Integrating Cisco Unity Connection with Phone System

- Calls to a user extension that does not answer are forwarded to the personal greeting of the user.
- Calls to a user extension that is busy are forwarded to the busy greeting of the user.
- Unity Connection receives caller ID information from the phone system (if available).
- A user has easy access to messages by pressing a button on the phone and entering a password.
- Unity Connection identifies the user who leaves a message during a forwarded internal call, based on the extension from which the call originated.
- Messages left for a user activate the message waiting indicator (MWI) on the extension.

See the following sections for detailed information:

Working of a Phone System Integration

- Lines and cables necessary to make physical connections (for PIMG/TIMG integrations) or a network connection (in Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, SIP proxy servers, and QSIG-enabled phone systems). Depending on the type of integration, the phone system connects through different combinations of lines. See the applicable section for more information:
- Settings in the phone system and in Unity Connection. For more information, see the Settings in the Phone System in Unity Connection, on page 4
- Call information exchanged by the phone system and Unity Connection. For more information, see the Call Information Exchanged by Phone System and Unity Connection, on page 5
- Call control (signals used to set up, monitor, and tear down a call) to determine and control the status of the call. For more information, see the Call Control, on page 5

Integration with Cisco Unified Communications Manager

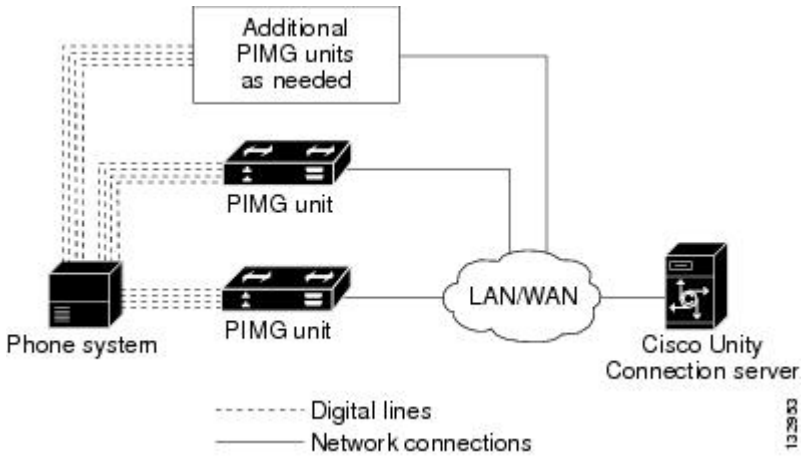
Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, and SIP proxy servers use network connections that carry all communication to and from Cisco Unity Connection. Figure shows the network connections used in an integration with Cisco Unified CM.

See the Integrating with Cisco Unified Communications Manager Express (Using SCCP or SIP) for additional information.

Digital Integration with Digital PIMG Units

The phone system sends call information, MWI requests, and voice connections through the digital lines, which connect the phone system to the PIMG units (media gateways). The PIMG units communicate with the Cisco Unity Connection server through the LAN or WAN using Session Initiation Protocol (SIP). Figure 11-2 shows the connections used in a digital integration using digital PIMG units.

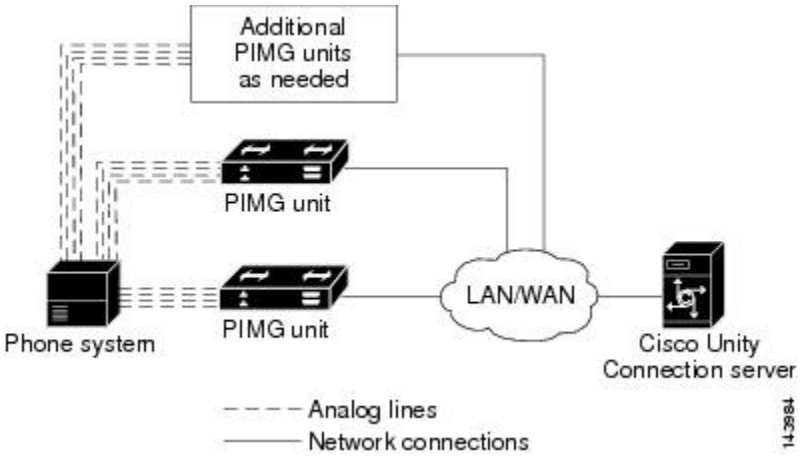
Figure 1: Connections for a Digital Integration Using Digital PIMG Units



DTMF Integration with Analog PIMG Units

The phone system sends call information, MWI requests, and voice connections through the analog lines, which connect the phone system to the PIMG units (media gateways). The PIMG units communicate with the Cisco Unity Connection server through the LAN or WAN using Session Initiation Protocol (SIP). Figure 11-3 shows the connections for a DTMF integration using analog PIMG units.

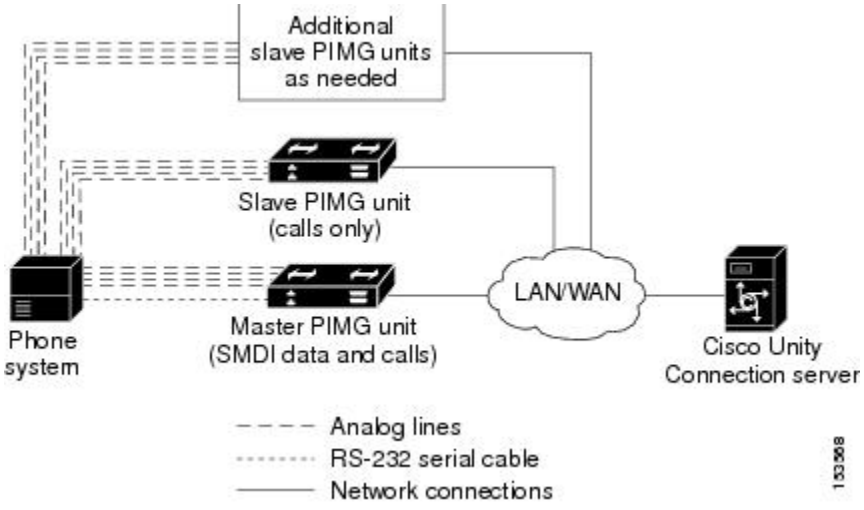
Figure 2: Connections for a DTMF Integration Using Analog PIMG Units



Serial (SMDI, MCI, or MD-110) Integration with Analog PIMG Units

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master PIMG unit (media gateways). Voice connections are sent through the analog lines between the phone system and the PIMG units. The PIMG units communicate with the Unity Connection server through the LAN or WAN using Session Initialization Protocol (SIP). Figure shows the connections for a serial integration using analog PIMG units.

Figure 3: Connections for a Serial (SMDI, MCI, or MD-110) Integration Using Analog PIMG Units



Note When you use multiple PIMG units, one PIMG unit must be designated the master PIMG unit, which is connected to the serial cable from the phone system. It is not possible to "daisy chain" the serial ports on the PIMG units.

You can add a secondary master PIMG unit to an integration. For details, see the "Adding a Secondary Master PIMG Unit" chapter of the *PIMG Integration Guide for Cisco Unity Connection Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/pimg/b_15cucintpimg.html.

TIMG Serial (SMDI, MCI, or MD-10) Integration

The TIMG integration uses one or more TIMG units between circuit-switched phone systems and IP networks. On the circuit-switched phone system side, there is a T1-CAS interface. On the IP side, there is a SIP interface, which is how Cisco Unity Connection communicates with the TIMG units. To Unity Connection, the integration is essentially a SIP integration. Unity Connection communicates with the TIMG units over the IP network using SIP and RTP protocols. The TIMG units communicate with the circuit-switched phone system over the phone network using serial protocols (SMDI, MCI, or MD-110).

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master TIMG unit. Voice connections are sent through the T1 digital lines between the phone system and the TIMG units. The TIMG units communicate with the Unity Connection server through the LAN or WAN using Session Initialization Protocol (SIP). Figure shows the connections for a serial integration using TIMG units.

TIMG In-Band Integration

The phone system sends call information, MWI requests, and voice connections through the T1 digital lines, which connect the phone system and the TIMG units. The TIMG units communicate with the Cisco Unity Connection server through the LAN or WAN using Session Initialization Protocol (SIP). Figure shows the required connections for an in-band integration using TIMG units.

PIMG/TIMG Integrations and Cisco Unified Communications Manager Using Cisco Unified SIP Proxy

The Cisco Unified SIP Proxy allows the PIMG/TIMG integrations and Cisco Unified Communications Manager to share the same voice messaging ports on Unity Connection by acting as a SIP proxy. The Cisco Unified SIP Proxy uses a SIP trunk integration with Unity Connection. Figure shows the connections. For more information, see the application notes for Cisco Unified SIP Proxy at http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/interOp_sipProxy.html.

Settings in the Phone System in Unity Connection

For an integration to be successful, Unity Connection and the phone system must know the connections to use (for example, IP addresses and channels) and the expected method of communication (for example, IP packets, serial packets, and DTMF tones). Certain integrations require specific codes or extensions for turning MWIs on and off.

There are required settings for Unity Connection, and programming for the phone system, that must be made in order to enable the integration. For information on these settings, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Call Information Exchanged by Phone System and Unity Connection

The phone system and Unity Connection exchange call information to manage calls and to make the integration features possible. With each call, the following call information is typically passed between the phone system and Unity Connection:

- The extension of the called party.
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the phone system supports caller ID).
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls). There is also a reason code for Direct Calls.

Cisco Unified Communications Manager SCCP and SIP trunk integrations can also provide the following call information:

- Called number
- First redirecting number
- Last redirecting number

Note Unity Connection can use either the first redirecting number or last redirecting number, depending on the setting of the Use Last (Rather than First) Redirecting Number for Routing Incoming Call check box on the System Settings > Advanced > Conversations page in Cisco Unity Connection Administration.

If the phone system sends the necessary information and if Unity Connection is configured correctly, an integration can provide the following integration functionality:

- Call forward to personal greeting
- Call forward to busy greeting
- Caller ID
- Easy message access (a user can retrieve messages without entering an ID because Unity Connection identifies the user based on the extension from which the call originated; a password may be required)
- Identified user messaging (Unity Connection identifies the user who leaves a message during a forwarded internal call, based on the extension from which the call originated)

Call Control

The phone system uses a set of signals to set up, monitor, and release connections for a call. Cisco Unity Connection monitors call control signals to determine the state of the call, and uses these signals to respond

appropriately to phone system actions and to communicate with the phone system. For example, a caller who is recording a message might hang up, so Unity Connection detects that the call has ended and stops recording.

Depending on the phone system, the following types of call control signals are used:

Table 1: Call Control Signals

Cisco Unified Communications Manager	For Skinny Call Control Protocol (SCCP) integrations, Cisco Unified Communications Manager generates SCCP messages, which are translated by Cisco Unity Connection. For SIP trunk integrations, Cisco Unified CM sends SIP messages, and Unity Connection sends SIP responses when a call is set up or terminated.
Circuit-switched phone system through PIMG/TIMG units	The phone system sends messages to the PIMG or TIMG units (media gateways), which send the applicable SIP messages to Unity Connection. Unity Connection sends SIP responses when a call is set up or terminated, and the PIMG or TIMG units communicate with the phone system.

Sample Path for a Call from the Phone System to a User

The following steps give an overview of a sample path that an external call can take when traveling from the phone system to a user.

1. For Cisco Unified Communications Manager, when an external call arrives, the gateway sends the call over the LAN or WAN to Cisco Unified CM. Cisco Unified CM routes the call to the Cisco Unity Connection voice mail pilot number.

   For circuit-switched phone systems, when an external call arrives via the PSTN, TI/PRI, DID or LS/GS analog trunks, the phone system routes the call to the Cisco Unity Connection voice mail pilot number.
2. The phone system routes the call to an available Cisco Unity Connection voice messaging port.
3. Unity Connection answers the call and plays the opening greeting.
4. During the opening greeting, the caller enters an extension. For example, the caller enters 1234 to reach a person at that extension.
5. Unity Connection notifies the phone system that there is a call for extension 1234.
6. Depending on whether Unity Connection is set up to perform a release transfer or a supervised transfer, the following occurs:

Release transfer (blind transfer)	Unity Connection passes the call to the phone system, and the phone system sends the call to extension 1234 without waiting to determine whether the line is available. Then the phone system and Unity Connection drop out of the loop. In this configuration, if the customer wants Unity Connection to take a message when a line is busy or unanswered, each phone must be configured to forward calls to Unity Connection when the line is busy or unanswered.

Supervised transfer	While Unity Connection holds the call, the phone system attempts to establish a connection with extension 1234. If the line is available, the phone system connects the call from Unity Connection to extension 1234. The phone system and Unity Connection drop out of the loop, and the call is connected directly from the original caller to extension 1234. If the line is busy or unanswered, the phone system gives that information to Unity Connection, and Unity Connection performs the operation the user has specified. For example, Unity Connection takes a message.

General Integration Issues

For a detailed list of the requirements for a specific integration, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

If Unity Connection is configured for a cluster, see the Balancing the Load of Calls Unity Connection Servers Handle and the Configuration for Dial-Out Voice Messaging Ports.

In addition, consider the following list of integration issues:

- Phone systems integrate with Unity Connection only through a network connection.
- The number of voice ports supported with Cisco Unity Connection depends upon the Unity Connection platform specifications. Install only the number of ports that are needed, so that system resources are not allocated to unused ports, and do not exceed the port limitations set for the platform.

For more information on supported platforms, see the *Cisco Unity Connection 15 Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/supported_platforms/b_15cucspl.html.

For additional information about configuring voice messaging ports, see the "Planning the Usage of Voice Messaging Ports in Cisco Unity Connection" chapter in the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Deployment Models for Integrations with Cisco Unified Communications Manager

Cisco Unity Connection and Cisco Unified Communications Manager deployment models, including single-site messaging, centralized messaging, and distributed messaging, can be combined to suit customer requirements. When choosing a deployment model, you must consider a range of issues, for example:

- Centralized messaging allows you to consolidate servers and administration, but requires that you plan for access to voice messages in the event of WAN outages and that you perform the appropriate QOS/capacity planning for voice-messaging traffic and call traffic.
- Distributed messaging may require more servers and administrative overhead, but, combined with distributed call processing, requires less capacity on intersite WAN links.

For a detailed explanation of deployment models and their relative merits, see the "Collaboration System Components and Architecture" chapter in *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html.

Deploying Phones Across the WAN

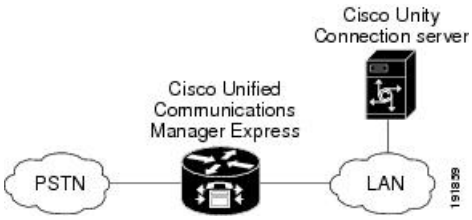
Some deployment models, such as centralized messaging with distributed call processing, require placement of phones across the WAN from the Unity Connection server. When deploying phones across the WAN from the Unity Connection server, see the "Collaboration System Components and Architecture" chapter in *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html.

For guidance on capacity planning and call admission control (CAC) for these phones. When integrating Cisco Unity Connection with a circuit-switched phone system (TDM PBX), see the *PIMG Integration Guide* or the *TIMG Integration Guide* at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html for capacity planning for the PIMG/TIMG units deployed at these remote/branch sites to support phones at these sites.

Integrating with Cisco Unified Communications Manager Express (Using SCCP or SIP)

Cisco Unity Connection supports Cisco Unified Communications Manager Express integrations through both SCCP and SIP interfaces. Figure 4: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN shows the connections.

Figure 4: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN



See Table 2: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express) for information on the differences in these integration methods.

Table 2: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express)

Feature	SCCP	SIP
Communication method	SCCP	SIP trunk
Cisco Unity Connection cluster (active/active high availability)	Supported	Supported

Feature	SCCP	SIP
Use of SCCP and SIP phones	Supported	Some SCCP phones may require use of a media termination point (MTP)
Support for Cisco Unified CM Express versions	All versions	Versions 3.4 and later
Cisco Unified CM Express authentication and encryption	Not supported	Not supported
First/last redirecting number	Supported	Supported
QOS	Supported	Supported

For information on the compatibility of Unity Connection and Cisco Unified Communications Manager Express versions, see the *Compatibility Matrix for Cisco Unity Connection* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html

For information on how to integrate Unity Connection with Cisco Unified CM Express, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

For more information on using the SIP protocol to integrate Unity Connection with Cisco Unified CM Express, see the Integrating Using SIP.

Cisco Unified Communications Manager Authentication and Encryption for Unity Connection Voice Messaging Ports

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Unity Connection and Cisco Unified Communications Manager. Possible threats include:

- Man-in-the-middle attacks, in which an attacker intercepts and changes the data flowing between Cisco Unified CM and Unity Connection voice messaging ports.
- Network traffic sniffing, in which an attacker captures phone conversations and signaling information that flow between Cisco Unified CM, the Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM.
- Changing the call signaling between the Unity Connection voice messaging ports and Cisco Unified CM.
- Changing the media stream between Unity Connection voice messaging ports and endpoints, for example, phones or gateways.
- Identity theft of the Unity Connection voice messaging port, in which a non-Unity Connection device presents itself to Cisco Unified CM as a Unity Connection voice messaging port.
- Identity theft of the Cisco Unified CM server, in which a non-Cisco Unified CM server presents itself to Unity Connection voice messaging ports as a Cisco Unified CM server.

Cisco Unified Communications Manager Security Features

Cisco Unified Communications Manager Release 4.1(3) or later for SCCP integrations or Cisco Unified Communications Manager Release 5.x or later for SIP trunk integrations can secure the connection with

Cisco Unity Connection against security threats. The Cisco Unified CM security features that Unity Connection can take advantage of are described in Table 3: Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity Connection.

Table 3: Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity Connection

Security Feature	Description
Signaling authentication	Uses the Transport Layer Security (TLS) protocol to validate that no tampering has occur signaling packets during transmission. Signaling authentication relies on the creation of t Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified the Unity Connection voice messaging ports. • Modification of the call signaling. • Identity theft of the Unity Connection voice messaging port. • Identity theft of the Cisco Unified CM server.
Device authentication	Validates the identity of the device. This process occurs between Cisco Unified CM and t Connection voice messaging ports when each device accepts the certificate of the other dev the certificates are accepted, a secure connection between the devices is established. Devi authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified the Unity Connection voice messaging ports. • Modification of the media stream. • Identity theft of the Unity Connection voice messaging port. • Identity theft of the Cisco Unified CM server.
Signaling encryption	Uses cryptographic methods to protect (through encryption) the confidentiality of all SCC signaling messages that are sent between the Unity Connection voice messaging ports and Unified CM. Signaling encryption ensures that the information that pertains to the parties digits that are entered by the parties, call status, media encryption keys, and so on are protect unintended or unauthorized access. This feature protects against: • Man-in-the-middle attacks that observe the information flow between Cisco Unified the Unity Connection voice messaging ports. • Network traffic sniffing that observes the signaling information flow between Cisco U and the Unity Connection voice messaging ports.

Security Feature	Description
Media encryption	Uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711 to ensure that onl recipient can interpret the media streams between the Unity Connection voice messag endpoints (for example, phones or gateways). Only audio streams are encrypted. Med creates a media master key pair for the devices, delivers the keys to Unity Connection and and secures the delivery of the keys while the keys are in transport. Unity Connection an use the keys to encrypt and decrypt the media stream. This feature protects against: • Man-in-the-middle attacks that listen to the media stream between Cisco Unified Unity Connection voice messaging ports. • Network traffic sniffing that eavesdrops on phone conversations that flow betwe Unified CM, the Unity Connection voice messaging ports, and IP phones that are Cisco Unified CM. Authentication and signaling encryption are required for media encryption; that is, if t not support authentication and signaling encryption, media encryption cannot occur.

Note that Cisco Unified CM authentication and encryption protects only calls to Unity Connection. Messages that are recorded on Unity Connection are not protected by Cisco Unified CM authentication and encryption but can be protected by the Unity Connection secure messaging feature.

For more information on secure messaging, see the "Securing User Messages" chapter of the Security Guide for Cisco Unity Connection *Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/guide/b_15cucsecx.html.

The security features (authentication and encryption) between Unity Connection and Cisco Unified CM require the following for SCCP integrations:

- A Cisco Unified CM CTL file that lists all Cisco Unified CM servers that are entered in Cisco Unity Connection Administration for secure clusters.
- A Unity Connection server root certificate for each Unity Connection server that uses authentication and/or encryption. A root certificate is valid for seven years from the time it was created.
- Unity Connection voice messaging port or port group device certificates that are rooted in the Unity Connection server root certificate, and voice messaging ports or port groups that are present when registering with the Cisco Unified CM server.

The process of authentication and encryption of Unity Connection voice messaging SCCP ports occurs as follows:

1. Each Unity Connection voice messaging port connects to the TFTP server, via TFTP port 69, downloads the CTL file, and extracts the certificates for all Cisco Unified CM servers.
2. Each Unity Connection voice messaging port establishes a network connection to the Cisco Unified CM TLS port. By default, the TLS port is 2443, though the port number is configurable.
3. Each Unity Connection voice messaging port establishes a TLS connection to the Cisco Unified CM server, at which time the device certificate is verified and the voice messaging port is authenticated.
4. Each Unity Connection voice messaging port registers with the Cisco Unified CM server, specifying whether the voice messaging port also uses media encryption.

The process of authentication and encryption of Unity Connection voice messaging SIP port groups occurs as follows:

1. Each Unity Connection voice messaging port group connects to the TFTP server, via TFTP port 69, downloads the CTL file, and extracts the certificates for all Cisco Unified CM servers.
2. Each Unity Connection voice messaging port group establishes a network connection to the Cisco Unified CM TLS port. By default, the TLS port is 2443, though the port number is configurable.
3. Each Unity Connection voice messaging port group establishes a TLS connection to the Cisco Unified CM server, at which time the device certificate is verified and the voice messaging port group is authenticated.
4. Each Unity Connection voice messaging port group registers with the Cisco Unified CM server, specifying whether the voice messaging port group also uses media encryption.

Data is Encrypted

When a call is made between Cisco Unity Connection and Cisco Unified CM, the call-signaling messages and the media stream are handled in the following manner:

- If both endpoints are set for encrypted mode, the call-signaling messages and the media stream are encrypted.
- If one endpoint is set for authenticated mode and the other endpoint is set for encrypted mode, the call-signaling messages are authenticated. But neither the call-signaling messages nor the media stream are encrypted.
- If one endpoint is set for non-secure mode and the other endpoint is set for encrypted mode, neither the call-signaling messages nor the media stream are encrypted.

Cisco Unified Communications Manager Cluster Security Mode Settings in Unity Connection

The Security Mode settings in Cisco Unity Connection Administration determine how the ports handle call-signaling messages and whether encryption of the media stream is possible. Table 4: Security Mode Settings for Voice Messaging Ports in an SCCP Integration describes the effect of the Security Mode settings on the Telephony Integrations > Port > Port Basics page for each port in an SCCP integration.

Table 4: Security Mode Settings for Voice Messaging Ports in an SCCP Integration

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages are not ensured because call-signaling messages are sent as clear (unencrypted) text and are connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream cannot be encrypted.
Authenticated	The integrity of call-signaling messages is ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages is not ensured because they are sent as clear (unencrypted) text. In addition, the media stream is not encrypted. **Note** You can ensure the integrity of call-signaling messages for the audio a calls using the authenticated TLS port.

Setting	Effect
Encrypted	The integrity and privacy of call-signaling messages is ensured because they are connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages are encrypted. In addition, the media stream can be encrypted. **Caution** Both endpoints must be registered in encrypted mode for the media stream to be encrypted. However, when one endpoint is set for non-secure or authenticated mode and the other endpoint is set for encrypted mode, the media stream is not encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream is not encrypted.

Disabling and Re-enabling Security

The authentication and encryption features between Cisco Unity Connection and Cisco Unified CM can be enabled and disabled by changing the Security Mode for all Cisco Unified CM clusters to Non-Secure, and by changing the applicable settings in the Cisco Unified Communications Manager Administration.

Authentication and encryption can be reenabled by changing the Security Mode to Authenticated or Encrypted.

Note After disabling or re-enabling authentication and encryption, it is not necessary to export the Unity Connection server root certificate and copy it to all Cisco Unified CM servers.

Multiple Clusters with Different Security Mode Settings

When Cisco Unity Connection has multiple Cisco Unified CM phone system integrations, each Cisco Unified CM phone system integration can have different Security Mode settings. For example, one Cisco Unified CM phone system integration can be set to Encrypted, and a second Cisco Unified CM phone system integration can be set to Non-Secure.

Settings for Individual Voice Messaging Ports

For troubleshooting purposes, authentication and encryption for Cisco Unity Connection voice messaging ports can be individually enabled and disabled. At all other times, the Security Mode setting for all individual voice messaging ports in a Cisco Unified CM port group should be the same.

Packetization

The Real-Time Transport Protocol (RTP) is used to send and receive audio and video packets over the IP network. Each discrete packet has a fixed-size header, but the packets themselves can vary in size, depending on the size of the audio stream to be transported (which varies by codec) and the packetization setting. This variable size function helps utilize network bandwidth more efficiently. Reducing the number of packets that are created per call sends fewer total bytes over the network.

Packetization is set in the Cisco Unified CM Service Parameters, in the Preferred G711 Millisecond PacketSize and Preferred G729 Millisecond PacketSize parameters. Cisco Unity Connection supports any packet size up to 30ms for G.711 audio, and any packet size up to 60 ms for G.729a audio. The default setting is 20ms for both; there may be latency issues with lower settings.

DSCP is a priority setting on each packet. DSCP helps intermediary routers manage network congestion and lets them know which packets to prioritize ahead of others. Following Cisco AVVID standards, Unity Connection marks the SCCP and SIP packets (call control) with a default DSCP value of 24 (the TOS octet is 0x60), and the RTP packets (audio and video traffic) with a default DSCP value of 46 (the TOS octet is 0xB8). Thus, the RTP audio and video packets can be assigned priority over other packets using the router settings. Note that even though Cisco Unified CM allows you set different DSCP values, when integrated with Unity Connection, the DSCP values set by Unity Connection always take precedence. The marking of both SCCP and SIP packets is configurable in Unity Connection on the System Settings > Advanced > Telephony Configuration page in Cisco Unity Connection Administration.

With each new audio stream (once per call), Cisco Unified CM tells Unity Connection which packet size to use, and Unity Connection sets the DSCP priority for the stream. The entire stream (call) stays at the specified packet size and priority. For example, an audio stream could be broken up into packets of 30ms each. A 30ms G.729a audio stream would be 30 bytes plus the header per packet, and a 30ms G.711 stream would be 240 bytes plus the header per packet. For information on setting Cisco Unified CM Service Parameters, see the Cisco Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Note You can change the codecs that Unity Connection advertises on the Telephony Integrations > Port Group > Edit Codec Advertising configuration page in Cisco Unity Connection Administration.

Port Group Configuration for Cisco Unified Communications Manager Cluster Failover

For Cisco Unified Communications Manager SCCP integrations, when a Cisco Unified CM cluster is configured and Cisco Unified CM failover occurs as calls are in progress, the voice messaging ports may experience a delay registering with the secondary Cisco Unified CM server.

Unity Connection ports can register more quickly after Cisco Unified CM failover occurs if the port groups are configured as follows:

- You create two port groups for the SCCP integration:
  - The first port group contains half the voice messaging ports for the Cisco Unified CM integration (including answering and dialout ports) configured as described in the applicable chapter of the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 15*.
  - The second port group contains the remaining half of the ports for the Cisco Unified CM integration (including answering and dialout ports) as described in the applicable chapter of the same guide.

Note The *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 15* is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/cucme_sccp/b_15cucintcucmesccp.html.

- On the Telephony Integrations > Port Group > Port Group Basics > Edit Servers page, you list the Cisco Unified CM servers in different orders:

- For the first port group, the Cisco Unified CM servers are listed in the order specified in the applicable chapter of the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 15*.
- For the second port group, the Cisco Unified CM servers are listed in the reverse order.

Internet Protocol Version 6 (IPv6) Support with Cisco Unified Communications Manager Integrations

Cisco Unity Connection supports IPv4, IPv6, or Dual Mode (IPv4/IPv6) addressing with Cisco Unified Communications Manager phone system integrations via SIP. When IPv6 is enabled, Connection can obtain an IPv6 address either through router advertisement, through DHCP, or by manually configuring an address either in Cisco Unified Operating System Administration or using the command-line interface.

For SIP integrations with Cisco Unified CM, if Unity Connection is configured to listen for incoming IPv4 and IPv6 traffic, you can configure the addressing mode that Unity Connection uses for call control signaling for each port group to use either IPv4 or IPv6. (This mode is also used when connecting to a TFTP server.) In addition, you can configure the addressing mode that Unity Connection uses for media for each port group to use either IPv4 or IPv6.

Note SCCP and SIP ANAT will not be deployed for IPv6 address.

IPv6 support is disabled by default. You can enable IPv6 and configure IPv6 address settings either in Cisco Unified Operating System Administration or in the CLI. For information on enabling and configuring IPv6 when setting up a new Cisco Unified CM integration, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

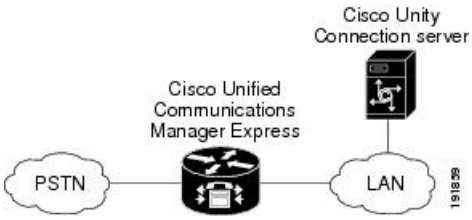
Note the following considerations when deploying IPv6 for Cisco Unified CM integrations:

- The CTL file required for security features (authentication and encryption) between Unity Connection and Cisco Unified CM for SCCP integrations uses IPv4 addressing. Therefore, in order to use authentication and/or encryption with SCCP, you must use either IPv4 or Dual Mode (IPv4/IPv6) addressing.
- Some versions of Cisco Adaptive Security Appliance (ASA) do not support application inspection for IPv6 traffic for Unified Communications application servers and endpoints. You should not be using IPv6 for Unified Communications if you are using a Cisco ASA version that does not provide this support. See the documentation for your version of Cisco ASA to determine whether application inspection is supported in your deployment.

Integrating with Cisco Unified Communications Manager Express (Using SCCP or SIP)

Cisco Unity Connection supports Cisco Unified Communications Manager Express integrations through both SCCP and SIP interfaces. Figure 5: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN shows the connections.

Figure 5: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN



See Table 5: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express) for information on the differences in these integration methods.

Table 5: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express)

Feature	SCCP	SIP
Communication method	SCCP	SIP trunk
Cisco Unity Connection cluster (active/active high availability)	Supported	Supported
Use of SCCP and SIP phones	Supported	Some SCCP phones may require use of a media termination point (MTP)
Support for Cisco Unified CM Express versions	All versions	Versions 3.4 and later
Cisco Unified CM Express authentication and encryption	Not supported	Not supported
First/last redirecting number	Supported	Supported
QOS	Supported	Supported

For information on the compatibility of Unity Connection and Cisco Unified Communications Manager Express versions, see the *Compatibility Matrix for Cisco Unity Connection* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html

For information on how to integrate Unity Connection with Cisco Unified CM Express, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

For more information on using the SIP protocol to integrate Unity Connection with Cisco Unified CM Express, see the Integrating Using SIP.

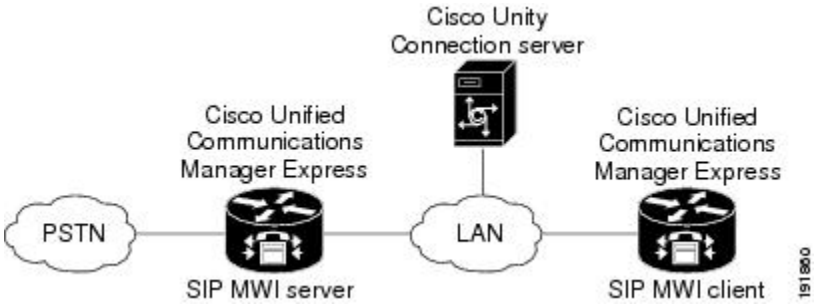
Multiple Cisco Unified Communications Manager Express Version Support

A single Cisco Unity Connection server can support multiple versions of Cisco Unified CM Express. The version of Unity Connection being used must support all versions of Cisco Unified CM Express. See the *Compatibility Matrix for cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html .

Multiple Cisco Unified Communications Manager Express Routers Integrating with a Single Cisco Unity Connection Server

A single, centralized Unity Connection server can be used by multiple Cisco Unified CM Express routers. This configuration requires that one Cisco Unified CM Express router be on the same LAN as the Unity Connection server, and that this Cisco Unified CM Express router register all Unity Connection voice messaging ports. This Cisco Unified CM Express router (the SIP MWI server) is a proxy server that relays SIP MWI messages between the Unity Connection server and all other Cisco Unified CM Express routers (the SIP MWI clients). Note that Unity Connection voice messaging ports register only with the SIP MWI server (the Cisco Unified CM Express router that is on the same LAN as the Unity Connection server), not with the SIP MWI clients. See Figure 11-9.

Figure 6: Connections between Multiple Cisco Unified CM Express Routers and a Single Cisco Unity Connection Server



For information on configuring Unity Connection to support multiple Cisco Unified CM Express routers, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

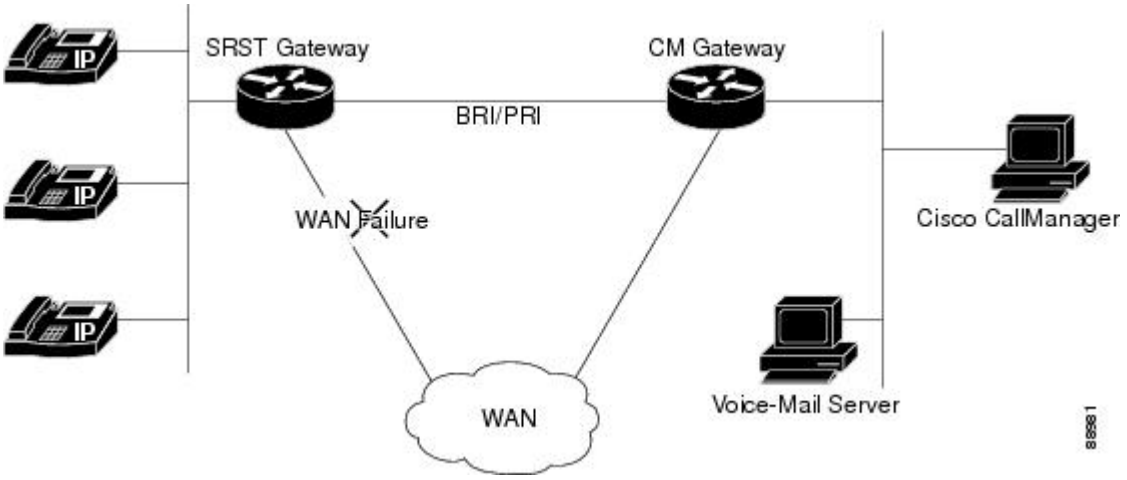
Integrating Unity Connection with Multiple Versions of Cisco Unified CM and Cisco Unified Communications Manager Express

A single Cisco Unity Connection server can support multiple versions of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express. The Unity Connection version must support all versions of Cisco Unified CM and/or Cisco Unified CM Express. See the Compatibility Matrix for Cisco Unity Connection at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.

Integrating Unity Connection with Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)

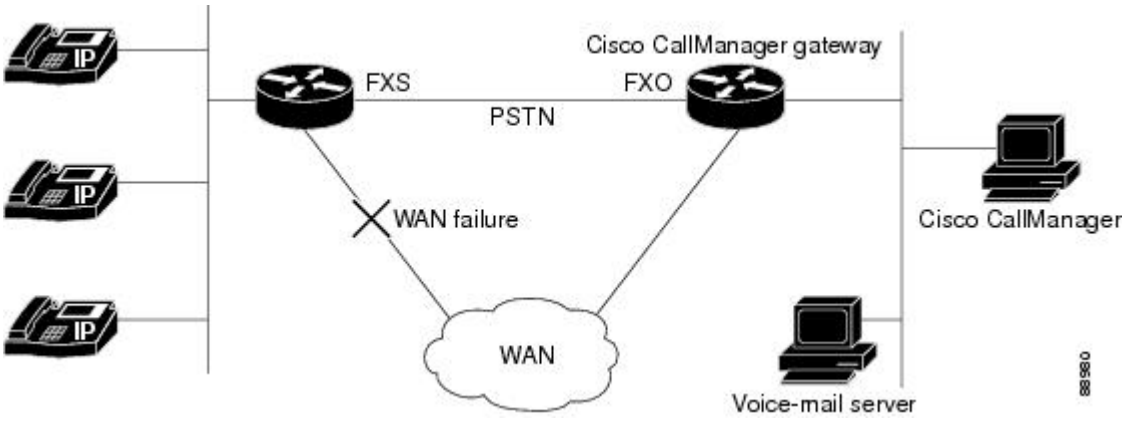
Cisco Unified Survivable Remote Site Telephony (SRST) can direct calls to Unity Connection during Cisco Unified CM fallback. When the WAN is down and Unity Connection has Basic Rate Interface (BRI) or Primary Rate Interface (PRI) access to the Cisco Unified SRST system, Unity Connection uses ISDN signaling (see Figure 11-10).

Figure 7: Cisco Unified Communications Manager Fallback with BRI or PRI



When the WAN is down and Unity Connection has foreign exchange office (FXO) or foreign exchange station (FXS) access to a public switched telephone network (PSTN), Unity Connection uses in-band dual tone multifrequency (DTMF) signaling (see Figure 11-11).

Figure 8: Cisco Unified Communications Manager Fallback with PSTN



In both configurations, phone message buttons remain active and calls to busy or unanswered numbers are forwarded to Unity Connection. The installer must configure access from the dial peers to the voice-mail system, and establish routing to Unity Connection for busy and unanswered calls and for the message button.

If Unity Connection is accessed over FXO or FXS, you must configure instructions (DTMF patterns) for Unity Connection so it can access the correct voice-mail system mailbox.

When using Cisco Unified SRST with Unity Connection, the integration has the following limitations during a WAN outage:

- **Call forward to busy greeting**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Unity Connection, the busy greeting cannot play.
- **Call forward to internal greeting**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Unity Connection, the internal greeting cannot play. Because the PSTN provides the calling number of the FXO line, the caller is not identified as a user.
- **Call transfers**—Because an access code is needed to reach the PSTN, call transfers from Unity Connection to a branch office fails.
- **Identified user messaging**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a user at a branch office leaves a message or forwards a call, the user is not identified. The caller appears as an unidentified caller.
- **Message waiting indication**—MWIs are not updated on branch office phones, so MWIs do not correctly reflect when new messages arrive or when all messages have been listened to. The resynchronizing of MWIs after the WAN link is re-established.
- **Message notification**—Because an access code is needed to reach the PSTN, message notifications from Unity Connection to a branch office fails.
- **Routing rules**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call arrives from a branch office to Unity Connection (either a direct or forwarded call), routing rules fail.

When the Cisco Unified SRST router uses PRI or BRI connections, the caller ID for calls from a branch office to Unity Connection may be the full number (exchange plus extension) provided by the PSTN and therefore may not match the extension of the Unity Connection user. In this case, you can let Unity Connection recognize the caller ID using alternate extensions.

When using Cisco Unified SRST, Redirected Dialed Number Information Service (RDNIS) must be supported.

For information on setting up Cisco Unified SRST routers, see the "Integrating Voice Mail with Cisco Unified SRST" chapter of the applicable *Cisco Unified SRST System Administrator Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html.

Impact of Non-Delivery of RDNIS on Voice Mail Calls Routed Using AAR

RDNIS must be supported when using Automated Alternate Routing (AAR).

AAR can route calls over the PSTN when the WAN is oversubscribed. However, when calls are rerouted over the PSTN, RDNIS can be affected. Incorrect RDNIS information can affect voice mail calls that are rerouted over the PSTN by AAR when Cisco Unity Connection is remote from its messaging clients. If the RDNIS information is not correct, the caller does not reach the mailbox of the dialed user but instead hears the automated attendant prompt, and might be asked to reenter the extension number of the party the caller wants to reach. This behavior is primarily an issue when the phone carrier is unable to ensure RDNIS across the network. There are numerous reasons why the carrier might not be able to ensure that RDNIS is properly sent.

Check with your carrier to determine whether it provides guaranteed RDNIS delivery end-to-end for your circuits. The alternative to using AAR for oversubscribed WANs is simply to let callers hear reorder tone in an oversubscribed condition.

Integrating Unity Connection with Cisco Unified Communications Manager Express in SRST Mode

Cisco Unity Connection supports a topology with centralized call processing and distributed messaging, in which your Unity Connection server is located at a remote site or branch office and registered with Cisco Unified CM at a central site.

When the WAN link fails, the phones fall back to the Cisco Unified CM Express-as-SRST device. Unity Connection can also fall back to the Cisco Unified CM Express-as-SRST device, which lets users at the remote site access their voice messages and see message waiting indicators (MWIs) during a WAN outage. Note that MWIs must be resynchronized from the Unity Connection server whenever a failover happens from Cisco Unified CM to Cisco Unified CM Express-as-SRST or vice versa.

For information on setting up this configuration, see the *Integrating Cisco Unity Connection with Cisco Unified CME-as-SRST* configuration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html.

Survivable Remote Site Voicemail

Cisco Unity Connection Survivable Remote Site Voicemail (Unity Connection SRSV) is a backup voicemail solution that works in conjunction with Cisco Unified Survivable Remote Site Telephony (SRST) for providing voicemail service to a branch during WAN outages.

Unity Connection SRSV is used in the centralized Cisco Unified Communications Manager and Cisco Unity Connection environment with multiple branch offices or small sites. It provides limited voicemail and auto-attendant features that remain in synchronization with the central Unity Connection voicemail service so that when the WAN outage or failure occurs, the Unity Connection SRSV solution can provide voicemail service to the subscribers at the branch. However, as soon as the network is restored, all the voicemails received by the branch subscribers are automatically uploaded to the central Unity Connection voicemail server.

For more information on how to configure Cisco Unity Connection SRSV at central Connection location, see the Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) for Release 15, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/srsv/guide/b_15cucsrsvx.html.

Integrating Using SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force standard for multimedia calls over IP. SIP is a peer-to-peer, ASCII-based protocol that uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more end points. See Table 6: SIP Network Components.

Table 6: SIP Network Components

Component	Description
SIP proxy server	An intermediate device that receives SIP requests from a client and then forwards the requests on behalf of the client. Proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
Redirect server	Provides information to the client about the next hop or hops that a message should take. The client then contacts the next hop server or user-agent server directly.
Registrar server	Processes requests from user agent clients for registration of their current location. Registrar servers are often installed on the redirect or proxy server.
Phones	Acts as either a server or client. Softphones (PCs that have phone capabilities installed) and Cisco SIP IP phones can initiate SIP requests and respond to requests.
Gateways	Provide call control. Gateways provide many services; the most common is a translation function between SIP call endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway translates between audio and video codecs, and performs call setup and clearing on both the LAN side and the switched-circuit network side.

Cisco Unity Connection accepts calls from a proxy server. Unity Connection relies on a proxy server or call agent to authenticate calls.

SIP uses a request/response method to establish communications between various components in the network and to ultimately establish a conference (call or session) between two or more endpoints. A single call may involve several clients and servers.

Users in a SIP network are identified by:

- A unique phone or extension number.
- A unique SIP address, which is similar to an email address and uses the format sip:<userID>@<domain>. The user ID can be either a user name or an E.164 address.

When a user initiates a call, a SIP request typically goes to a SIP server (either a proxy server or a redirect server). The request includes the caller address (From) and the address of the called party (To).

SIP messages are in text format using ISO 10646 in UTF-8 encoding (like HTML). In addition to the address information, a SIP message contains a start-line specifying the method and the protocol, a number of header fields specifying call properties and service information, and an optional message body which can contain a session description.

Supported SIP Integrations

Unity Connection supports the following SIP integrations:

- SIP trunks to supported versions of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express. For a list of Cisco Unified CM and Cisco Unified CM Express versions supported as SIP trunks, see SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco

Unified Communications Manager, and Cisco Unified Communications Manager Express at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.

- Cisco SIP Proxy Server (CSPS).
- Cisco ISR voice gateways for integrating Unity Connection to a QSIG-enabled phone system (see the Integrating Unity Connection with a QSIG-Enabled Phone System Using Cisco ISR Voice Gateways, on page 27).

Third-party SIP trunks are currently not supported.

For more information on configuring SIP trunks between Unity Connection and Cisco Unified CM or Cisco Unified CM Express, see the applicable SIP trunk integration guide at https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

Note Cisco Unity Connection extracts Caller Id from Remote Party Id field and FROM field in SIP Invite. In addition, when the Remote Party Id option is unchecked on CUCM SIP trunk and the FROM field is set to Anonymous in a SIP header, Connection treats the caller as unknown.

Integrating with Circuit-Switched Phone Systems Using PIMG or TIMG Units

Cisco Unity Connection can integrate with circuit-switched phone systems using the PIMG or TIMG units (media gateways) between circuit-switched phone systems and IP networks.

For a list of circuit-switched phone systems supported with Unity Connection using PIMG and TIMG integrations, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Description of PIMG Integrations

The PIMG integration uses one or more PIMG units between the circuit-switched phone systems and IP network. On the circuit-switched phone system side, there are both digital (feature-set) and analog interfaces; the interface used depends on the phone system to which Cisco Unity Connection is connected. On the IP side, there is a SIP interface, which is how Unity Connection communicates with the PIMG units. To Unity Connection, the integration is essentially a SIP integration. Unity Connection communicates with the PIMG units over the IP network using SIP and RTP protocols. The PIMG units communicate with the circuit-switched phone system over the phone network using phone system-specific protocols (digital, analog, or serial).

For high-level descriptions of each PIMG integration type, and illustrations showing the network connections, see the Working of a Phone System Integration, on page 2.

Setup and Configuration

For PIMG/TIMG setup and configuration, the installer does the following steps as documented in the applicable integration guide:

1. Configure the phone system.

2. Configure the PIMG/TIMG units. PIMG/TIMG settings are somewhat phone system-specific, but less so than phone system configuration.
3. Configure Cisco Unity Connection for the integration.

For information on configuring the phone system, PIMG/TIMG units, and Unity Connection, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Firmware Updates

Note that when receiving shipment of PIMG or TIMG units, it may be necessary to update the firmware on the units. The PIMG/TIMG Administration interface provides a simple method to update the firmware files. Firmware updates are available at http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240 (note that you must sign in to www.cisco.com to access the URL). For details, see the applicable integration guide.

Serial Integrations

Cisco Unity Connection supports the following serial protocols:

- SMDI
- MCI
- MD-110

The serial port on PIMG/TIMG units was originally designed as a management port rather than as a standard RS-232 serial port. Consequently, a custom serial cable (which is available from Cisco) is necessary for the data link between the phone system and the master PIMG/TIMG unit.

Increasing Port Capacity

PIMG units have eight ports. To increase system port capacity, multiple PIMG units can be stacked. For example, if 32 ports are needed, four PIMG units can be stacked.

TIMG units, which integrate with circuit-switched phone systems that support T1-CAS, have 24 T1 ports per span in a single rack-optimized unit. Single-span, dual-span, and quad-span TIMG units are available.

Unity Connection Clusters

PIMG/TIMG integrations support Unity Connection clusters (active/active high availability). Configuration changes are required both for the PIMG/TIMG units and for the Unity Connection servers, as described in the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Multiple Integration Support/Branch Office Consolidation

PIMG/TIMG units can be separated by a WAN to support circuit-switched phone systems at remote branch office sites. For example, Cisco Unity Connection could be placed at a centralized headquarters and support circuit-switched phone systems both at the headquarters and at the branch office sites.

As an example, assuming there are four phone systems from four different manufacturers (for example, Nortel, Avaya, NEC, and Siemens), four different phone system integrations could be created on the Unity Connection server to support the four phone systems. A standalone Unity Connection server supports up to 144 ports that connects to the four phone systems. For example:

- At the Seattle site, 15 PIMG units can be stacked to support 120 ports.
- At the New York site, two PIMG units can be stacked to support 16 ports.
- At the Tokyo site, one PIMG unit can be used to support four ports.
- At the Dallas site, one PIMG unit can be used to support two ports.

Note that even though the PIMG units come with eight ports, fewer than eight ports can be used on each unit.

If PIMG units are separated by a WAN to support remote phone systems, correct audio codec selection, bandwidth capacity planning, and QOS planning are required. Both the G.729a and G.711 audio codecs are supported by PIMG units and by Unity Connection. Because PIMG units are Dialogic devices rather than Cisco devices, the use of location-based CAC is not applicable. The following network and bandwidth requirements are required when placing the PIMG across a WAN:

- For the G.729a audio codec, a minimum of 32.76 Kbps (assumes Ethernet, payload of 20 bytes, 5 percent overhead) guaranteed bandwidth for each voice messaging port.
- For the G.711 audio codec, a minimum of 91.56 Kbps (assumes Ethernet, payload of 160 bytes, 5 percent overhead) guaranteed bandwidth for each voice messaging port.
- No network devices that implement network address translation (NAT).

When PIMG units are separated by a WAN, prioritize your call control and media traffic through proper QOS traffic, marking for voice traffic originating on the PIMG units. Set the Call Control QOS Byte and RTP QOS Byte on PIMG units to the following values:

- In the Call Control QOS Byte field, enter 104.
- In the RTP QOS Byte field, enter 184.

Note that the Call Control QOS Byte and RTP QOS Byte fields on PIMG units define a decimal value that represents QOS bit flags. These values can be interpreted as either IPv4 TOS or Differentiated Services Codepoint (DSCP). For more details, see the *Dialogic 1000 and 2000 Media Gateway Series User's Guide*, provided by Dialogic.

Integrating with Multiple Phone Systems

Unity Connection supports as many phone systems as needed up to the maximum number of ports supported per Unity Connection server or active/active server pair. See the *Multiple Phone System Integration Guide for Cisco Unity Connection Release 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/multiple/b_cuc15intmultiple.html.

Requirements for Integrations with Multiple Phone Systems

Unity Connection has the following requirements for multiple phone system integrations:

- All phone system and Unity Connection server requirements have been met. See the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
- There must be an adequate number of voice messaging ports on the Unity Connection server to connect to the phone systems.

Alternate Extensions

In addition to the primary extension for each user, you can set up alternate extensions. Alternate extensions can be used for various reasons, such as handling multiple line appearances on user phones. Alternate extensions can also make calling Cisco Unity Connection from an alternate device—such as a mobile phone, a home phone, or a phone at another work site—more convenient.

When you specify the phone number for an alternative extension, Unity Connection handles all calls from that number in the same way that it handles calls from a primary extension (assuming that ANI or caller ID is passed along to Unity Connection from the phone system). This means that Unity Connection associates the alternate phone number with the user account, and when a call comes from that number, Unity Connection prompts the user to enter a password and sign in.

URI Dialing for Alternate Extensions

Unity Connection supports dialing using URIs for alternate extensions. URIs look like email addresses and follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. A URI is a uniform resource identifier, a string of characters that can be used to identify a directory number. If that directory number is assigned to a phone then Cisco Unity Connection can route calls to that phone using the URI. URI dialing is available for both SIP endpoints that support URIs.

The administrator can import the end users directory URI into Unity Connection from the LDAP directory or Cisco Unified Communications Manager.

Note In HTTPS, CCI, and Diginet networking, URI for alternate extensions is replicated only on the nodes that support directory URI.

Directory URI Format

URIs are alphanumeric strings consisting of a user and a host address separated by the @ symbol. The URI field has a maximum length of 40 characters.

Unity Connection supports the following formats for URIs:

- user@domain (for example, joe@cisco.com)
- user@ip_address (for example, joe@10.10.10.1)

Unity Connection supports the following formats in the user portion of a URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, !, $, %, &, *, _, +, ~, -, =, \, ?, \, ', ,, ., /, "", {}, []. <>.

- The user portion is case sensitive.

Unity Connection supports the following formats in the host portion of a URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are a-z, A-Z, 0-9, hyphens, and dots.
- The host portion cannot start or end with a hyphen.
- The host portion cannot have two dots in a row.
- Minimum of one character.
- The host portion is case sensitive.

Note Use lower case for URIs.

Alternate MWIs

You can set up Cisco Unity Connection to activate alternate MWIs when you want a new message for a user to activate the MWIs at up to 10 extensions. For example, a message left at extension 1001 can activate the MWIs on extensions 1001 and 1002.

Unity Connection uses MWIs to alert the user to new voice messages. MWIs are not used to indicate new email, fax, or return receipt messages.

Centralized Voice Messaging

Cisco Unity Connection supports centralized voice messaging through the phone system, which supports various inter-phone system networking protocols including proprietary protocols such as Avaya DCS, Nortel MCDN, or Siemens CorNet, and standards-based protocols such as QSIG or DPNSS. Note that centralized voice messaging is a function of the phone system and its inter-phone system networking, not voice mail. Unity Connection supports centralized voice messaging as long as the phone system and its inter-phone system networking are properly configured.

When discussing phone systems involved in centralized voice messaging, there are essentially two types:

- **Message Center PINX**—The phone system hosts the voice messaging system (the phone system is directly connected to the voice messaging system).
- **User PINX**—The phone system is remote from the voice messaging system (the phone system is not directly connected to the voice messaging system).

Centralized voice messaging provides voice messaging services to all users in a networked phone system environment. Unity Connection can be hosted on a message center PINX and provide voice messaging services to all users in an enterprise assuming the message center PINX and all user PINX phone systems are properly networked.

For a centralized voice messaging configuration to exist, a suitable inter-phone system networking protocol must exist to deliver a minimum level of feature support, such as:

- Message waiting indication (MWI).
- Transfer, which ensures that the correct calling/called party ID is delivered to the voice messaging system.
- Divert, which ensures that the correct calling/called party ID is delivered to the voice messaging system.

Other features may be required depending on how the voice messaging system is to be used. For example, if it is also serving as an automated attendant, path-replacement is needed as this feature prevents calls from hair-pinning.

Not all phone systems can serve as a message center PINX. In this case, customers may wish to consider relocating Unity Connection to Cisco Unified Communications Manager and have Cisco Unified CM act as the message center PINX with the circuit-switched phone system now acting as the user PINX.

For information on configuring Unity Connection in a centralized voice messaging environment to be hosted on Cisco Unified CM serving as the message center PINX, see the following:

- The application note *Cisco CallManager 4.1-Voicemail Interoperability: Cisco Unity 4.0(4) with Cisco CallManager 4.1(2) Configured as Message Center PINX Using Cisco Catalyst 6608 T1 Q.SIG with MGCP* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/pbx/interop/notes/414111.pdf.
- The applicable application note for configuring QSIG trunks between Cisco Unified Communications Manager and various circuit-switched phone systems on the Cisco Interoperability Portal at http://www.cisco.com/en/US/netsol/ns728/networking_solutions_products_generic_content0900aecd805b561d.html.

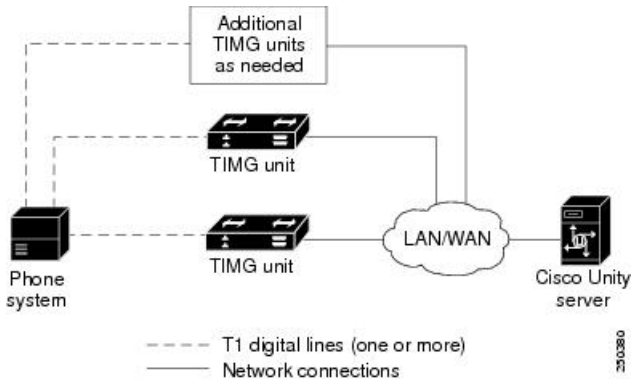
Note that if customers are deploying centralized voice messaging with Unity Connection and a circuit-switched phone system, it is up to the customer to determine whether the circuit-switched phone system can serve as a message center PINX on which Unity Connection can be hosted. If so, the customer should also confirm that there is support for the desired features, for example, MWIs, transfer, divert, and path-replacement.

Inter-cluster trunks between Cisco Unified CM clusters can be QSIG-enabled using the Annex M.1 feature, which allows Unity Connection to integrate with a single Cisco Unified CM cluster. Ports in the cluster with which Unity Connection is integrated can be dedicated to turning MWIs on and off for phones in other clusters.

Integrating Unity Connection with a QSIG-Enabled Phone System Using Cisco ISR Voice Gateways

Unity Connection supports an integration with a QSIG-enabled phone system through a Cisco ISR voice gateway. See Figure 9.

Figure 9: Connections Between the Phone System and Cisco Unity Connection



For more information on integrating Unity Connection with a QSIG-enabled phone system using Cisco ISR voice gateways, see the *QSIG-Enabled Phone System with Cisco ISR Voice Gateway Integration Guide for Cisco Unity Connection 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/sip-qsig_gw/b_cuc15intqsig.html.

Links to Additional Integration Information

For a list of all supported versions of Cisco Unified Communications Manager and Cisco Unified CM Express, see the *Compatibility Matrix for Cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html

For the most current list of other supported phone system integrations, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Unity Connection can integrate with one or more phone systems at the same time. For details, see the *Multiple Phone System Integration Guide for Cisco Unity Connection Release 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/multiple/b_cuc15intmultiple.html.