Networking

HTTPS Networking

Unity Connection supports HTTPS Networking, that allows you to connect different Unity Connection servers and clusters in a single site network. HTTP networking provides more scalable Unity Connection deployments as compared to legacy networking. The architecture of HTTPS networking is scalable both in terms of number of Unity Connection locations and the total directory size. HTTPS Protocol is used for directory synchronization within a network.

In addition to HTTPS networking, Unity Connection also supports legacy networking to connect multiple Unity Connection servers in a network. However, you should deploy a new network as per HTTPS networking. Legacy networking includes both intrasite (digital) and intersite networking.The legacy and HTTPS networking are not supported simultaneously in the same network. In legacy networking, SMTP is the method used within a site, and HTTPS is used in Intersite networking when linking two separate sites.

Designing a Unity Connection Network using HTTPS

When the messaging needs of your organization require more than one Unity Connection server or cluster, you need a way to combine multiple Unity Connection directories or to ensure that the connected servers can communicate with each other. The concept of networking, HTTPS Networking, is introduced to connect different Unity Connection servers and clusters in a network.

Note The legacy (SMTP) and new HTTPS networking are not supported simultaneously in the same network.

In hub-spoke topology, all the directory information among the spokes is shared through the hub(s) connecting the spokes. For example, in the above figure, if spoke A needs to synchronize directory information with spoke E, the directory information flows from spoke A to hub B, hub B to hub C, hub C to hub D, and then from hub D to spoke E.

Each Unity Connection server (or cluster) is represented in the network as a single Unity Connection location, which is created locally during installation and which cannot be deleted from the server itself. When you join the server (or cluster) to an existing location in a network, a Unity Connection location is automatically created for the server (or cluster).

Note Unity Connection Release 14SU3 and later, the directory size limit for users has been increased to 160k in a network . For more information, see *HTTPS Networking Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/https_networking/guide/b_15cuchttpsnet.html.

Note HTTPS networking supports single site networks only. You cannot connect multiple HTTPS networks or single site networks together to form a larger network. The maximum number of Unity Connection locations that you can connect in an HTTPS network is 25. In an HTTPS network the round-trip latency should not be more than 250 ms between Hub and Spoke nodes.

OVA Selection and HTTPS

When deciding which OVA template to deploy, it is important to determine the role of the servers in your environment relative to HTTPS networking. For example, if you are building a VPIM server to support 150,000 VPIM users, you would use the largest OVA template, and the server would only contain VPIM accounts, not subscribers.

Due to the limitations of the smaller OVA templates, you need to take careful consideration of growth as well as whether the node is a hub or spoke in the network when choosing your OVA. If your network size grows past the directory size limits of your chosen OVA, you need to rebuild or replace your servers with larger Novas to accommodate the larger directory size. It is a good idea to select a larger template than you think you need for just this reason. The smallest OVA template, in most cases, should only be used for spoke servers in the network.

For information about the maximum number of locations and other directory objects supported in a Unity Connection site, see the "Directory Object Limits" section in the *System Requirements for Cisco Unity Connection, Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html

Migrating from Legacy (SMTP) Networking to HTTPS Networking

Currently, the only supported method of migrating from legacy networking to HTTPS networking is a manual method. In the future, there is a migration tool available to make the process easier. The migration method is outlined in the *HTTPS Networking Guide for Cisco Unity Connection , Release 15*.

For information about the migration method, see the "Migration from Legacy network to HTTPS Network" chapter in the *HTTPS Networking Guide for Cisco Unity Connection , Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/https_networking/guide/b_15cuchttpsnet.html

.

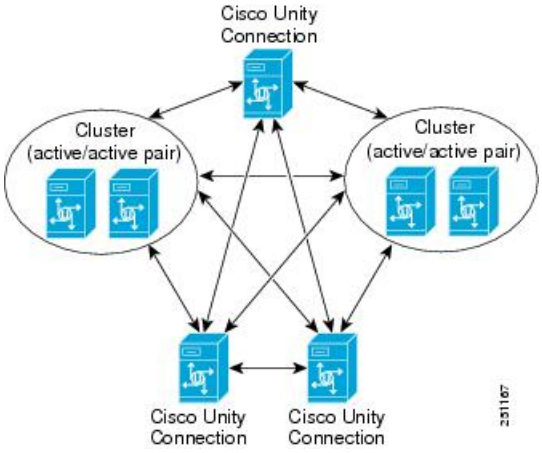
Legacy Networking

Intrasite Networking

If your organization has more users than a single Unity Connection server or cluster pair can support, you can join two or more Connection servers or clusters (up to a maximum of ten) to form a well-connected network, referred to as a Connection site. The servers that are joined to the site are referred to as locations. (When a Connection cluster is configured, the cluster counts as one location in the site.) Each location is said to be linked to every other location in the site via an intrasite link. Figure 5-2 illustrates a site of five Connection locations joined by intrasite links.

Intrasite networking is supported only with Cisco Business Edition 6000/7000.

Figure 1: A Cisco Unity Connection Site Joined by Intrasite Links Among Locations



Within a site, Unity Connection locations automatically exchange directory information, so that a user on one location can dial out to or address messages to a user on any other system by name or extension, provided that the target user is reachable in the search scope of the originating user. The networked systems function as though they share a single directory. Users do not need to know where another user is located; they need only the name or extension number to address a message to any user or system distribution list in the directory.

Because intrasite links use SMTP transport for both directory replication and message transport, Unity Connection locations in a site can be deployed across geographic boundaries. Each server that is joined to the site must be able to access all other servers in the site directly through TCP/IP port 25, or SMTP messages must be routable among the servers through an SMTP smart host.

If your site includes a Unity Connection cluster, you must have a smart host available to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down.

In a site, each Unity Connection object is created and homed on a single Unity Connection location. An object can only be modified or deleted on the location where it was created. Each location has its own directory of users and other objects, and replicates a subset of these objects and their properties to other locations.

The following objects are replicated in a Unity Connection site:

- Users

- Administrator-defined contacts (including those associated with a VPIM location)
- System distribution lists (including membership)
- Locations (Unity Connection and VPIM)
- Partitions
- Search spaces
- Recorded voice names

For information about the maximum number of locations and other directory objects supported in a Unity Connection site, see the "Directory Object Limits" section in the *System Requirements for Cisco Unity Connection, Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html

You can also optionally deploy additional cross-server features between locations in a site. Cross-server sign in allows all users to dial the same number when calling from outside the organization to sign in to Unity Connection, regardless of which Unity Connection server they are homed on. Cross-server transfer enables calls from the automated attendant of one Unity Connection location to be transferred to a user on another networked Unity Connection location, according to the call transfer and screening settings of the called user. When you enable cross-server transfer, cross-server live reply is also enabled, allowing users to return calls to message senders who are users on other networked Unity Connection locations, according to the call transfer and screening settings of the called user.

The Unity Connection site concept was known as a Digital Network in release 7.x. You can join 7.x locations, 8.x locations, and 9.x locations, 10.x locations, 11.x locations and 12.x locations in the same Unity Connection site, as long as you do not link the site to any other site.

For more information on intrasite networking, see the "Overview of Networking Concepts" chapter of the *Networking Guide for Cisco Unity Connection, Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/https_networking/guide/b_15cuchttpsnet.html.

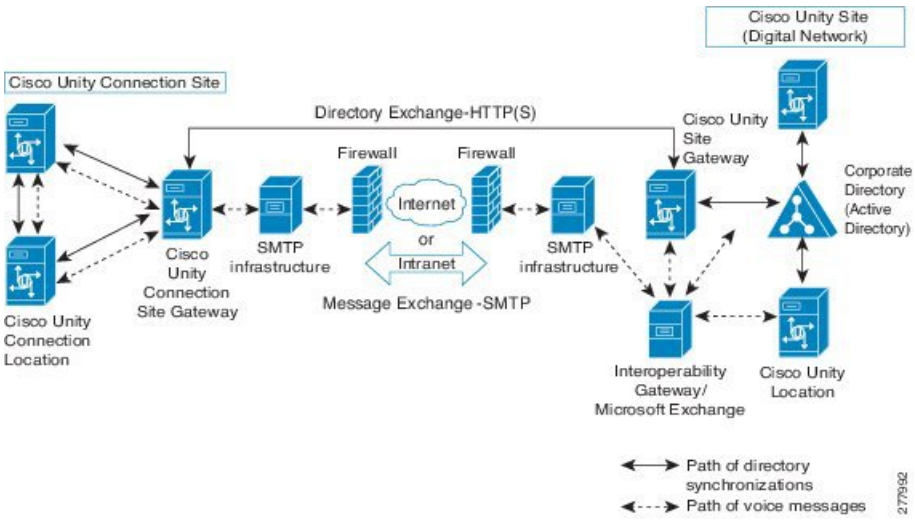
Intersite Networking between Two Unity Connection Sites

You can use an intersite link to connect one Unity Connection site to another Unity Connection site, allowing you to scale your organization from a maximum of ten locations to a maximum of twenty. The linked sites are referred to as a Cisco Voicemail Organization.

To create an intersite link, you select a single location from each site to act as a gateway to the other site. All directory synchronization communications and voice messages pass between the two site gateways, thereby limiting the connectivity requirements and bandwidth usage to the link between those two site gateway locations. The gateways use the HTTPs protocol to exchange directory synchronization updates. Intersite voice messages are transmitted and received via SMTP.

Figure 5-3 illustrates the role of the site gateways and the intersite link in connecting two Connection sites.

Figure 2: Cisco Voicemail Organization Consisting of Two Unity Connection Sites Linked via an Intersite Link



Only one intersite link is supported per site. (This restriction applies to all types of intersite links, so you cannot link a Unity Connection site to another Unity Connection site and also to a Cisco Unity site.) In order to link a Unity Connection site to another site, all Unity Connection locations in the site must be running Unity Connection release 8.0 or later. Intersite Networking is not supported for use with Cisco Business Edition.

As with intrasite networking, users, system distribution lists, partitions, search spaces, and Unity Connection locations are replicated between sites. (System distribution list replication is optional.) However, contacts, system distribution list membership, and VPIM locations are not replicated between sites. Also, site gateways do not relay VPIM messages to other sites. Therefore, to deploy VPIM in the entire organization, you must independently configure each site for VPIM.

All of the optional cross-server features that are available within a Unity Connection site (cross-server sign in, cross-server transfers, and cross-server live reply) are also available between sites.

When you use a Unity Connection cluster as a site gateway, only the publisher server in the cluster participates in directory synchronization over the intersite link. However, the subscriber server can continue to provide message exchange over the intersite link if the publisher server is down. Note that in this configuration you must have a smart host available to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down.

For more information on intersite networking, see the "Overview of Networking Concepts" chapter of the *Networking Guide for Cisco Unity Connection, Release 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/https_networking/guide/b_15cuchttpsnet.html.

Designing a Unity Connection Network with Intrasite and Intersite Links

If you have a requirement to mix Unity Connection servers running releases 7.x, 8.x, 9.x, 10.x, 11.x, and 12.x or if you have more than 10 locations to network, the design is fairly straightforward—you must use only intrasite links if mixing release versions, and you must use a combination of intrasite links and an intersite link if you have more than 10 locations. However, if you have up to 10 Unity Connection locations and have the flexibility to run version 10.x on all of them, you can choose whether to link all locations in the same Connection site or to create two sites and link them together.

Table 2 helps you compare and contrast the benefits and drawbacks of each type of link.

Table 1: Intrasite Networking Versus Intersite Networking

	Intrasite Networking	Intersite Networking

Benefits	• Easier to administer:
	  • System distribution list membership is replicated throughout the site, so you do not have to decide which site should home a list.
	  • For each remote messaging server that you connect to via VPIM, you only have to configure VPIM location details once.
	• The message recall feature works across all locations in the site.
	• You can mix Unity Connection release 7.x, 8.x, 9.x, 10.x, 11.x and 12.x servers.
	• You have the flexibility to add an intersite link to a Cisco Unity Digital Network or to another Unity Connection site in the future.
		• Supports up to 20 locations (in combination wit networking).
		• Requires less bandwidth than intrasite network replication traffic over the intersite link, particu there are many locations on each side of the lir
		  • Data is replicated once between the gatew the link rather than being replicated direct nodes in the network.
		  • System distribution list membership is not across the link.
		  • Replication can be scheduled to occur onl off-hours.
		  • The intersite link uses a synchronous prot is more bandwidth-efficient than SMTP.

Drawbacks	• Requires higher bandwidth for replication than intersite networking. • Supports only up to 10 locations.	• Requires more administrative overhead, especi both sites must be configured for VPIM locatio • Message recall does not work between sites. • All locations must be running Unity Connectio 12.x. • Does not allow for linking to a Cisco Unity Di Network.

Note Dispatch messaging does not work between locations either within the same site or across sites. VPIM Networking

VPIM Networking

Cisco Unity Connection 10.x supports the Voice Profile for Internet Mail (VPIM) protocol, which is an industry standard that allows different voice messaging systems to exchange voice and text messages over the Internet or any TCP/IP network. VPIM is based on the Simple Mail Transfer Protocol (SMTP) and the Multi-Purpose Internet Mail Extension (MIME) protocols.

Unity Connection supports internetworking with voice messaging systems that support the VPIM version 2 protocol, as defined in Internet RFC 3801. For a list of messaging systems that are supported by Unity

Connection for VPIM networking, see the "Requirements for VPIM Networking " section in the System Requirements for Cisco Unity Connection, Release 15, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html.

Each Unity Connection server, cluster pair, or site has a maximum number of VPIM locations and VPIM contacts that it can support. For limit information, see the " Directory Object Limits for Unity Connection " section in the System Requirements for Cisco Unity Connection, Release 15, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html. When intrasite networking is configured, VPIM location and contact information is replicated to all locations in the site. If you deploy both VPIM and intrasite networking, you should designate a single Unity Connection location in the site as the bridgehead to handle the configuration of VPIM locations and contacts. Managing these objects from a single location simplifies maintenance tasks and avoids potential overlaps in contact information that could cause confusion to users when they attempt to address messages. VPIM locations and contacts are not replicated over intersite links, and site gateways do not relay VPIM messages to other sites. Therefore, if you deploy VPIM in a Cisco Voicemail Organization consisting of two Unity Connection sites or of a Unity Connection site and a Cisco Unity site, you must independently configure each site for VPIM.

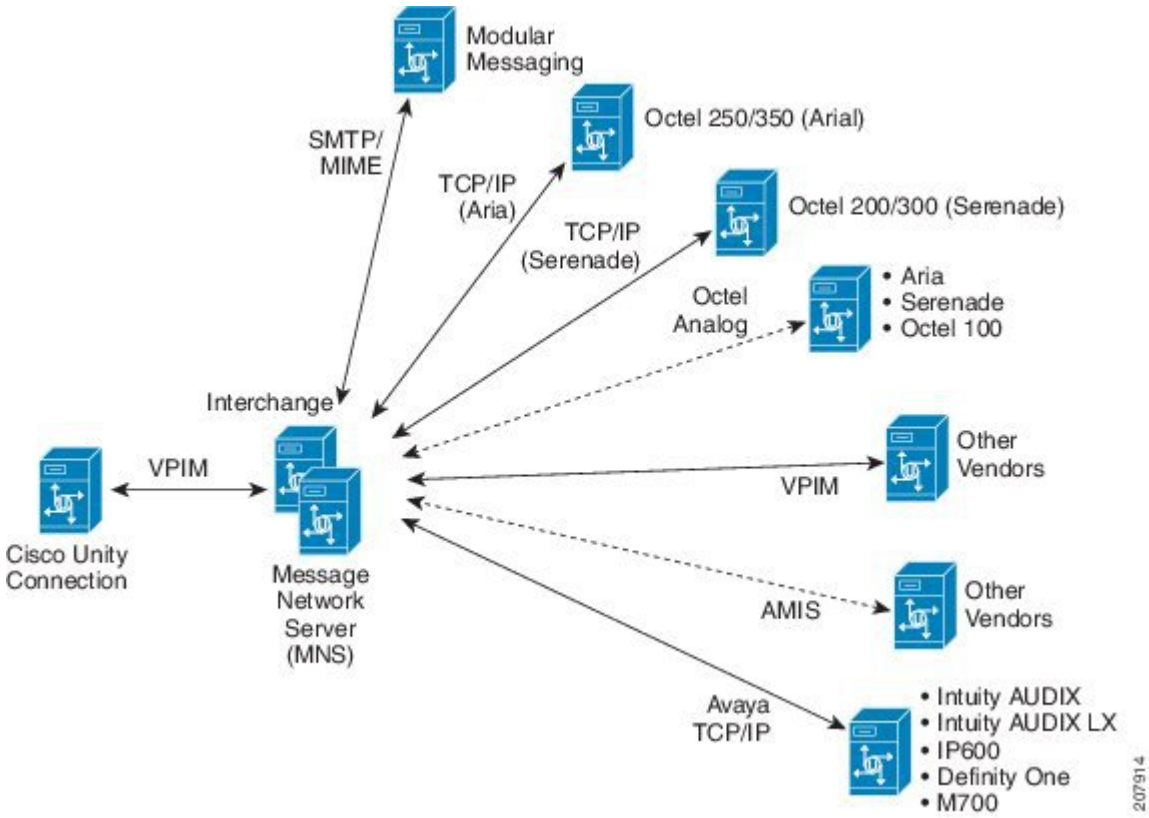
To internetwork with more VPIM locations than your server, cluster, or site can support, you can use the Cisco Unified Messaging Gateway (Cisco UMG). The Cisco UMG is configured as a single VPIM location in Unity Connection, and acts as a central hub to handle message routing and delivery to other systems (Cisco Unity, Cisco Unity Connection, Cisco Unity Express, or Avaya Message Networking solution/Interchange) that are connected to it.

For more information on VPIM Networking, design considerations, and configuration details, see the "VPIM Networking" chapter of the Networking Guide for Cisco Unity Connection Release 15, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/networking/guide/b_15cucnetx.html

Using VPIM between Unity Connection and Avaya Message Networking Solution or Avaya Interchange

The Avaya Message Networking solution (or the Avaya Interchange) uses a hub-and-spoke topology to allow voice messaging between systems, using a number of protocols, thus allowing a voice messaging system such as Cisco Unity Connection to send and receive network voice messages with any other system in the network. Unity Connection uses the VPIM protocol to communicate with the Interchange, and the Interchange takes care of routing the messages to and from other systems on the network using the applicable protocol. Figure 5-5 illustrates an example topology.

Figure 3: Cisco Unity Connection Communicates with the Avaya Message Network Solution



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 Unity Connection SRSV at branch location Unity Connection, see the guide available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/srsv/guide/b_15cucsrsvx.html