV configurations are described in Appendix 2: DNS Records.

- 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 (for example, before

an external endpoint registers, it will query the external DNS servers to determine the IP address of the Expressway-E).

- 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.