# Chapter 2: Network Infrastructure Considerations for Cisco Unity Express

**Revised: August 18, 2009**

Cisco Unity Express is an IP application that physically integrates into a router chassis and that takes advantage of the infrastructure provided by the host router and the associated IP network connected to the router.

The specific sections in this chapter address the following aspects of your IP network that can affect Cisco Unity Express implementations:

- IP Connectivity, page 7
- Private and Public Addressing, page 9
- Date and Time, page 13
- TFTP and FTP Servers, page 15
- TTY Port Numbers, page 16
- Security, page 18
- System Management Considerations, page 31
- Power Backup, page 33

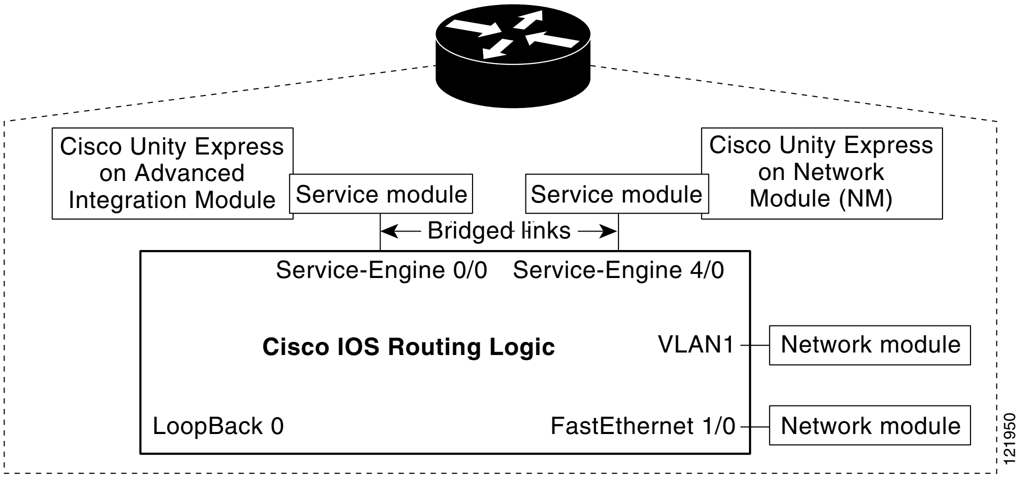
## IP Connectivity

The Cisco Unity Express module connects to its host router via a back-to-back Ethernet configuration that physically travels across the backplane of the router. The Cisco Unity Express module has an internal IP address and a default gateway configuration. The service-engine interface on the router has its own IP address which may be configured as unnumbered. The following sections illustrate the IP connectivity configuration options for the Cisco Unity Express module.

Topics addressed in this section include the following:

- IP Unnumbered, page 8
- Stub Network, page 9
- VLAN, page 9

*Figure 5 IP Connectivity Configuration*



# IP Unnumbered

The most common way to configure the Cisco Unity Express module is to use the unnumbered IP address method. An **ip unnumbered** command configuration, shown in the following configuration fragment, allows the Cisco Unity Express module to consume an IP address in the subnet of the network associated with a particular router egress port, such as FastEthernet 0/0. The router interface with which the Cisco Unity Express interface is associated must be in an “up” state at all times for Cisco Unity Express to communicate.

**Note** This method requires the configuration of a static route to the service-engine interface.

IP unnumbered configuration example:

```
interface FastEthernet0/0
 ip address b.68.10.1 255.255.255.0
!
interface Service-Engine4/0
 ip unnumbered FastEthernet0/0
 service-module ip address b.68.10.10 255.255.255.0
 service-module ip default-gateway b.68.10.1
!
ip route b.68.10.10 255.255.255.255 Service-Engine4/0
```

The IP address of the Cisco Unity Express module in the example is b.68.10.10. The default-gateway on the Service Engine must be set to the IP address of the Ethernet interface on the router that the unnumbered statement refers to (b.68.10.1 in the example). If this is a Cisco CME deployment, then this default-gateway setting must be the Cisco CME router.

It is also possible to use a subinterface or a loopback interface as the **ip unnumbered** command parameter (such as **`ip unnumbered fastethernet0.1`**).

## Stub Network

Stub network configuration requires Cisco Unity Express to have its own IP subnet assigned, but does not require a static route. Using a stub network is one recommended approach for configuring Cisco Unit Express when using a private address space. When implementing a stub network configuration, the IP address must be routable, so that the TFTP/FTP server used for software installation or backup-and-restore knows how to reach the Cisco Unity Express module. This is shown in the following configuration example:

Stub network configuration example:

```
router# show running-config
interface FastEthernet0/0
 ip address b.68.10.1 255.255.255.0
!
interface Service-Engine4/0
 ip address b.68.20.1 255.255.255.0
 service-module ip address b.68.20.10 255.255.255.0
 service-module ip default-gateway b.68.20.1
```

## VLAN

This configuration illustrates a situation in which an Etherswitch module is present in the router for which a VLAN interface is most commonly used. A VLAN-specific configuration is shown in the following configuration fragment and is very similar to the **ip unnumbered** configuration given in the "IP Unnumbered" section on page 8. A VLAN implementation also requires a static route.

VLAN configuration example:

```
interface VLAN1
 ip address b.68.10.1 255.255.255.0
!
interface Service-Engine4/0
 ip unnumbered VLAN1
 service-module ip address b.68.10.10 255.255.255.0
 service-module ip default-gateway b.68.10.1
!
ip route b.68.10.10 255.255.255.255 Service-Engine4/0
```

# Private and Public Addressing

If you decide to configure an actual IP address for Cisco Unity Express (as opposed to using unnumbered), the next decision is to determine the type of IP address that should be assigned. The IP address can be public or private.

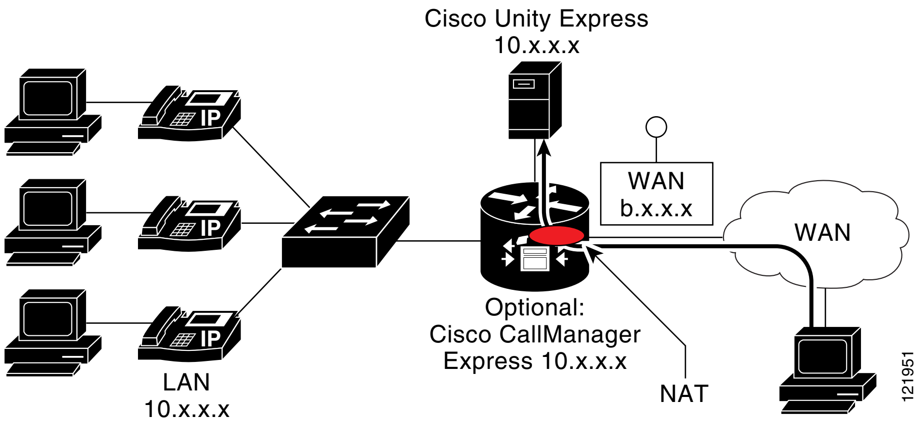
Topics addressed in this section include the following:

- Private Addressing, page 10
- Public Addressing, page 10
- Cisco Unity Express with Private Addressing and Cisco CME with Public Addressing, page 11
- NAT, page 11
- Network Infrastructure Configuration Trade-Offs for Cisco Unity Express, page 12
- Best Practises, page 13

## Private Addressing

In many voice networks, the voice devices have private addresses (indicated by 10.x.x.x), while the WAN link may have a public address (indicated by b.x.x.x). You can assign private addresses to both Cisco CME (if present in the deployment) and Cisco Unity Express in order to fit in a large network and also for voice security reasons. This design is shown in Figure 6.

***Figure 6 Cisco Unity Express with a Private Address***

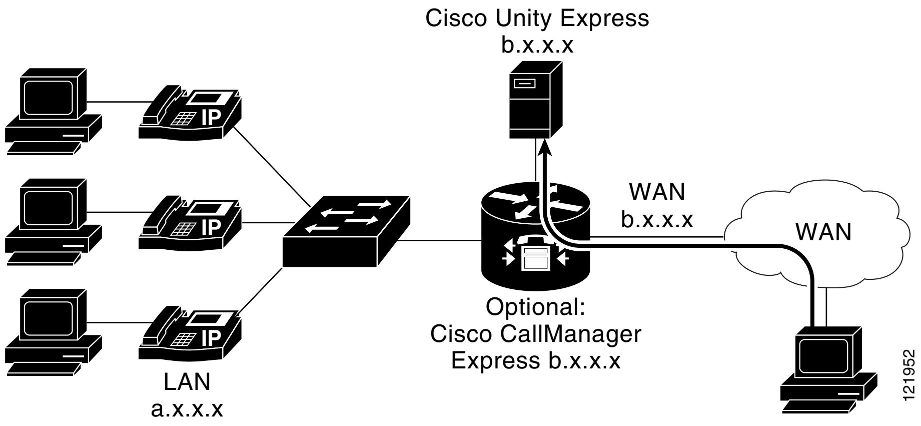


If you choose this design, then remote management access via HTTP—for the Cisco Unity Express or Cisco CME graphical user interface (GUI)—must pass through Network Address Translation (NAT) to be able to reach the Cisco Unity Express module. The GUI uses both the Cisco IOS HTTP server as well as an HTTP server on the Cisco Unity Express module.

## Public Addressing

In this configuration, Cisco Unity Express has a public addresses (indicated by b.x.x.x). If Cisco CME is present, it too has a public address that is assigned to it. This makes sense in networks where voice devices in general have public addresses, or where remote management access to Cisco Unity Express or Cisco CME must work without requiring NAT. This design is shown in Figure 7.

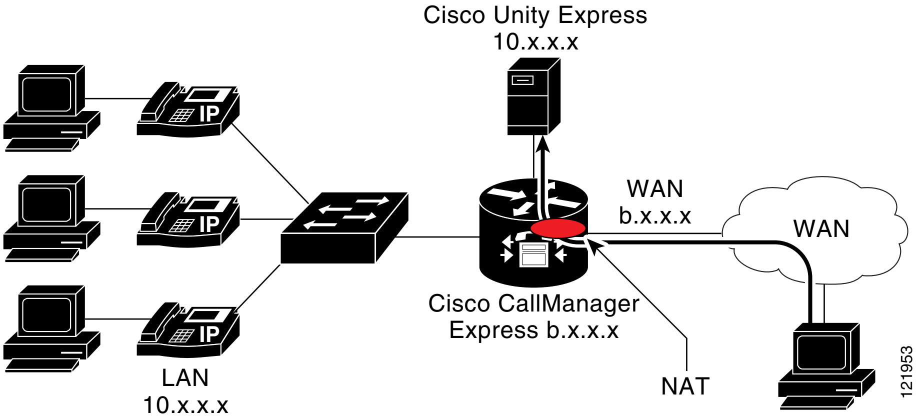
***Figure 7 Cisco Unity Express with a Public Address***



# Cisco Unity Express with Private Addressing and Cisco CME with Public Addressing

In a Cisco CME deployment, it is possible to configure Cisco Unity Express with a private address (indicated by 10.x.x.x), like the phones and other telephony devices, while Cisco CME has a public address (indicated by b.x.x.x) assigned. This is a common scenario in a cable- or DSL-attached branch office location where a single public address is allocated to the site. All outbound H.323 traffic would use the Cisco CME public address for voice traffic while the IP Phones and Cisco Unity Express addresses remain "hidden" from the network. This design is shown in Figure 8.

*Figure 8 Cisco Unity Express with Private Addressing and Cisco CME with Public Addressing*



The side effect of the configuration is that while Cisco CME is remotely accessible (HTTP for GUI), the Cisco Unity Express GUI—which is integrated with the Cisco CME GUI—still requires NAT to work with the configuration, as described in "Private Addressing" section on page 10.

# NAT

Network Address Translation (NAT) affects Cisco Unity Express implementation. These considerations are discussed in the following sections.

## GUI Access

If NAT is required for remote GUI (HTTP) access, use the following configuration process:

**Step 1** Assign a private address to the Cisco Unity Express interface.

**Step 2** Create a static source NAT IP translation.

**Step 3** Make the service-engine interface the inside interface.

**Step 4** Make the FastEthernet interface the outside interface.

A NAT configuration is shown in the following:

```
router# show running-config
interface FastEthernet0/0
```

```
 ip address b.19.153.38 255.255.255.0
 ip nat outside
!
interface Service-Engine2/0
  ip address 10.10.10.1 255.255.255.0
  ip nat inside
  service-module ip address 10.10.10.2 255.255.255.0
  service-module ip default-gateway 10.10.10.1
!
ip nat inside source static tcp 10.10.10.2 80 b.19.153.38 80
```

This configuration allows access to the Cisco Unity Express GUI (at http://b.19.153.38/, not 10.10.10.2), as well as Telnet access to the router.

**Note** If this is a Cisco CME deployment, access to the integrated Cisco Unity Express and Cisco CME GUI works correctly, but access to the Cisco CME-specific GUI (http://b.19.153.38/telephony-service.html) does not work as port 80 is being accessed via NAT. To restore operation to the Cisco CME-specific GUI (if access to this is required in the deployment), the HTTP port for Cisco CME must be changed to something other than 80. Use the **ip http port** *port* configuration command.

This ensures that the Cisco CME HTTP server uses a different port. To access the Cisco CME GUI, use a port-specific URL, such as http://b.19.153.38:<port>/telephony_service.html. Any other HTTP access to the servers on the private LAN also requires configuration to use a port other than 80.

A static NAT statement for port 21 might also be needed to enable remote FTP software installation or upgrade for Cisco Unity Express.

### Java Telephony Application Programming Interface

Java Telephony Application Programming Interface (JTAPI) communications does not currently work via NAT or firewall, so you cannot configue Cisco Unity Express on the other side of NAT from a Cisco CallManager controlling calls via JTAPI.

### Voice Mail Networking

Cisco Unity Express voice mail networking (VPIM) configurations with NAT will be addressed in subsequent releases of this document.

## Network Infrastructure Configuration Trade-Offs for Cisco Unity Express

The previous sections covered different types of configurations. Some trade-offs to consider when deciding between these options include the following:

- Address availability—If spare subnets are available, the best way to configure the Cisco Unity Express module is to put it on its stub network. If IP addressing is tight, the unnumbered approach is best, and you can use a loopback interface if one is available.
- Reliable reachability of Cisco Unity Express AA and voice mail—A key consideration is to ensure that the Cisco Unity Express module is always reachable. If an interface fails and the Cisco Unity Express module is using the failed module as its unnumbered interface, then AA and voice mail applications are not reachable. If the unnumbered approach is used for IP addressing, use a loopback interface and not a physical interface.

- Remote management—For a Cisco CME deployment, GUI access uses an HTTP server in Cisco IOS as well as an HTTP server on the Cisco Unity Express module. For the GUI to work, HTTP traffic to both Cisco CME and Cisco Unity Express must be routable. If Cisco Unity Express is given a private network address, use NAT to route HTTP traffic to the private address. CLI access is not affected by the IP addressing (private, public or unnumbered) scheme used by Cisco Unity Express, as CLI access always uses Telnet to the router, but not to the Cisco Unity Express IP address.
- Security—Reachability of network addresses may be a concern in some networks, and for this reason you may decide to use a private address for Cisco Unity Express. One view is that Cisco Unity Express is a host device (server) on the network that just happens to be integrated in the router chassis; therefore, it should have a routable and reachable address from your internal network. An opposite view is that the casual user on your internal network should not be able to reach the Cisco Unity Express IP address in any direct manner (such as ping) for security reasons; therefore, Cisco Unity Express should be a “hidden” device with a private address, and traffic specifically destined to Cisco Unity Express (like the GUI HTTP) should go through NAT.

## Best Practises

The preceding sections describe the different options and tradeoffs for configuring the IP addresses for Cisco Unity Express. In general, the recommended way to configure Cisco Unity Express IP addressing is shown in the following configuration example, which shows an IP unnumbered interface referencing a loopback interface to guard against LAN and WAN interface failures affecting the availability of Cisco Unity Express.

```
interface Loopback0
 ip address a.32.152.9 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip bind srcaddr a.32.152.9
!
interface Loopback2
 ip address a.32.152.241 255.255.255.252
 ip ospf network point-to-point
!
interface Service-Engine4/0
 ip unnumbered Loopback2
 service-module ip address a.32.152.242 255.255.255.252
 service-module ip default-gateway a.32.152.241
!
ip route a.32.152.242 255.255.255.255 Service-Engine4/0

GigabitEthernet3/0       unassigned      YES unset  administratively down down
Service-Engine4/0        a.32.152.241   YES TFTP   up                    up
Loopback2                a.32.152.241   YES NVRAM  up                    up
```

**Note** Enable IP routing on the router for packets to be forwarded to the Cisco Unity Express application.

# Date and Time

Date and time for Cisco Unity Express are controlled via two configurations of the system:

- Timezone and geographic area configuration
- Network Time Protocol (NTP) source

Topics addressed in this section include the following considerations:

- Operation, page 14
- Best Practices, page 14

## Operation

While the Cisco Unity Express module has its own onboard clock, you cannot set the clock via the GUI or the CLI. The clock is controlled entirely via NTP, which is in Coordinated Universal Time (UTC), and the timezone setting (the offset from UTC to local time). The clock is synchronized with the NTP source during Cisco Unity Express software startup. While Cisco Unity Express is running, small clock drifts are corrected, but no large (greater than 1 second) clock changes take place until the software is rebooted.

**Note** On a Cisco CME system with Cisco Unity Express, the GUI clock-set capability in the **Configure** > **System Parameters** > **System Time** GUI window displays and controls the Cisco CME (router) clock, not the Cisco Unity Express module clock. Setting the router's clock has no effect on Cisco Unity Express, unless the router is also defined as the NTP server for Cisco Unity Express (not a recommended configuration).

The following is an example Cisco Unity Express module configuration that is required to set the NTP source for the clock:

```
ntp server b.19.153.31
```

When you initially insert the Cisco Unity Express module into a router and apply power, the software (installed by the factory), has already started up by the time the IP addressing and other basic configuration is done. After the NTP configuration is completed on both the router and the Cisco Unity Express module, you must restart the application to synchronize the clocks.

Cisco Unity Express 2.0 and later releases contain an NTP auto-sync feature that automatically resets the Cisco Unity Express clock if a discrepancy of more than 0.5 second is detected. In older Cisco Unity Express releases, resetting the clock for discrepancies of larger than 1 second required a software reboot.

## Best Practices

The following practices are recommend for optimal date and time control:

- Use a robust NTP server in your network for maximum clock stability.
- Use the Cisco Unity Express host router (or any other low-end router) as the NTP server only as a last resort. A host router can easily incur clock drift and does not contain batteries to maintain clock settings over a power cycle.
- Use multiple NTP servers to enhance the reliability of clock synchronization and server availability. Up to three NTP servers can be configured for Cisco Unity Express. The NTP protocol's algorithm determines which NTP server is the most stable and draws its clock from that server.

# TFTP and FTP Servers

The Cisco Unity Express bootloader uses TFTP to load the RAM-based Linux kernel (cue_installer) from a network location as the first step of a software installation or upgrade. This is the only use of TFTP in the Cisco Unity Express system. FTP is used for the remainder of the software installation and upgrade, as well as for backup and restore communication.

Topics addressed in this section include the following:

- FTP Server Location and Access, page 15
- FTP Packages, page 15
- FTP Server Configuration Guidelines, page 16

## FTP Server Location and Access

Setup the FTP server so that all Cisco Unity Express sites using it have reliable, high-speed, and secure access to the FTP server. The following are considerations to take into account:

- Backup and restore bandwidth required—The size of the backup depends on the Cisco Unity Express license (number of mailboxes) and storage capacity of each site. If only the Cisco Unity Express system's configuration is backed up, very little bandwidth is needed. If the system's voice mail message content is also backed up, then much higher bandwidth is needed.
- Security of the FTP connection—A Cisco Unity Express backup or restore operation transmits the voice message content over the FTP connection. If ensuring the privacy of this information is important, use IPSec technology between the Cisco Unity Express site and the FTP server.
- Security of information on the FTP server—A Cisco Unity Express backup is stored unencrypted in files on the FTP server. Ensure that access to the FTP server's accounts and disk drives are secured from tampering and unintended access. Choose strong passwords for FTP server account access.
- Cisco Unity Express system access to the FTP server—Ensure that Cisco Unity Express can access the FTP server by either name or IP address. If the FTP server is accessed by name, then ensure that Cisco Unity Express is DNS enabled. Any firewall between the FTP server and Cisco Unity Express must allow FTP traffic to go through.

## FTP Packages

This section does not provide any Cisco endorsement or recommendation of FTP packages. It simply lists some FTP packages that have been tested with Cisco Unity Express.

- Linux
  - ProFTPD 1.2.8 Server
  - PureFTPd
  - WU-FTPD
- Windows
  - FileZilla FTP Server 0.8.8
  - GuildFTPd
  - Serv-U
  - Microsoft IIS FTP

**Note** An FTP package that is known to be incompatible with Cisco Unity Express is the TYPSoft FTP server. When a file does not exist on the FTP server, the TYPSoft FTP server returns 501 (Syntax error in parameters or arguments) instead of 550 (Requested action not taken. File unavailable).

## FTP Server Configuration Guidelines

There are numerous FTP servers and they all have different configurations. This section provides only general guidelines for the types of features and characteristics your FTP server should have to work with Cisco Unity Express:

- The FTP server must support PASV mode (PASSIVE FTP). Ensure that PASV mode is enabled on the FTP server (if there is an option for this).
- Don’t use anonymous FTP for Cisco Unity Express Backup and Restore.
- Use the default port (Port 21) for the FTP server.
- When creating user accounts, ensure that each user account is assigned a different home directory.
- Give full permissions to the user over the home directory. Ensure that the user account can upload and download files. Also ensure that the user can create, modify, delete, and rename files and directories from the home directory.
- Ensure that there is enough disk space on the FTP server. Regularly monitor the disk space on the FTP server.
- If a particular directory is configured as the backup directory for Cisco Unity Express, do not manually delete any files or directories from the directory that is configured on Cisco Unity Express. The Backup and Restore service on Cisco Unity Express manages the contents of the directory, cross-references files from different subdirectories, and indexes files into the log files. For example, if Cisco Unity Express is using ftp://server.com/backupdir as the configured backup URL, and "bkpuser" as the user account, then the backup files go into the directory "~bkpuser/backupdir". Cisco Unity Express automatically creates this directory. Do not delete any files/directories under the "backupdir" directory.
- If a single FTP server is used to store backups from multiple Cisco Unity Express sites, ensure that the directory for each site is different. For example, if there are five sites, configure the backup URL for the sites as ftp://server.com/backupdir/site1, ftp://server.com/backupdir/site2 etc.

# TTY Port Numbers

The TTY port numbers for the Cisco Unity Express module varies based on the router platform model and router slot where the Cisco Unity Express hardware is inserted. Generally this TTY number is not needed, except to do the following

- Enter a password on the TTY line for security reasons (to prohibit unauthorized telnet access to Cisco Unity Express).
- Clear the line in the event the previous session was disconnected without clearing the line properly.
- Force a security session inactivity disconnect for Cisco Unity Express CLI session.

The TTY port number formulas for different router platforms and Cisco Unity Express hardware is given in Table 3.

*Table 3 Cisco Unity Express TTY Formulas*

| Router Platform | NM-CUE | AIM-CUE |
|---|---|---|
| Cisco 2600XM and Cisco 3700 | 2000 + ((NM-slot-num * 32) + 1) | 2000 + (( number-of-NM-slots in router + 1) * 32) + AIM-slot-num + 1 |
| Cisco 2811, Cisco 2821, Cisco 2851 | 2 + (NM-slot-num * 64) | 2 + ((number-of-NM-slots-in-router + 2 + AIM-slot-num) * 64) |
| Cisco 3800 | 2 + (NM-slot-num * 64) | 2 + ((number-of-NM-slots-in-router + 1 + AIM-slot-num) * 64) |

The Cisco 2600XM series routers have one AIM slot (0/0) while the Cisco 2691, Cisco 2800 series, Cisco 3700 series and Cisco 3800 series all have two AIM slots (0/0 and 0/1).

The TTY ports for Cisco Unity Express NMs are given in Table 4, while AIM numbering is given in Table 5.

*Table 4 NM-CUE TTY Port Numbers*

| Platform | NM-CUE Slot | TTY Port Number |
|---|---|---|
| Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745 | 1/0 | 2033 |
| Cisco 3725, Cisco 3745 | 2/0 | 2065 |
| Cisco 3745 | 3/0 | 2097 |
| Cisco 3745 | 4/0 | 2129 |
| Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, Cisco 3845 | 1/0 | 66 |
| Cisco 3825, Cisco 3845 | 2/0 | 130 |
| Cisco 3845 | 3/0 | 194 |
| Cisco 3845 | 4/0 | 258 |

*Table 5 AIM-CUE TTY Port Numbers*

| Platform | Number of NM Slots | AIM-CUE Slot | TTY Port Number |
|---|---|---|---|
| Cisco 2600XM, Cisco 2691 | 1 | 0/0 | 2065 |
| Cisco 2691 | 1 | 0/1 | 2066 |
| Cisco 3725 | 2 | 0/0 | 2097 |
| Cisco 3725 | 2 | 0/1 | 2098 |
| Cisco 3745 | 4 | 0/0 | 2161 |
| Cisco 3745 | 4 | 0/1 | 2162 |

*Table 5 AIM-CUE TTY Port Numbers*

| Platform | Number of NM Slots | AIM-CUE Slot | TTY Port Number |
|---|---|---|---|
| Cisco 2801 | 0 | 0/0 | 66 |
| Cisco 2801 | 0 | 0/1 | 130 |
| Cisco 2811, Cisco 2821, Cisco 2851 | 1 | 0/0 | 194 |
| Cisco 2811, Cisco 2821, Cisco 2851 | 1 | 0/1 | 258 |
| Cisco 3825 | 2 | 0/0 | 194 |
| Cisco 3825 | 2 | 0/1 | 258 |
| Cisco 3845 | 4 | 0/0 | 322 |
| Cisco 3845 | 4 | 0/1 | 386 |

# Security

The following topics summarize network security strategies that aid in preventing unauthorized access to Cisco Unity Express:

- System and Remote Access, page 18
- Toll Fraud Prevention, page 21
- Application Environment, page 22
- User Interfaces and Login Types, page 27
- Security Best Practices, page 31

## System and Remote Access

There are no external interfaces on the Cisco Unity Express hardware (physically there is an FE interface port, but it is disabled in software and unusable). All access must pass through the host router and across the backplane to the NM-CUE or AIM-CUE.

### Local Access

The only local access to a Cisco Unity Express system is via the host router's console interface into the router CLI and then opening a "session" to the Cisco Unity Express CLI by using the following command:

```
service-module service-Engine x/y session
```

Entering this command requires you to be in enable mode on the router which is protected by the router's enable login and password settings. Although there is also an enable mode in the Cisco Unity Express module CLI, Cisco Unity Express has no password capability. Any network administrator with access to enable mode on the router, also can access the Cisco Unity Express CLI. There is no user ID or password control on the Cisco Unity Express CLI. Access is controlled via the router, and if logging is required, set up the router with AAA/RADIUS monitoring of login access.

GUI access via a browser to Cisco Unity Express is always considered remote access as it is across an IP segment from the router.

## Remote Access via Telnet

The following IP configuration is used as the baseline configuration in this section:

```
interface FastEthernet0/0
 ip address b.19.153.41 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Service-Engine1/0
 ip unnumbered FastEthernet0/0
 service-module ip address b.19.153.37 255.255.255.0
 service-module ip default-gateway b.19.153.41
```

Direct telnet access to the Cisco Unity Express IP address is disabled by default as shown in the following example:

```
pc> telnet b.19.153.37
Trying b.19.153.37...
telnet: Unable to connect to remote host: Connection refused
```

Remote CLI access to Cisco Unity Express is therefore only possible via telnet to the router (b.19.153.41) and then by the using the session command to get access to the Cisco Unity Express CLI. That way, all the security protections that are built into telnet access to your router automatically also protect access to Cisco Unity Express. A Telnet session to the router, followed by a session into Cisco Unity Express is shown in the following example:

```
pc> telnet b.19.153.41
Trying b.19.153.41...
Connected to b.19.153.41.
Escape character is '^]'.

User Access Verification

Password:
lab-2691>enable
Password:
lab-2691#service-module service-Engine 1/0 session
Trying b.19.153.41, 2033 ... Open
```

Telnet to the router address, followed by the explicit TTY port number that is allocated to Cisco Unity Express (which depends on the slot where it is inserted as per Table 4 and Table 5) is not blocked and can provide undesirable "direct" access to Cisco Unity Express as shown in the following example:

```
pc> telnet b.19.153.41 2033
Trying b.19.153.41...
Connected to b.19.153.41.
Escape character is '^]'.

User Access Verification

Password:
Password OK
```

To protect against this kind of access, insert a login and password configuration on the TTY port. In this example, the Cisco Unity Express module is in slot 1/0 on a Cisco 2691 and has a TTY port of 2033 leading to Cisco Unity Express as shown in the following configuration example:

Configuration example for login/password on telnet access:

```
line 33
 password cisco
 flush-at-activation
 no activation-character
 login
 no exec
 transport preferred none
 transport input all
```

## Access Timeout

Cisco Unity Express CLI access via the TTY port in the router (as described in the "Local Access" section on page 18 and the "Remote Access via Telnet" section on page 19) does not time out by default. The connection stays up until it is disconnected by the user who initiated it. If an inactivity timeout on access to Cisco Unity Express CLI is required, use the the **session-timeout** command on the router TTY configuration to disconnect the session after a configured number of minutes. The following example configuration of an inactivity timeout on Cisco Unity Express CLI access.

```
line 33
 session-timeout 5
 password 7 02050D480809
 login
```

## Remote Access via SSH

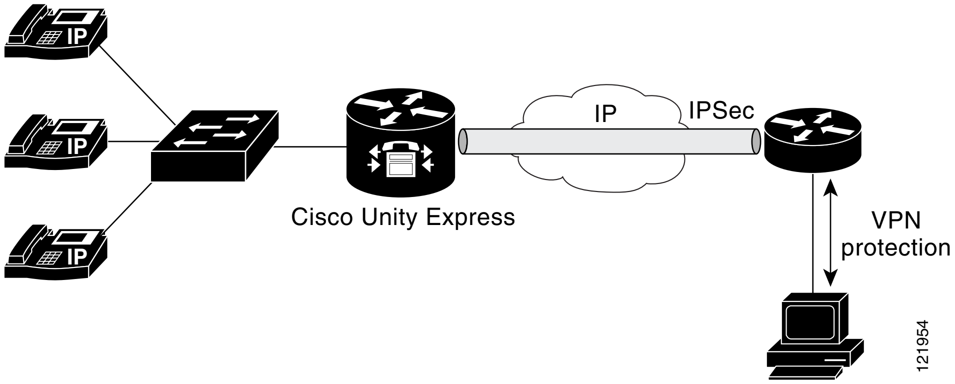
For secure CLI access to Cisco Unity Express, enable secure shell (SSH) on the router and use an SSH-enabled remote access application, such as the Secure Shell windows application.
Cisco Unity Express itself does not support SSH (but neither does it support telnet access), but communication between the router and Cisco Unity Express is via the router backplane.
Cisco Unity Express is not exposed to any external interfaces or IP segments. SSH access to the router is sufficient to protect telnet access to Cisco Unity Express.

## Remote Access via HTTPS

Cisco Unity Express does not support HTTPS for browser access. This capability is on the roadmap of security features to be added. While login to the GUI is password protected, the login ID and password currently travel in clear text across the IP network.

You can protect GUI access in Cisco Unity Express by using IPSec tunnels on the routers between the nearest router to where the browser is located and the router hosting the Cisco Unity Express module. You can use VPN technology to protect the segment between the client PC and the nearest router where IPSec is available, as shown in Figure 9. As an alternative, you can use VPN technology all the way from the client PC to the host router.

*Figure 9 Secure HTTP Access*



HTTPS is supported on Cisco CME, and requires at least the Cisco IOS 12.3.4T Advanced IP Services IOS image. HTTP access for Cisco Unity Express and the IP Phones (which do not support HTPPS/SSL) continue to use port 80, while the Cisco CME GUI access uses HTTPS on port 443. For this to work, include the following commands on the router:

**ip http server**

**ip http secure-server**

# Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports—By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)—Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports—If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060—If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration—If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.

- SIP Digest Authentication—If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers—Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on Cisco Unified CME, Cisco Unified SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns—Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules—Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts—Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation—Use the “permit hostname” feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)—If you are using DNS as the “session target” on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the “Cisco IOS Unified Communications Toll Fraud Prevention” paper.

# Application Environment

Cisco Unity Express is an IP application and therefore communicates with its environment via various TCP and UDP protocols and ports.

## Protocols and Port Numbers

The protocols and port numbers used by Cisco Unity Express are listed in Table 6.

*Table 6 Cisco Unity Express Protocols and Port Numbers*

| Protocol | Remote Source Port | Cisco Unity Express Destination Port | Cisco Unity Express Source Port | Remote Device Destination Port | Remote Device | Notes |
|---|---|---|---|---|---|---|
| | | | | | | |
| SSH | | | | | Secure Shell Client | Not supported on Cisco Unity Express. Use SSH to the host router. |
| Telnet | | | | | Telnet Client | Not supported on Cisco Unity Express. Use telnet to the host router. |
| DNS | | | TCP/UDP 53 | | DNS Servers | |
| TFTP | | | UDP 69 | | TFTP Server | Used for loading RAM kernel. |
| FTP | | | TCP 20 (data), TCP 21 (control) | | FTP Server | Used for software install; backup and restore. |
| HTTP | | TCP 80 | | | Administrator / User Web browsers | Cisco Unity Express and Cisco CME Admin and User browser access. |
| NTP | | UDP 123 | | | NTP server | Date/Time server. |
| SNMP | | | | | Network Management station | SNMP hardware inventory for Cisco Unity Express is supported out of the host router. Cisco Unity Express itself does not support SNMP. |
| Syslog | | TCP 514 | | | Syslog service | |
| SIP | | UDP 5060 | | | Cisco CME or SRST Host router | No SIP trunking is supported. |
| RTP | UDP 16384-32767 | UDP 16384-32767 | UDP 16384-32767 | UDP 16384-32767 | Voice Media | IP Phone and gateway ports. |
| JTAPI | | | | TCP 2748 | Cisco CallManager | Used for call control in Cisco CallManager deployments. |
| SMTP | | TCP 25 | TCP 25 | | Cisco Unity Express or Cisco Unity | Voice mail networking between sites. |

## Suggested Access Control Lists

The following IP configuration example applies to the description provided in this section:

**Note** As you customize the access control lists (ACLs) for your environment, substitute your network's configuration information into the appropriate places in the ACLs presented in this section.

```
service-module ip default-gateway b.19.153.41
Address of Cisco UE service module: b.19.153.37
FTP Server for software backup and download: a.10.1.150
Admin Subnet: a.10.1.0/24
IP Phone/GW Subnet: a.10.2.0/24
Syslog Server: a.10.1.160
DNS: a.10.1.170
Call manager server 1: b.84.23.10
Call manager server 2: b.84.23.11
```

The ACL in the following configuration examples are recommended to be used with Cisco Unity Express. The ACLs specific to Cisco CallManager should be included only if Cisco Unity Express is deployed with a Cisco CallManager. The following ACLs should be applied on the Cisco Unity Express service-engine interface on the router, as shown in Cisco Unity Express service-engine examples that follow.

Recommended inbound ACLs:

```
access-list 101 remark Filter Outbound Traffic from CUE - Apply Inbound on Interface
ServiceEngine
access-list 101 remark Restrict DNS to only a.10.1.170, add additional dns servers as
required
access-list 101 permit udp host b.19.153.37 host a.10.1.170 eq domain
access-list 101 permit tcp host b.19.153.37 host a.10.1.170 eq domain

access-list 101 remark Restrict TFTP to only the host router
access-list 101 permit udp host b.19.153.37 host b.19.153.41 eq tftp

access-list 101 remark Restrict FTP traffic to only a single server
access-list 101 permit tcp host b.19.153.37 host a.10.1.150 eq ftp
access-list 101 permit tcp host b.19.153.37 host a.10.1.150 eq ftp-data

access-list 101 remark Restrict NTP traffic to only the host router
access-list 101 permit udp host b.19.153.37 host b.19.153.41 eq ntp

access-list 101 remark Restrict Syslog traffic to single server
access-list 101 permit tcp host b.19.153.37 host a.10.1.160 eq syslog

access-list 101 remark Restrict SIP signaling to host router
access-list 101 permit tcp host b.19.153.37 host b.19.153.41 eq 5060
access-list 101 permit udp host b.19.153.37 host b.19.153.41 eq 5060

access-list 101 remark Restrict RTP to IP phone and GW segment plus router
access-list 101 permit udp host b.19.153.37 a.10.1.0 0.0.0.255 range 16384 32767
access-list 101 permit udp host b.19.153.37 host b.19.153.41 range 16384 32767

access-list 101 remark Restrict SMTP communication to host router
access-list 101 permit tcp host b.19.153.37 any eq smtp

access-list 101 remark Restrict CCM communication to host router
access-list 101 permit tcp host b.19.153.37 host b.84.22.11 eq 2748
access-list 101 permit tcp host b.19.153.37 host b.84.23.10 eq 2748
```

Recommended outbound ACLs:

```
access-list 102 remark Filter Traffic to CUE - Apply Outbound on Interface ServiceEngine
access-list 102 remark Restrict http access to management and phone segment
access-list 102 permit tcp a.10.1.0 0.0.0.255 host b.19.153.37 eq www
access-list 102 permit tcp a.10.2.0 0.0.0.255 host b.19.153.37 eq www

access-list 102 remark Restrict SIP signaling to host router
access-list 102 permit tcp host b.19.153.41 host b.19.153.37 eq 5060
access-list 102 permit udp host b.19.153.41 host b.19.153.37 eq 5060

access-list 102 remark Restrict RTP to IP phone and GW segment plus router
access-list 102 permit udp a.10.1.0 0.0.0.255 host b.19.153.37 range16384 32767
access-list 102 permit udp host b.19.153.41 host b.19.153.37 range 16384 32767

access-list 102 remark Restrict SMTP communication to host router
access-list 102 permit tcp host A.B.C.D host b.19.153.37 eq smtp

access-list 102 remark Restrict CCM communication to host router
access-list 102 permit tcp host b.84.22.11 eq 2748 host b.19.153.37
access-list 102 permit tcp host b.84.23.10 eq 2748 host b.19.153.37
```

The inbound ACL for SMTP `access-list 101 permit tcp host b.19.153.37 any eq smtp` allows Cisco Unity Express to send SMTP messages to any other host in the network. If you want to restrict this operation to allow Cisco Unity Express to send STMP traffic only to specific hosts in the network, then expand this ACL to list those hosts explicitly.

Similarly, in the outbound ACL for SMTP `access-list 102 permit tcp host A.B.C.D host b.19.153.37 eq smtp`, replace A.B.C.D with the explicit addresses of the hosts that you want to allow to send SMTP traffic to Cisco Unity Express.

Attach ACLs to the service-engine interface as follows:

```
interface Service-Engine1/0
 ip unnumbered FastEthernet0/0
 ip access-group 101 in
 ip access-group 102 out
 service-module ip address b.19.153.37 255.255.0.0
 service-module ip default-gateway b.19.153.41
```

## Operating System (Linux)

Cisco Unity Express is an embedded Linux-based application. There is no access via CLI, telnet, or any other interface into the Linux operating system.

## LDAP

While Cisco Unity Express includes an Lightweight Directory Access Protocol (LDAP) directory as part of the application, there is no access via CLI, telnet, or any other interface or protocol into LDAP— it is an entirely embedded system.

## SQL

While Cisco Unity Express includes an Structured Query Language (SQL) database as part of the application, there is no access via CLI, telnet, or any other interface or protocol into the database—it is an entirely embedded system.

## Software Installation

Cisco Unity Express 1.0 and 1.1 use TFTP for the initial installation step of loading the cue_installer image from a server. Cisco Unity Express 2.0 introduces an onboard installer that eliminates this step from the install process, except when the installer must be upgraded.

In all cases, the actual software installation uses FTP because of the following:

- TFTP is insecure and has no login/password control.
- FTP access can be secured with a login/password combination, even though the actual file transfer is not secure unless it travels over an IPSec-protected route between the FTP server and the Cisco Unity Express host router.

During the software installation, a command that is similar to the following is required to start loading software from the FTP server:

```
se-1-3-235-101installer#> s i p u ftp://a.3.61.16/cue-vm.1.1.1.pkg user ftpuser
```

In this example, “user” is the FTP account user ID, and “ftpuser” is the password. If the command is entered exactly as shown, then the password is echoed in clear text on the screen. If this operation is undesirable, omit the password from the “s i p u” command and the installer will prompt for a password (which is not echoed to the screen or stored anywhere).

## Software Image and File Checking

All the files that are used during a software or license installation on Cisco Unity Express contain digital signatures that are cross checked during software installation and start-up. You can view an example list of files at http://www.cisco.com/cgi-bin/tablebuild.pl/cue-netmodule11. This digital signature precludes rogue software from being installed or started on the Cisco Unity Express platform.

## Backup and Restore

Cisco Unity Express uses an FTP server for backup and restore. The FTP server’s password configuration in Cisco Unity Express is protected in the GUI (the field is blanked out) as well as in the CLI as shown in the following backup configuration show output examples:

```
cue# show backup
Server URL:                       ftp://127.0.0.1/ftp
User Account on Server:           test
Number of Backups to Retain:      20

cue# show running-config
backup server url "ftp://127.0.0.1/ftp" credentials hidden
"EWlTygcMhYmjazXhE/VNXHCkplVV4KjescbDaLa4fl4WLSPFvv1rWUnfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35jwAAA
AA="
```

There are several other considerations for securing backups. These include the following:

- The data transfer of the backup (or restore) uses FTP between Cisco Unity Express and the FTP server; therefore, only secured if this connection is protected by an IPSec tunnel between the router and the FTP server (or a router close to the FTP server).
- The storage of backup files is as secure as the access to the FTP server. The files are not encrypted unless you use an offline utility to encrypt these files after Cisco Unity Express has completed its backup (and decrypt them again before attempting a restore operation).

- All Cisco Unity Express user password fields (part of the user account information) inside the backed up files are encrypted. The backed up files are also encrypted on the Cisco Unity Express local storage and cannot be read directly or reverse engineered.

## User Interfaces and Login Types

Cisco Unity Express supports three separate user interfaces: GUI, CLI, and TUI, and two types of users:

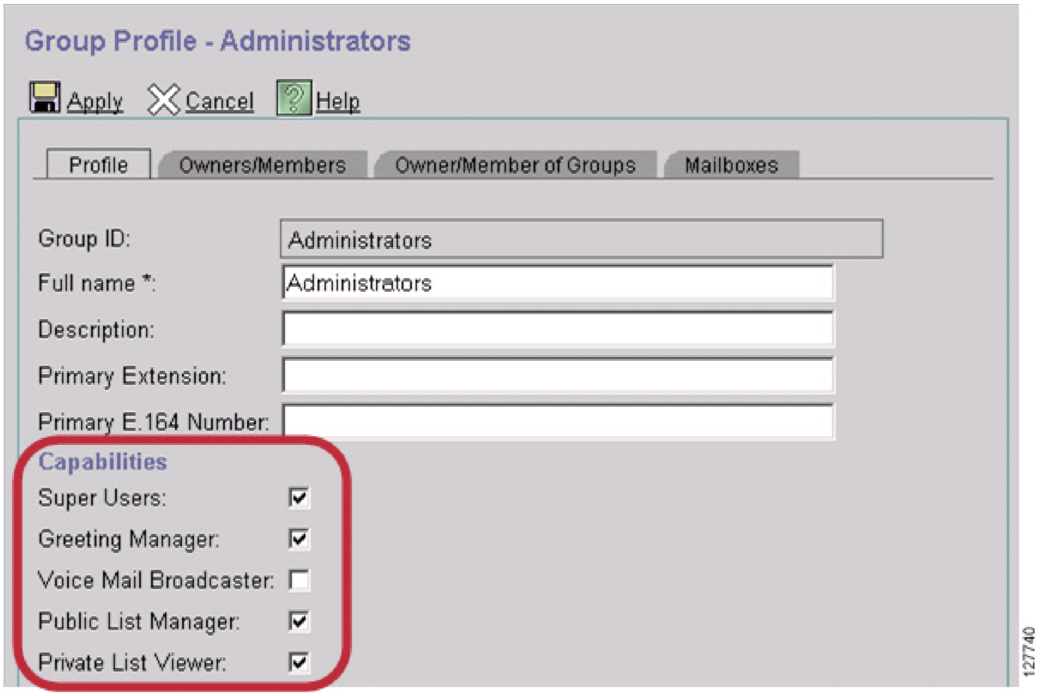
- Administrators—An administrator is a member of a group that has Super User privileges enabled. The system-default Administrators group has super-user privileges that are enabled by default, but you can also define your own groups that have this privilege.
- End users (subscribers)—A subscriber is defined as any user account that does not have Super User privileges enabled (in other words, any user account that is not a member of any group that has these privileges).

The following configuration example shows the CLI of a system with the system-default Administrators group as the only group in the system with super-user privileges. Two user accounts (administrator and admin) are members of this group and can therefore log in to the GUI with full access. Figure 10 shows a screenshot of the GUI configuration for the same parameters.

Administrator definition configuration example:

```
groupname Administrators member admin
groupname customer-service member bob
groupname customer-service member cary
groupname customer-service member ggarrett
groupname Administrators privilege superuser
groupname Administrators privilege ManagePrompts
groupname Administrators privilege ManagePublicList
groupname Administrators privilege ViewPrivateList
groupname Broadcasters privilege broadcast
```

*Figure 10 IP Connectivity Configuration*



Group Profile - Administrators

| | |
|---|---|
| Group ID: | Administrators |
| Full name *: | Administrators |
| Description: | |
| Primary Extension: | |
| Primary E.164 Number: | |

Capabilities

| | |
|---|---|
| Super Users: | ☑ |
| Greeting Manager: | ☑ |
| Voice Mail Broadcaster: | □ |
| Public List Manager: | ☑ |
| Private List Viewer: | ☑ |

Up to Cisco Unity Express 2.0, only the Super User and Greeting Manager were defined in the system. As of Cisco Unity Express 2.1, five privileges are defined:

- Super User—This privilege grants access to the full GUI window of the system and can do any configuration task.
- Greeting Manager—This privilege grants Administration via Telephony (AVT) TUI access to administer AA prompts.
- Voice Mail Broadcaster—This privilege grants AVT TUI access to send broadcast messages.
- Public List Manager—This privilege grants GUI access to define and administer public distribution lists.
- Private List Viewer: This privilege grants GUI access to view the existence and membership of other users' private distribution lists. No changes can be made.

The preceding privileges can be assigned (in any combination) to any group defined in the system. User accounts who are members of that group then inherit the group's privileges.

Up to Cisco Unity Express 2.0, a single default system group (Administrators) existed. It included the Super User and Greeting Manager privileges. As of Cisco Unity Express 2.1, two default system groups are defined with privileges as follows:

- Administrators—Super User, Greeting Manager, Public List Manager, and Private List Viewer
- Broadcasters—Voice Mail Broadcaster

Access to a Cisco Unity Express system is summarized in Table 7.

*Table 7 Cisco Unity Express Administrator and Subscriber Access Privileges*

| | Administrator | Subscriber |
|---|---|---|
| **GUI access** | Full GUI (all menus and fields). | View access to users and groups defined in the system. Modify access only to personal profile password, personal identification number (PIN), mailbox greeting, and mailbox 0-out destination. |
| **Password and PIN reset** | Access to password and PINs for all users on the system. Passwords cannot be viewed (unless the default assigned by the system is still active and the password has never been changed), but can be changed. | Access to own password only. Passwords cannot be viewed, but can be changed. |
| **CLI** | Via router access only. The Cisco Unity Express administrator or user account information is not used for this access. | None. |
| **Voice-mail TUI** | For own mailbox. Same as Subscriber access. | For own mailbox. |
| **AVT TUI—AA alternate greeting and customer prompts** | Yes. | No. |
| **AVT TUI—Broadcast messaging** | No. | Members of "Broadcasters" group only. |
| **AVT TUI—Remote User Administration** | Yes. | No. |

## Passwords and PINs

All Cisco Unity Express user accounts (administrator and subscriber) defined on the system are password controlled on login. Passwords are used for Web login access, while PINs are used for TUI mailbox and AVT login access.

Rules that govern passwords and PINs include the following:

- Passwords are mandatory, can be 3 to 32 characters long, are case sensitive, and allow alphabetic and numeric characters.
- PINs are mandatory, can be up to 3 to 16 digits long, and are numeric only.
- Passwords and PINs do not expire up to Cisco Unity Express 2.0. As of Cisco Unity Express 2.1, you can configure passwords and PINs to expire (with a default system setting of 30 days).
- Passwords and PINs are not checked against a history of recently used passwords. As of Cisco Unity Express 2.1, when a password or PIN expires, the most recently used password and PIN cannot be selected again.
- Passwords and PINs can never be viewed, displayed, or extracted from the system, passwords and pins are encrypted and stored with a one-way hash algorithm.

- Default passwords and PINs are assigned by the system when new user accounts are created—these can be blank or randomly generated (the latter is recommended). Randomly generated system default passwords and PINs appear in the GUI to a user with Administrator privileges, until the you change the password and PIN; then, they are never visible again. Passwords and PINs are never visible in the CLI.

When a password or PIN is changed, checks done include the following:

- Password and PIN grammar (valid characters)
- The new password or PIN is a minimum of 3 characters long (as of Cisco Unity Express 2.1, the minimum length of a password or PIN can be configured if the system default does not comply with your security policy)
- The new password or PIN is different from the current password

There is an idle timeout of 10 minutes on any GUI login. Mouse movements do not count as activity; you must click menu items and open or close windows to reset the inactivity timer. The user is forced off after the inactivity timer expires.

## Password and PIN Recovery

A forgotten password or PIN cannot be recovered by a subscriber; contact the system administrator to do this. An administrator can never extract an existing password or PIN from the system, but can reset any user account password or PIN to a known string, and then advise the user of the new setting. The user can then log back in and change the password or PIN to a private setting.

If the Administrator cannot log in (due to a forgotten or incorrect password), and another administrator is defined on the system, the other administrator can log in and reset the password. If there is no other administrator defined on the system, your only recovery path is to log in to the Cisco Unity Express CLI, and either reset the password by using the CLI, or add another administrator to the system who can log in to the GUI to reset the password. To do this, you need the router enable password.

By using the user account definitions given previously in the "Suggested Access Control Lists" section on page 24, you can reset the administrator's password or the user account PIN. You can reset account's PIN to 1234, by using the Cisco Unity Express CLI command **username admin password** *xxxx* or **username admin pin 1234**. As an example, you can add a new administrator with a known password to the system as shown in the following:

```
cue> username new-admin create
cue> username new-admin password xxxx
cue> username new-admin group Administrators
```

## Default System Password Policy

Any new user account created on the Cisco Unity Express system is automatically assigned a password and a PIN. The default policy can be set to blank or to randomly generate a password and a PIN. The latter policy is recommended and is the system default. If you want to assign blank passwords as the default policy, use the **Defaults** > **User** window to set the policy.

The first time any user logs in to the GUI (password) or into a mailbox (TUI), the user is forced to change the password and PIN before any access to the system is granted. At this time, the password can no longer be blank, it must be a valid password and PIN of the minimum number of characters that are configured on the system (system default is 3).

There is a retry limit of three attempts on a PIN (not applicable to passwords). When you exceed the limit, an error message is logged and the user is returned to the top-level prompt ("if you have a mailbox on the system, enter it, otherwise please hold for an operator"). The mailbox is not disabled.

### CLI

There is no CLI password on the Cisco Unity Express system itself. But the Cisco IOS session command on the router is required to gain access to the Cisco Unity Express CLI, and Cisco Unity Express is therefore protected by the router CLI password protections. The Cisco IOS session command requires enable mode on the router.

## Security Best Practices

The following recommendations summarize suggested actions required to secure access to your Cisco Unity Express system:

- Assign an enable password to the router hosting the Cisco Unity Express module.
- Restrict telnet access to the router.
- Enable login and password control on the router TTY port connecting to Cisco Unity Express.
- Configure an inactivity timeout on the router TTY port connecting to Cisco Unity Express.
- Enable SSH on the router to protect telnet traffic; use only SSH-capable telnet client software.
- Use VPN/IPSec router technology to protect HTTP web access into Cisco Unity Express HTTPS is supported in a later release.
- Use ACLs to close access to any ports that are not actively in use by Cisco Unity Express.
- Use ACLs to restrict traffic into and from Cisco Unity Express.
- Protect the FTP server that is used for software installation with a login/password control.
- Protect the FTP server that is used for backup and restore with login/password control.
- During a Cisco Unity Express software install/upgrade, do not provide the FTP password on the install command line; let the installer prompt you for it.
- Maintain the Cisco Unity Express system with the "generate random password and PIN" user access policy. This is the default policy in a newly installed system.
- If you're using Cisco Unity Express 2.1 or a later release, enable the password and PIN expiry feature.
- Set the minimum length for passwords and PINs on Cisco Unity Express to be in line with your security policies.

# System Management Considerations

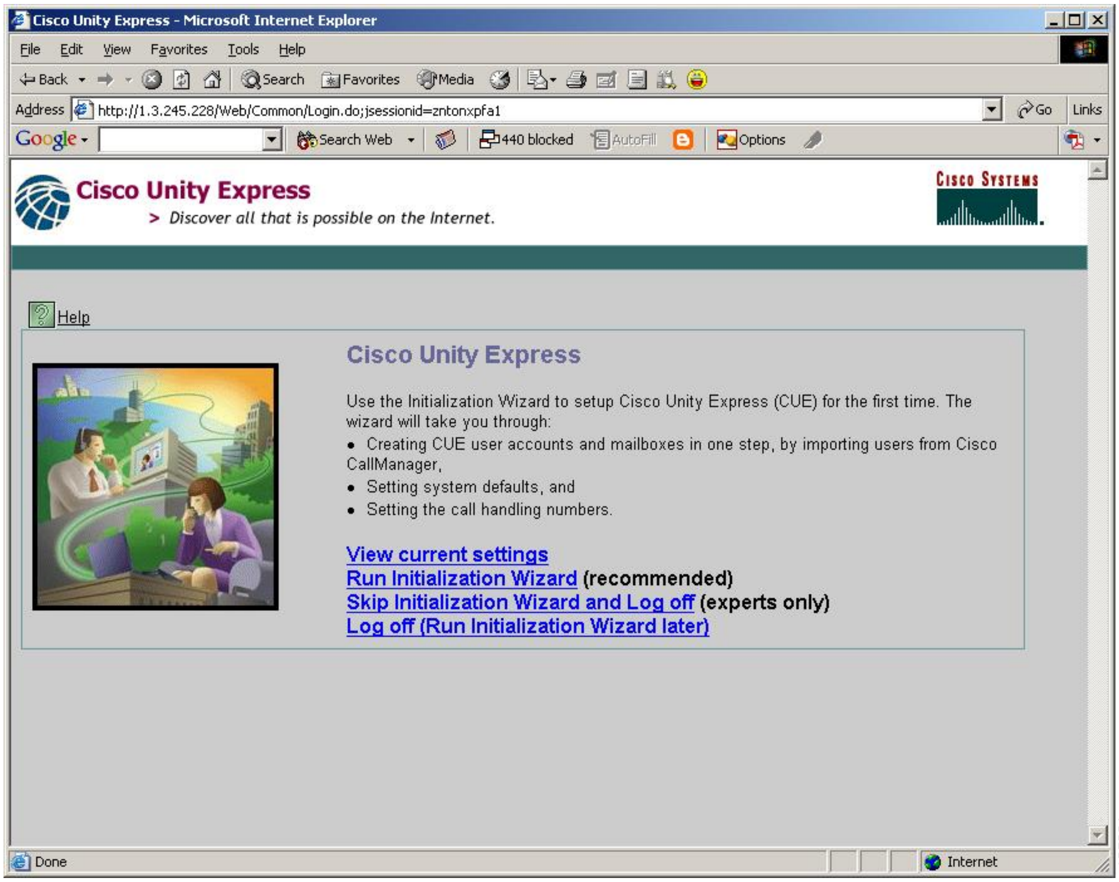
System management considerations for Cisco Unity Express deployment are bulk provisioning and call-detail record maintenance.

# Bulk Provisioning

Cisco Unity Express offers a CLI and can therefore be provisioned via scripting from a central Network Management station.

If the Cisco Unity Express system is provisioned entirely via CLI, the Initialization Wizard flag is never reset. This has no operational impact on the system other than when administrators log in to the GUI.AT that point, adminstrators are presented with the Initialization Wizard banner window, even though the system is by now fully configured and operational. In this situation, the administrator should choose the "Skip Initialization Wizard" link shown in Figure 11, as it is not applicable to a system that is already fully configured.

*Figure 11 Bypass the Initialization Wizard for a Fully Configured System*


Cisco Unity Express - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
Search Web
440 blocked
AutoFill
Options
Cisco Unity Express
> Discover all that is possible on the Internet.
Cisco Systems
Help
Done
Internet
135261

http://1.3.245.228/Web/Common/Login.do;jsessionid=zntonxpfa1

Cisco Unity Express

Use the Initialization Wizard to setup Cisco Unity Express (CUE) for the first time. The wizard will take you through:

- Creating CUE user accounts and mailboxes in one step, by importing users from Cisco CallManager,
- Setting system defaults, and
- Setting the call handling numbers.

View current settings
Run Initialization Wizard (recommended)
Skip Initialization Wizard and Log off (experts only)
Log off (Run Initialization Wizard later)

# Call Detail Records

There is no information specific to Cisco Unity Express captured in call detail records (CDRs). CDRs are produced by the call control engine, either Cisco CME or Cisco CallManager.

# Power Backup

A Linux platform should be disconnected from its power source without going through an orderly shutdown. Not doing so risks corruption of the file system. However, on a router platform, you can power cycle the chassis without regard to what is plugged into it. Also, there are unexpected power failures that no one can control. While every precaution has been taken to harden Cisco Unity Express's file system against corruption when power is removed unexpectedly from the system, there is a risk of data corruption associated with power failures.

## Best Practices

The following "best practices" are recommended for Cisco Unity Express implementation:

- Follow the Cisco Unity Express system shutdown procedures at all times before disconnecting power from the router that hosts Cisco Unity Express.
- For any router that has telephony features of any kind, an uninterrupted power supply (UPS) is recommended.