CHAPTER 25

Mobile Unified Communications

Revised: July 31, 2012; OL-21733-18

Mobile Unified Communications solutions and applications provide the ability to deliver features and functionality of the enterprise IP communications environment to mobile workers wherever they might be. With mobile Unified Communications solutions, mobile users can handle business calls on a multitude of devices and access enterprise applications whether moving around the office building, between office buildings, or between geographic locations outside the enterprise. Mobile Unified Communications solutions provide mobile workers with persistent reachability and improved productivity as they move between, and work at, a variety of locations.

Unified Communications mobility solutions can be divide into two main categories:

- Mobility within the enterprise

  This type of mobility is limited to movement of users within enterprise locations.

- Mobility beyond the enterprise

  This type of mobility refers to mobility beyond the enterprise infrastructure and typically involves some form of Internet, mobile voice network, and/or mobile data network traversal.

Mobility within the enterprise is limited to utilization within the network boundaries of the enterprise, whether those boundaries span only a single physical building, multiple physical buildings in close proximity or separated by long distances, or even home offices where network infrastructure is still controlled and managed by the enterprise when it is extended to the home office.

On the other hand, mobility beyond the enterprise involves a bridging of the enterprise infrastructure to the Internet or mobile provider infrastructures and finds users leveraging public and private networks for connectivity to enterprise services. In some cases the lines between these two types of mobility are somewhat blurred, especially in scenarios where mobile devices are connecting back to the enterprise for Unified Communications services over the Internet or mobile data and mobile voice networks.

Mobility within the enterprise can be divided into three main areas based on feature sets and solutions:

- Campus or single-site mobility

  With this type of enterprise mobility, users move around within a single physical location typically bounded by a single IP address space and PSTN egress/ingress boundary. This type of mobility involves operations and features such as phone movement from one physical network port to another, wireless LAN device roaming between wireless infrastructure access points, and even Cisco Extension Mobility (EM), where users temporarily apply their device profile including their enterprise number to a particular phone in a different area.

- Multisite mobility

  With this type of mobility, users move within the enterprise from one physical location to another, and this movement typically involves crossing IP address spaces as well as PSTN egress/ingress boundaries. This type of mobility involves the same types of operations and features as with campus mobility (physical hardware moves, WLAN roaming, and Cisco Extension Mobility) but replicated at each site within the enterprise. In addition, the Device Mobility feature can be leveraged to ensure that, as user's move devices between sites, phone calls are routed through the local site egress gateway, media codecs are negotiated appropriately, and call admission control mechanisms are aware of the device's location.

- Remote site mobility

  With this type of mobility, users move to a location outside the enterprise but still have some form of secure connection back to the enterprise, which virtually extends the enterprise network to the remote location. This type of mobility typically involves remote teleworker solutions such as Cisco Virtual Office as well as other remote connectivity methods such as VPN-based phones and the Office Extend Access Point feature.

Mobility beyond the enterprise can be divided into four high-level Cisco solution sets:

- Cisco Unified Mobility

  As part of Cisco Unified Communications Manager (Unified CM), the Cisco Unified Mobility feature suite offers the ability to associate a mobile user's enterprise number to their mobile or remote devices and provides connectivity between the user's fixed enterprise desk phone on the enterprise network and the user’s mobile device on the mobile voice provider network. This type of functionality is sometimes referred to as fixed mobile convergence.

- Dual-mode phones and clients

  Dual-mode phones and devices provide dual radio antennas for connecting to both 802.11 wireless LAN networks and cellular voice and data networks. With a dual-mode client deployed on these devices, they can be associated to Unified CM through the enterprise wireless LAN or over a secure Internet-based connection (public or private WLAN hot spot or mobile data network) and can in turn leverage the IP telephony infrastructure of the enterprise for making and receiving calls. When mobile users do not have connectivity to the enterprise with these devices, phone calls are made using the mobile voice provider network.

- Cisco Unified Mobile Communicator

  The Cisco Unified Mobile Communicator solution provides remote access to a variety of enterprise Unified Communications applications from a user's mobile device. By connecting to the enterprise over a secure mobile data connection, the Cisco Unified Mobile Communicator client has access to enterprise mobility features as well as call routing, voicemail, and presence services.

- Direct connect mobile clients

  Direct connect mobile clients also provide secure remote access to enterprise voice and collaboration applications and services such as call routing, corporate directory access, and presence and instant messaging services, all from a user's mobile device. These clients also provide dual-mode functionality, enabling voice over WLAN capabilities when connected to the enterprise WLAN network.

The various applications and features discussed in this chapter apply to all Cisco Unified Communications deployment models unless otherwise noted.

This chapter begins with a discussion of mobility features and solutions available within the enterprise infrastructure. It includes an examination of functionality and design considerations for campus or single-site deployments, multisite deployments, and even remote site deployments. This comprehensive set of solutions provides many benefits for mobile workers within the enterprise, including

enterprise-class communications and improved productivity regardless of physical location. This discussion of mobility within the enterprise paves the way for examination of mobility solutions beyond the enterprise that leverage the mobile provider and Internet provider infrastructure and capabilities. These solutions enable a bridging of the enterprise network infrastructure and mobile functionality to the provider network infrastructure in order to leverage advanced mobile features and communication flows that can be built on the solid enterprise mobility infrastructure.

This chapter provides a comprehensive examination of mobility architectures, functionality, and design and deployment implications for enterprise Unified Communications mobility solutions. The analysis and discussions contained within this chapter are organized at a high level as follows:

- Mobility within the Enterprise
  - Campus Enterprise Mobility, page 25-5
  - Multisite Enterprise Mobility, page 25-13
  - Remote Enterprise Mobility, page 25-32
- Mobility beyond the Enterprise
  - Cisco Unified Mobility, page 25-38
  - Dual-Mode Phones and Clients, page 25-66
  - Cisco Unified Mobile Communicator, page 25-87
  - Direct Connect Mobile Clients, page 25-102

What's New in This Chapter

Table 25-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 25-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in	Revision Date
Minor corrections and change	Various sections throughout this chapter	July 31, 2012
Cisco Jabber for iPhone dual-mode/direct connect mobile client	Dual-Mode Clients: Cisco Mobile and Cisco Jabber, page 25-74	April 30, 2012
Cisco Jabber IM clients for XMPP-based IM and presence	XMPP-Based IM and Presence, page 25-109	April 30, 2012
End-of-Sale (EoS) and End-of-Life (EoL) notices for Nokia Call Connect, Cisco Unified Mobile Communicator, and Cisco Mobile 8.5 for Nokia	Dual-Mode Clients: Nokia Call Connect, page 25-80 Cisco Unified Mobile Communicator, page 25-87 Direct Connect Mobile Client: Cisco Mobile 8.5 for Nokia, page 25-110	April 30, 2012

Table 25-1 New or Changed Information Since the Previous Release of This Document (continued)

New or Revised Topic	Described in	Revision Date
Mobile client remote secure connectivity considerations, including voice quality, connectivity issues, and Cisco AnyConnect and Jabber secure connect	Dual-Mode Phone Architecture, page 25-66 Remote Secure Enterprise Connectivity, page 25-72 Cisco AnyConnect and Secure Connect, page 25-80 VPN Infrastructure, page 25-104	April 30, 2012
Minor corrections and changes	Various sections throughout this chapter	July 29, 2011
Cisco Jabber 8.6 dual-mode client for Android devices	Dual-Mode Phones and Clients, page 25-66	June 2, 2011
Direct connect mobile clients solution, including coverage for the Cisco Mobile 8.5 for Nokia client	Direct Connect Mobile Clients, page 25-102	June 2, 2011
Mobile Toll Bypass Optimization feature	Mobile Toll Bypass Optimization, page 25-108	June 2, 2011
Session Resumption feature (formerly, Dial-via-Office Forward Redial)	Session Resumption, page 25-107	June 2, 2011
Cisco Mobile iPhone dual-mode client desk phone integration	Dual-Mode Clients: Cisco Mobile and Cisco Jabber, page 25-74	November 15, 2010
Enterprise campus, multisite, and remote mobility solutions and features	Mobility Within the Enterprise, page 25-5	November 15, 2010
The original Device Mobility chapter has been eliminated from this version of the SRND, and its content has been merged with this chapter on Mobile Unified Communications.	Device Mobility, page 25-16	November 15, 2010
Enterprise Feature Access two-stage dialing feature automation available with the Nokia Call Connect dual-mode client	Dual-Mode Clients: Nokia Call Connect, page 25-80	July 23, 2010
Handoff Number method of hand-out for Cisco Mobile iPhone dual-mode clients	Dual-Mode Clients: Nokia Call Connect, page 25-80	July 23, 2010
WLAN design guidance regarding AP-to-AP roaming for Cisco Mobile iPhone dual-mode client	WLAN Design Considerations for Cisco Mobile and Cisco Jabber Dual-Mode Clients, page 25-79	July 23, 2010
WLAN design guidance regarding handoff and AP-to-AP roaming for the Nokia Call Connect dual-mode client	WLAN Design Considerations for Nokia Call Connect Dual-Mode Client, page 25-83	July 23, 2010
Dual-mode phone solutions, including coverage for the Cisco Mobile iPhone dual-mode client and the Nokia Call Connect dual-mode client	Dual-Mode Phones and Clients, page 25-66	April 2, 2010
Intelligent Session Control feature, which provides mobility call anchoring for calls originated inside the enterprise and destined for remote destination or mobility identity numbers	Dial Plan Considerations for Cisco Unified Mobility, page 25-58	April 2, 2010

Table 25-1 New or Changed Information Since the Previous Release of This Document (continued)

New or Revised Topic	Described in	Revision Date
New mid-call Session Handoff feature invoked by using *74 (default feature access code), and the implications for the desk phone pickup operation	Desk Phone Pickup, page 25-41	April 2, 2010
Unified Mobility capacity planning information for Cisco Business Edition	Capacity Planning for Cisco Unified Mobility, page 25-63	April 2, 2010

Mobility Within the Enterprise

This section examines mobility features and solutions available within the enterprise. This examination includes discussions related to architecture, functionality, and design and deployment implications for the following types of enterprise mobility

- Campus Enterprise Mobility, page 25-5
- Multisite Enterprise Mobility, page 25-13
- Remote Enterprise Mobility, page 25-32

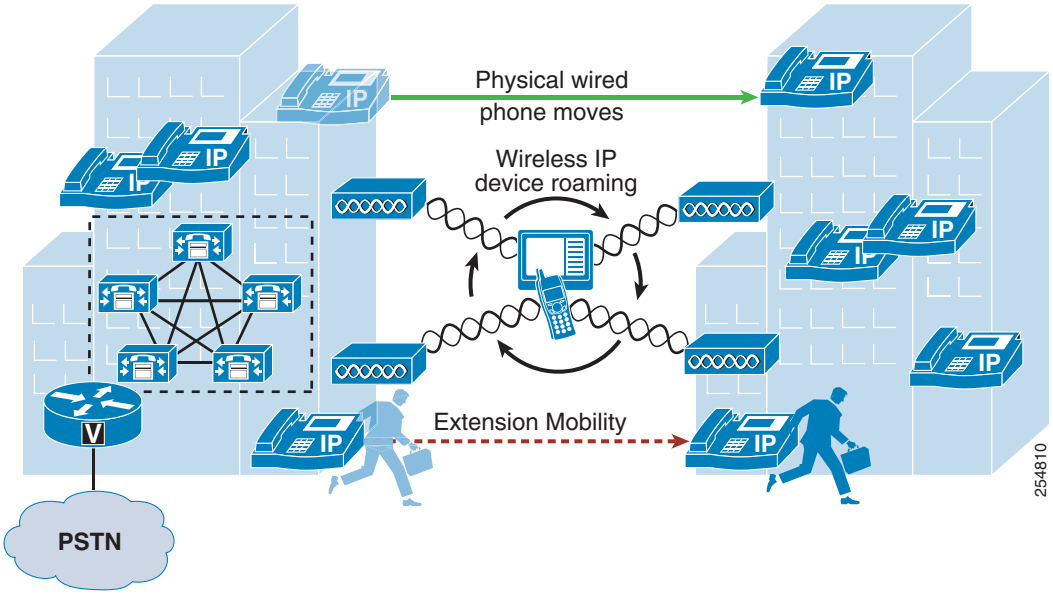
Campus Enterprise Mobility

Campus or single-site enterprise mobility refers to mobility within a single physical location typically bounded by a single IP address space and PSTN egress/ingress boundary. Mobility here not only includes the movement of users within this physical location but also the movement of endpoint devices.

Campus Enterprise Mobility Architecture

As illustrated in Figure 25-1, the enterprise campus mobility architecture is based on a single physical location that may include a single building or multiple buildings (as depicted) in close proximity, such that users are able to move freely within the campus and maintain IP and PSTN connectivity. Typically campus deployments involve a shared common connection or set of connections to the PSTN and Internet provider networks bound by a single IP address space and PSTN egress/ingress boundary. All users within this enterprise campus are connected to and reachable from a common network infrastructure.

Figure 25-1 Campus Enterprise Mobility Architecture



Types of Campus Mobility

Mobility within the campus enterprise typically involves the movement of devices, users, or both throughout the campus infrastructure. Campus enterprise mobility within Cisco Unified Communications deployments can be divided into three main categories: physical wired phone movement, wireless device movement, and user movement without phone hardware or software. Each of these types of movements are discussed below.

Physical Wired Device Moves

As shown in Figure 25-1, movement of physical wired phones is easily accommodated within the campus infrastructure. These types of phone movements can occur within a single floor of a building, across multiple floors of a building, or even between buildings within the campus. Unlike with traditional PBX deployments where physical phone ports are fixed to a particular office, cubicle, or other space within the building, in IP telephony deployments a phone can be plugged into any IP port within the network infrastructure in order to connect to the IP PBX.

In a Cisco environment, this means a user can simply unplug a Cisco Unified IP Phone from the network, pick it up and carry it to another location within the campus, and plug it into another wired network port. Once connected to the new network location, the phone simply re-registers to Unified CM and is able to make and receive calls just like in the previous location.

This same physical device movement also applies to software-based phones running on wired personal computers. For example, a user can move a laptop computer running Cisco IP Communicator or Cisco Unified Personal Communicator from one location to another within the campus, and after plugging the laptop into a network port in the new location, the software-based phone can re-register to Unified CM and begin to handle phone calls again.

To accommodate physical device mobility within the campus, care should be taken when physically moving phone devices or computers running software-based phones to ensure that the network connection used at a new location has the same type of IP connectivity, connection speed, quality of service, security, and network services such as in-line power and dynamic host control protocol (DHCP), as were provided by the previous location. Failure to replicate these connection parameters, services, and features will lead to reduced functionality or in some cases complete loss of functionality.

Wireless Device Roaming

Wireless devices can move or roam throughout the enterprise campus, as shown in Figure 25-1, provided a wireless LAN network has been deployed to provide wireless network connectivity to the campus edge.

Examples of wireless devices include Cisco Unified Wireless IP Phone 7925G, wirelessly attached Cisco Unified IP Phone 9971, Cisco Cius, direct connect mobile clients such as Cisco Mobile 8.5 for Nokia (see Direct Connect Mobile Clients, page 25-102), and dual-mode phone clients such as Cisco Jabber and Nokia Call Connect (see Dual-Mode Phones and Clients, page 25-66).

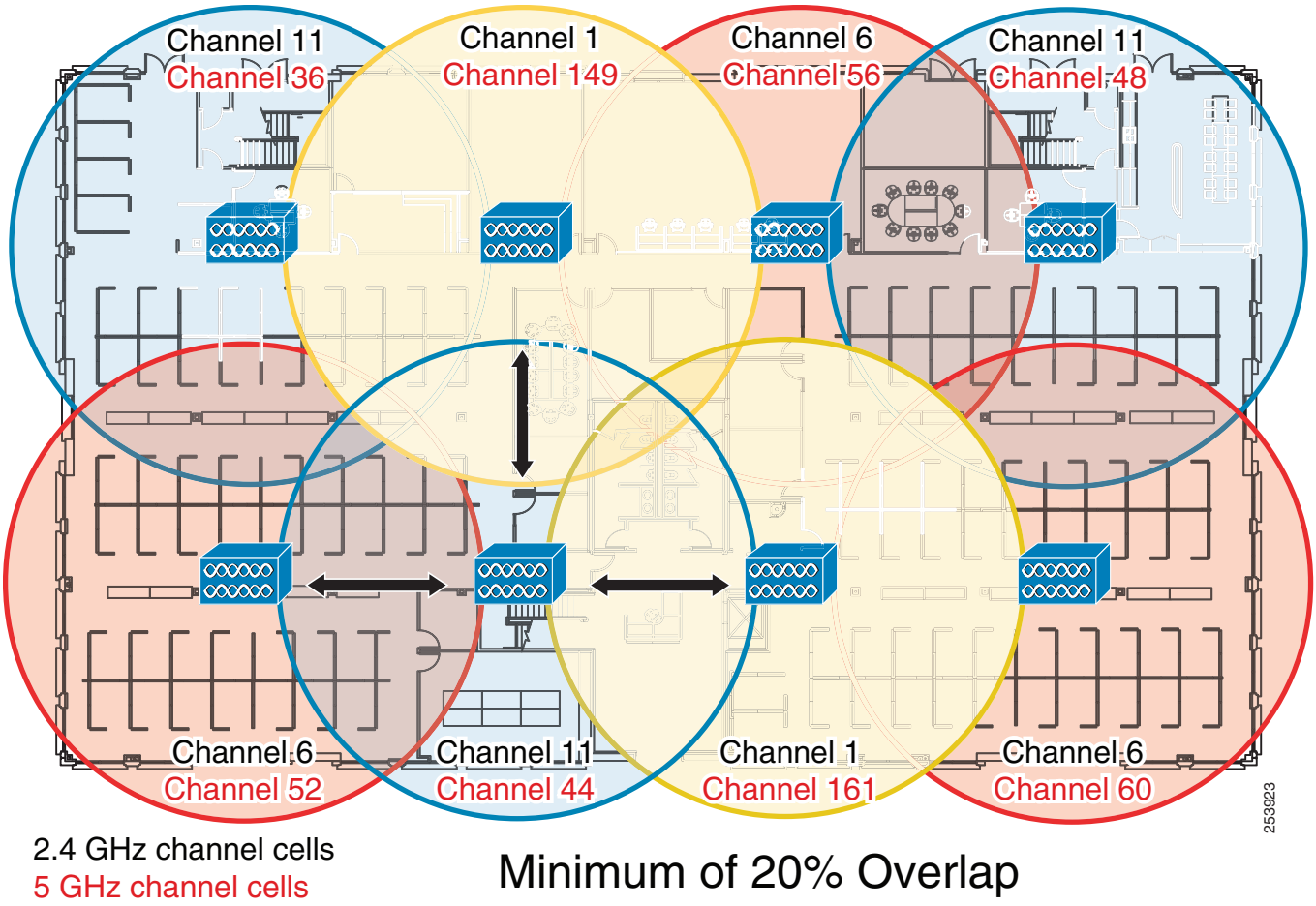
A WLAN network consists of one or more wireless access points (APs), which provide wireless network connectivity for wireless devices. Wireless APs are the demarcation point between the wireless network and the wired network. Multiple APs are deployed and distributed over a physical area of coverage in order to extend network coverage and capacity.

Because wireless phones rely on the underlying WLAN infrastructure to carry both critical signaling and the real-time voice media traffic, it is necessary to deploy a WLAN network optimized for both data and real-time voice traffic. A poorly deployed WLAN network will be subjected to large amounts of interference and diminished capacity, leading not only to poor voice quality but in some cases dropped or missed calls. This will in turn render the WLAN deployment unusable for making and receiving voice calls. Therefore, when you deploy wireless phones and client devices, it is imperative to conduct a WLAN radio frequency (RF) site survey before, during, and after the deployment to determine appropriate cell boundaries, configuration and feature settings, capacity, and redundancy to ensure a successful voice over WLAN (VoWLAN) deployment.

APs can be deployed autonomously within the network so that each AP is configured, managed, and operated independently from all other APs, or they can be deployed in a managed mode in which all APs are configured, managed, and controlled by a WLAN controller. In the latter mode, the WLAN controller is responsible for managing the APs as well as handling AP configuration and inter-AP roaming. In either case, to ensure successful VoWLAN deployment, APs should be deployed using the following general guidelines:

- As shown in Figure 25-2, non-adjacent WLAN AP channel cells should overlap by a minimum of 20%. This overlap ensures that a wireless device can successfully roam from one AP to the next as the device moves around within the campus location while still maintaining voice and data network connectivity. A device that successfully roams between two APs is able to maintain an active voice call without any noticeable change in the voice quality or path.

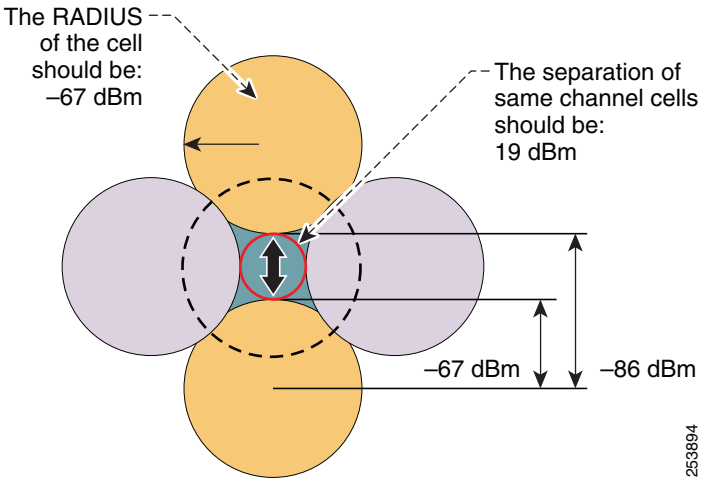
Figure 25-2 WLAN Channel Cell Overlap



- As shown in Figure 25-3, WLAN AP channel cells should be deployed with cell power-level boundaries (or channel cell radius) of -67 decibels per milliwatt (dBm). Additionally, the same-channel cell boundary separation should be approximately 19 dBm.

  A cell radius of approximately -67 dBm (or less) minimizes packet loss, which can be problematic for real-time voice traffic. A same-channel cell separation of 19 dBm is critical to ensure that APs or clients do not cause co-channel interference to other devices associated to the same channel, which would likely result in poor voice quality. The cell radius guideline of -67 dBm applies for both 2.4 GHz (802.11b/g) and 5 GHz (802.11a) deployments.

Figure 25-3 WLAN Cell Radius and Same Channel Cell Separation



Note The 19 dBm same-channel cell separation is simplified and is considered ideal. It is very unlikely that this 19 dBm of separation can be achieved in most deployments. The most important RF design criteria are the -67 dBm cell radius and the minimum 20% recommended overlap between cells. Designing to these constraints optimizes channel separation.

Wireless roaming is not limited to wireless phones but also applies to software-based phones running on wireless personal computers. For example, a user can roam wirelessly throughout the campus with a laptop computer running Cisco IP Communicator or Cisco Unified Personal Communicator.

Most wireless APs, wireless phones, and wireless PC clients provide a variety of security options for providing secure access to the enterprise WLAN. In all cases, select a security method supported by both the WLAN infrastructure and the wireless devices that matches the security policies and requirements of the enterprise.

For more information on the Cisco Unified Wireless Network Infrastructure, see Wireless LAN Infrastructure, page 3-57. For more details on Voice over WLAN design, refer to the *Voice over Wireless LAN Design Guide*, available at

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_voice_wireless.html

Extension Mobility (EM)

As shown in Figure 25-1, in addition to physical movement of wired and wireless phones, the users themselves can also move around within the campus infrastructure without phone or PC hardware. In these cases, a user can move their enterprise extension or number from one device to another by applying a device profile containing the user's enterprise number and other settings.

The EM feature allows users to log on to IP phones located throughout the campus using a set of security credentials (user ID and PIN number). Once logged on, the user's personal device profile, including their enterprise phone number, calling privileges, and even their configured speed dials, is applied to the phone temporarily until the user logs out of the device or the login times out. The EM feature is available as part of Unified CM.

This feature is particularly useful for mobile enterprise users who spend considerable amounts of time outside the enterprise and are physically in the office only occasionally. By providing temporary office space for these types of mobile users, sometimes referred to as hot seating or free seating, a system administrator can accommodate large numbers of mobile users who only occasionally and temporarily need to use IP phone hardware.

To leverage EM within the campus the Unified CM administrator must configure user device profile(s) and user credentials, and subscribe IP phone(s) to the EM phone service.

For more information about EM, see Extension Mobility, page 19-7.

Campus Enterprise Mobility High Availability

Campus enterprise mobility features and solutions should be configured and deployed in a redundant fashion to ensure high availability of mobility functions and features.

For example, to effectively support hard-wired IP phones and computers running software-based IP phones, redundant and prevalent network connections or ports should be made available. Furthermore, these redundant network connections should be deployed with appropriate characteristics, including appropriate security, quality of service, and other network-based features to ensure optimal operation and voice quality for wired devices as they are moved from location to location. Ultimately a successful campus mobility deployment is possible only if the underlying network connectivity, PSTN connectivity, and other applications and services are deployed in a highly available fashion.

Likewise, when deploying or tuning a WLAN network for wireless device connectivity and roaming, it is also important to consider high availability for wireless services. To ensure resilient and sufficient coverage for the number of devices being deployed, a WLAN network should be deployed in a manner that ensures that adequate and redundant cells of coverage are provided without overlapping same-channel cells. Network connectivity for wireless devices and clients can be made highly available by providing ample cell coverage without same-channel cell overlap and sufficient overlap of different channel cells in order to facilitate roaming between APs.

Finally, when leveraging EM for user mobility within the campus, you should deploy this feature in a redundant fashion so that the failure of a single node within the Unified CM cluster does not prevent the operation of the Extension Mobility feature. For information on deploying Cisco Extension Mobility in a highly available manner, see High Availability for Extension Mobility, page 19-14.

Capacity Planning for Campus Enterprise Mobility

Deploying campus enterprise mobility successfully requires providing ample capacity to accommodate all mobile users exercising these mobility features and solutions.

Capacity considerations for physical movement of wired devices and computers depend completely on the number of network ports that are made available within the campus network infrastructure. In order for users to move devices around the campus, there must be some number of available network ports in each location that can be used to connect these mobile users' devices. A shortage of network ports to accommodate this wired device movement can result in an inability to move a device physically from one location to another.

When deploying wireless devices and leveraging wireless device roaming within the enterprise WLAN, it is also important to consider the device connectivity and call capacity of the WLAN infrastructure. Oversubscription of the campus WLAN infrastructure in terms of number of devices or number of active calls will result in dropped wireless connections, poor voice quality, and delayed or failed call setup. The chances of oversubscribing a VoWLAN deployment are greatly minimized by deploying sufficient numbers of APs to handle required call capacities. AP call capacities are based on the number of simultaneous VoWLAN bidirectional streams that can be supported in a single channel cell area. The general rule for VoWLAN call capacities is as follows:

- Maximum of 27 simultaneous VoWLAN bidirectional streams per 802.11g/n (2.4 GHz) channel cell with Bluetooth disabled and 24 Mbps or higher data rates.
- Maximum of 27 simultaneous VoWLAN bidirectional streams per 802.11a/n (5 GHz) channel cell with 24 Mbps or higher data rates.

These call capacity values are highly dependent upon the RF environment, the VoWLAN wireless handset features, and underlying WLAN system features. Actual capacities for a particular deployment could be less.

Note A single call between two wireless phones associated to the same AP is considered to be two simultaneous VoWLAN bidirectional streams.

Scalability of EM is dependent almost completely on the login/logout rate of the feature within Unified CM. A maximum of 375 sequential login and logout operations per minute is supported per Unified CM cluster when login and logout operational load is spread across two nodes of the cluster. Depending on the Unified CM cluster server hardware, the capacity of a deployment could be much less than this. Therefore, it is important to know the number of extension mobility users enabled within the Unified CM cluster as well as how many users are moving around the campus and exercising this feature at any given time to ensure that sufficient EM login/logout capacity can be provided to these mobile users. For more information on EM capacity planning, see Capacity Planning for Extension Mobility, page 19-16.

In all cases, the Unified CM cluster within the campus must have sufficient device registration capacity to handle device registration for moved devices, regardless of whether they are wired or wireless devices. Of course, assuming all devices being moved throughout the campus are already deployed within the campus network, then sufficient capacity within Unified CM should already be in place prior to the movement of devices. If new devices are added to the deployment for mobility purposes, however, device registration capacity should be considered and, if necessary, additional capacity should be added.

Finally, given the many features and functions provided by Unified CM, configuration and deployment of these mobility solutions does have sizing implications for the overall system. Determining actual system capacity is based on considerations such as the number of endpoint devices, EM users, busy hour

call attempt (BHCA) rates, and number of CTI applications deployed. For more information on general system sizing, capacity planning, and deployment considerations, see the chapter on Unified Communications Design and Deployment Sizing Considerations, page 29-1.

Design Considerations for Campus Enterprise Mobility

Observe the following design recommendations when deploying campus enterprise mobility features and solutions:

- To accommodate physical device mobility within the campus ensure that the network connection used at a new location has the same type of IP connectivity (VLANs, inter-VLAN routing, and so forth), connection speed, quality of service, security, and network services (in-line power, dynamic host control protocol (DHCP), and so forth) as provided by the previous network connection. Failure to replicate these connection parameters, services, and features will lead to diminished functionality and in some case complete loss of functionality.
- When deploying wireless IP devices and software-based clients, it is imperative to conduct a WLAN radio frequency (RF) site survey before, during, and after the deployment to determine appropriate cell boundaries, configuration and feature settings, capacity, and redundancy to ensure a successful voice over WLAN (VoWLAN) deployment.
- APs should be deployed with a minimum cell overlap of 20%. This overlap ensures that a dual-mode device can successfully roam from one AP to the next as the device moves around within a location, while still maintaining voice and data network connectivity.
- APs should be deployed with cell power level boundaries (or channel cell radius) of -67 dBm in order to minimize packet loss. Furthermore, the same-channel cell boundary separation should be approximately 19 dBm. A same-channel cell separation of 19 dBm is critical for ensuring that APs or clients do not cause co-channel interference to other devices associated to the same channel, which would likely result in poor voice quality.
- Deploy EM services in a highly redundant manner so that the loss of a single Unified CM node does not have adverse effects on the feature operation. If EM services are critical, consider deploying a server load balancing solution to route around Unified CM node failures and provide highly available functionality. For more information on EM high availability, see High Availability for Extension Mobility, page 19-14.
- Provide sufficient wireless voice call capacity on the campus network by deploying the appropriate number of wireless APs to handle the desired call capacity based on wireless user BHCA rates. Each 802.11g (2.4 GHz) or 802.11a (5 GHz) channel cell can support a maximum of 27 simultaneous bidirectional streams or calls with 24 Mbps or higher data rates. For 802.11g deployments, Bluetooth must be disabled to achieve this capacity.
- A maximum of 375 sequential EM logins and logouts per minute can be supported across a single Unified CM cluster. A maximum of two Unified CM subscriber nodes can actively handle EM logins. For more information on EM capacity, see Capacity Planning for Extension Mobility, page 19-16.

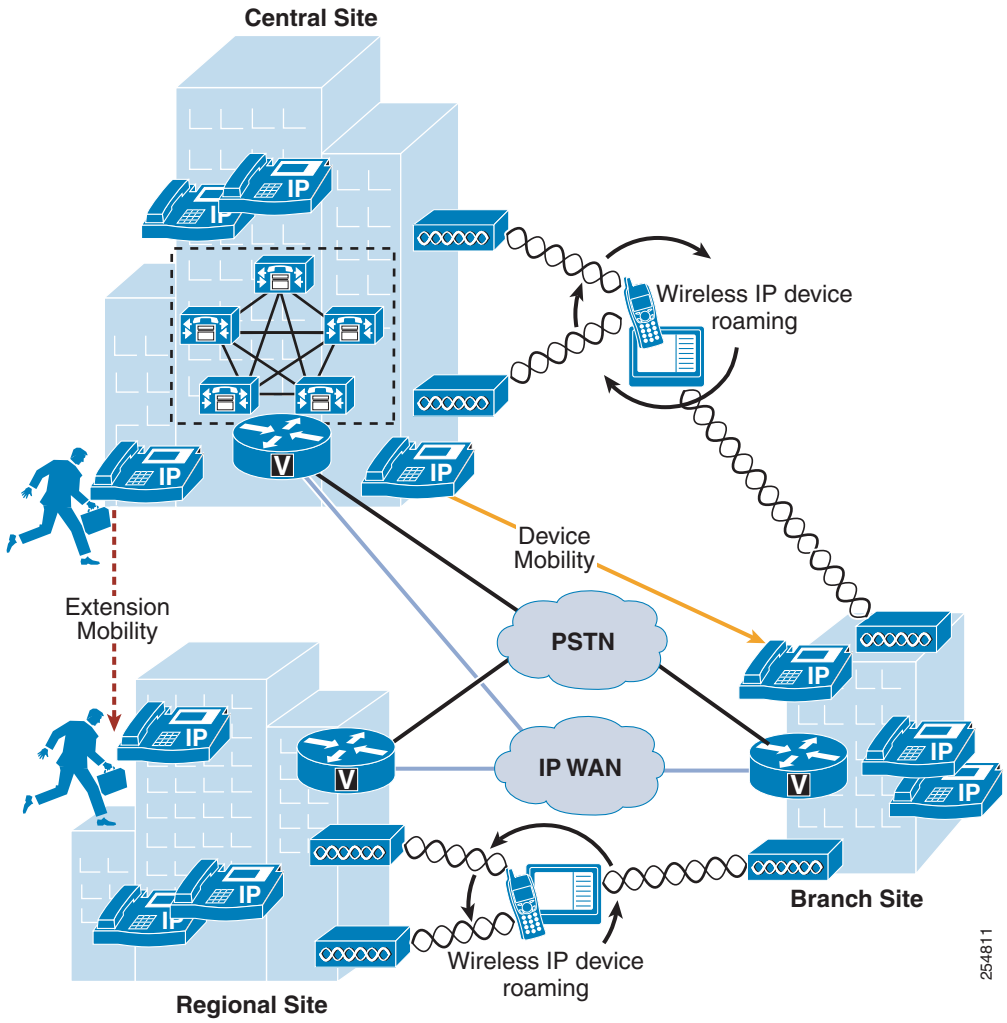
Multisite Enterprise Mobility

Multisite enterprise mobility refers to mobility within an enterprise with multiple physical locations, each with a unique IP address space and PSTN egress/ingress boundary. Mobility in this case includes not only the movement of users and endpoint devices within each physical location but also movement of users and endpoint devices between sites and locations.

Multisite Enterprise Mobility Architecture

As shown in Figure 25-4, the multisite enterprise mobility architecture is based on two or more locations or sites geographically separated. Sites may vary in size from large numbers of users and devices in a central or campus site to smaller numbers of users and devices in medium-sized regional sites or smaller branch sites. Typically multisite enterprise deployments consist of IP WAN links interconnecting sites as well as local PSTN egress/ingress at each location. In addition, critical services are often replicated at each physical site in order to maintain features and functions during network outages between sites. From a mobility perspective, users and their devices may be mobile within a site or between sites.

Figure 25-4 Multisite Enterprise Mobility Architecture



Note While Figure 25-4 depicts a multisite deployment with centralized call processing (as evidenced by a single Unified CM cluster within the central site), the same design and deployment considerations for multisite enterprise mobility deployments apply to distributed call processing environments. Differences in mobility feature operation when deployed in distributed call processing environments are described in the following discussions.

Types of Multisite Enterprise Mobility

Mobility within a multisite enterprise deployment involves not only the movement of devices, users, or both within a single site, but also movement of users and devices between sites.

The same types of mobility features and solutions supported with campus or single site enterprise deployments apply to intra-site movement of users and devices within any single site of a multisite deployment. These include physical wired phone movement, wireless phone roaming, and extension mobility. For information on these types of mobility solutions and functions, see Campus Enterprise Mobility, page 25-5.

For inter-site mobility in a multisite deployment, these same mobility features are also supported in much the same way. However, the key difference with these features when applied between two or more sites is that they are augmented with the Device Mobility feature. The Device Mobility feature provides a mechanism for dynamic location awareness of devices based on the IP address the device uses when connecting to the enterprise network.

Physical Wired Device Moves

Movement of physical wired phones is easily accommodated within each site of a multisite deployment as well as between sites. Just as with a campus or single-site deployment, wired device movement limited to a single site of a multisite deployment simply involves unplugging a Cisco Unified IP Phone from the network, moving it to another location within the site, and plugging it into another wired network port. Once connected to the new network location, the phone simply re-registers to Unified CM and is able to make and receive calls just like in the previous location.

Movement of wired devices between sites or locations in a multisite deployment involve the same basic behavior. However, the Device Mobility feature, when combined with this type of mobility, ensures that call admission control operations and gateway and codec selection are appropriate once the device re-registers in the new location to which it has been moved. See Device Mobility, page 25-16, for information about this feature.

Wireless Device Roaming

Just as with a single-site campus deployment, wireless devices can move or roam throughout a multisite enterprise deployment, as shown in Figure 25-4, provided wireless LAN network infrastructure is available at each site to provide wireless network connectivity. However, as with the movement of wired phones between sites, the Device Mobility feature should also be deployed for wireless devices to ensure that the correct gateway and codec are used when making and receiving calls and that call admission control manages bandwidth appropriately. See Device Mobility, page 25-16, for information about this feature.

For distributed call processing environments, just as with wired phones, wireless devices should be configured to register with only a single Unified CM cluster to avoid potential issues with call routing.

Extension Mobility (EM)

In addition to supporting EM within a single site, as illustrated in Figure 25-4, this feature is also supported between sites to enable users to move between sites within the enterprise and log on to phones in each locations.

EM is also supported in distributed call processing deployments when users move between sites and phones on different Unified CM clusters. To support extension mobility in distributed call processing environments, you might need to configure the Cisco Extension Mobility Cross Cluster (EMCC) feature. For information about this feature, see Extension Mobility Cross Cluster (EMCC), page 19-9.

Device Mobility

In Cisco Unified Communications Manager (Unified CM), a site or a physical location is identified using various settings such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones residing in a particular site are statically configured with these settings. Unified CM uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when dual-mode phones and other mobile client devices such as Cisco IP Communicator, Cisco Cius, or Cisco Unified Wireless IP Phones are moved from their home site to a remote site, they retain the home settings that are statically configured on the phones. Unified CM then uses these home settings on the phones in the remote site. This situation is undesirable because it can cause problems with call routing, codec selection, media resource selection, and other call processing functions.

Cisco Unified CM uses a feature called Device Mobility, which enables Unified CM to determine if the IP phone is at its home location or at a roaming location. Unified CM uses the device's IP subnets to determine the exact location of the IP phone. By enabling device mobility within a cluster, mobile users can roam from one site to another, thus acquiring the site-specific settings. Unified CM then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

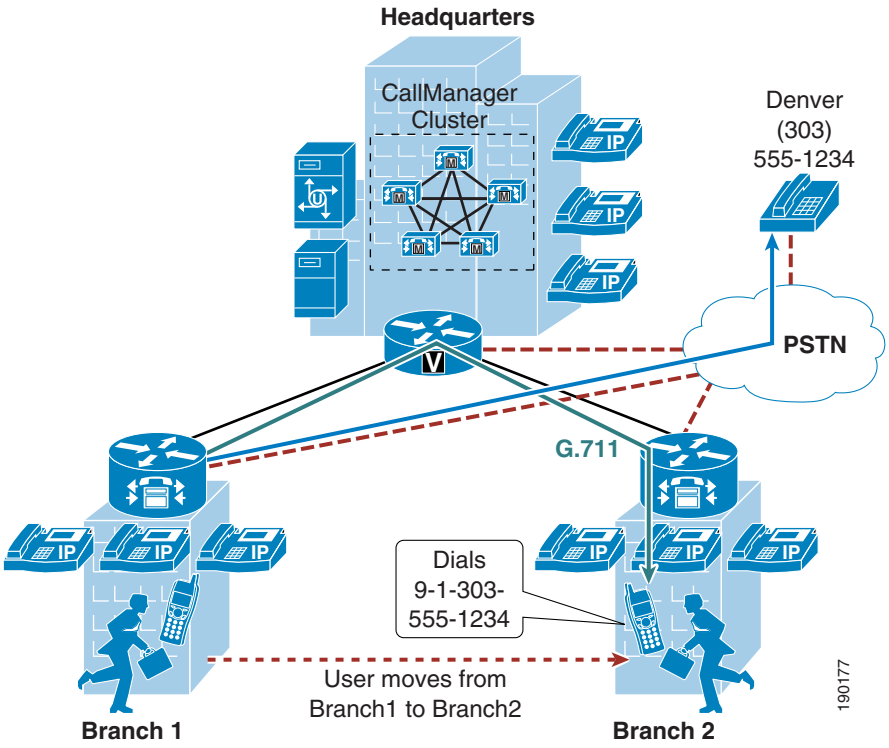
This section begins with a discussion surrounding the main purpose for the Device Mobility feature, followed by an in-depth discussion of the Device Mobility feature itself. This discussion covers the various components and configuration constructs of the Device Mobility feature. This section also presents an in-depth discussion of the impact of the Device Mobility feature on the enterprise dial plan, including the implication for various dial plan models.

Need for Device Mobility

This section explains the need for device mobility when there are many mobile users in a Unified CM cluster.

Figure 25-5 illustrates a hypothetical network containing a Unified CM cluster without the Device Mobility feature, located at the headquarter site (HQ). The cluster has two remote sites, Branch1 and Branch2. All intra-site calls use G.711 voice codecs, while all inter-site calls (calls across the IP WAN) use G.729 voice codecs. Each site has a PSTN gateway for external calls.

Figure 25-5 Example Network with Two Remote Sites



When a user in Branch1 moves to Branch2 and calls a PSTN user in Denver, the following behavior occurs:

- Unified CM is not aware that the user has moved from Branch1 to Branch2. An external call to the PSTN is sent over the WAN to the Branch1 gateway and then out to the PSTN. Thus, the mobile user continues to use its home gateway for all PSTN calls.
- The mobile user and Branch1 gateway are in the same Unified CM region and location. Location-based call admission control is applicable only for devices in different locations, and an intra-region call uses the G.711 voice codec. Thus, the call over the IP WAN to the Branch1 gateway uses the G.711 codec and is not tracked by Unified CM for purposes of call admission control. This behavior can result in over-subscription of the IP WAN bandwidth if all the remote links are low-speed links.
- The mobile user creates a conference by adding multiple Branch2 users to the existing call with the PSTN user in Denver. The mobile user uses the conferencing resource that is on the Branch1 gateway, therefore all conference streams flow over the IP WAN.

Note Device Mobility is an intra-cluster feature and does not span multiple Unified CM clusters. In distributed call processing environments, Device Mobility must be enabled and configured on each Unified CM cluster within the deployment.

Device Mobility Architecture

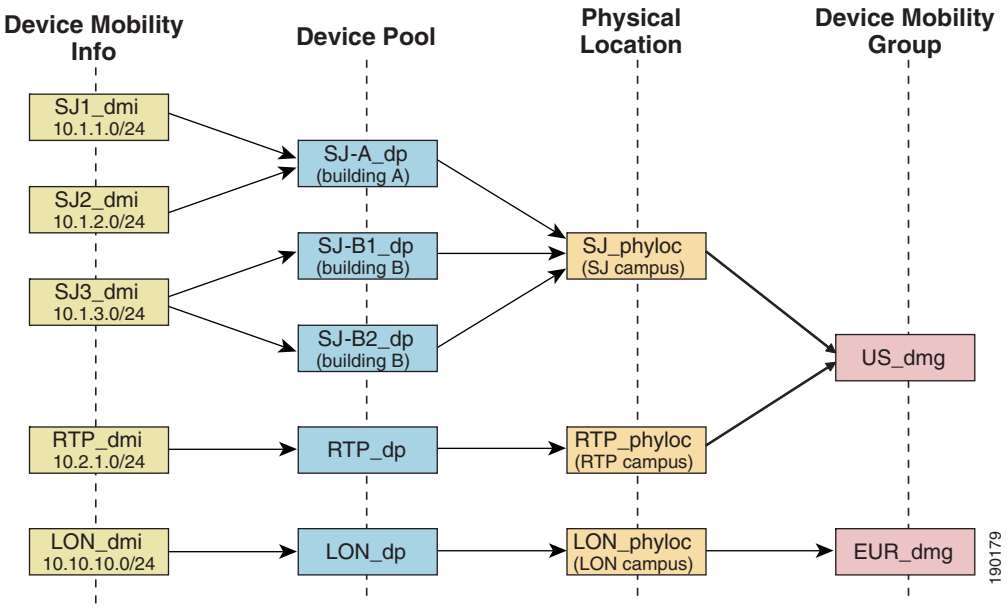
The Unified CM Device Mobility feature helps solve the problems mentioned above. This section briefly explains how the feature works. However, for a detailed explanation of this feature, refer to the product documentation available on http://www.cisco.com.

Some of the device mobility elements include:

- Device Mobility Info — Configures IP subnets and associates device pools to the IP subnets.
- Device Mobility Group — Defines a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg in Figure 25-6).
- Physical Location — Defines the physical location of a device pool. In other words, this element defines the geographic location of IP phones and other devices associated with the device pool. (For example, all San Jose IP phones in Figure 25-6 are defined by physical location SJ_phyloc.)

Figure 25-6 illustrates the relationship between all these terms.

Figure 25-6 Relationship of Device Mobility Components

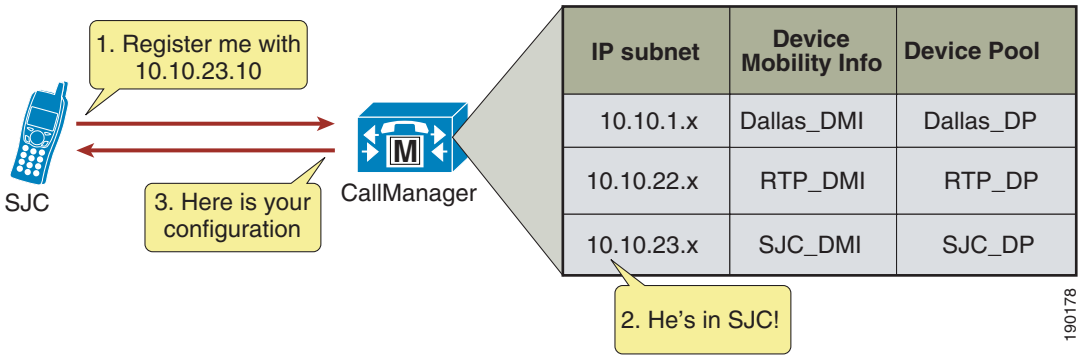


Unified CM assigns a device pool to an IP phone based on the device's IP subnet. The following steps, illustrated in Figure 25-7, describe the behavior:

1. The IP phone tries to register to Unified CM by sending its IP address in the Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) registration message.
2. Unified CM derives the device's IP subnet and matches it with the subnet configured in the Device Mobility Info.

3. If the subnet matches, Unified CM provides the device with a new configuration based on the device pool configuration.

Figure 25-7 Phone Registration Process



Unified CM uses a set of parameters under the device pool configuration to accommodate Device Mobility. These parameters are of the following two main types:

- Roaming Sensitive Settings, page 25-19
- Device Mobility Related Settings, page 25-20

Roaming Sensitive Settings

The parameters under these settings will override the device-level settings when the device is roaming within or outside a Device Mobility Group. The parameters included in these settings are:

- Date/time Group
- Region
- Media Resource Group List
- Location
- Network Locale
- SRST Reference
- Physical Location
- Device Mobility Group

The roaming sensitive settings primarily help in achieving proper call admission control and voice codec selection because the location and region configurations are used based on the device's roaming device pool.

For more details on various call admission control techniques, see the chapter on Call Admission Control, page 11-1.

The roaming sensitive settings also update the media resource group list (MRGL) so that appropriate remote media resources are used for music on hold, conferencing, transcoding, and so forth, thus utilizing the network efficiently.

The roaming sensitive settings also update the Survivable Remote Site Telephony (SRST) gateway. Mobile users register to a different SRST gateway while roaming. This registration can affect the dialing behavior when the roaming phones are in SRST mode.

For example, if a user moves with their phone to a new location that loses connectivity to Unified CM, then based on the roaming sensitive Device Mobility settings, a new SRST reference is configured for the moved phone and the moved phone will now be under control of the local roaming location SRST router. When this occurs, not only would the user's phone be unreachable from the PSTN or other sites because the device's DID will not have changed and will still be anchored at their home location, but in addition reachabililty from devices within the local failed site might be difficult without the use of abbreviated dialing as implemented within SRST.

As an example, assume that a user moves a phone from their home location in San Jose, which has a directory number of 51234 and an associated DID of 408 555 1234 to a remote location in New York, and that the link between the New York site and San Jose fails shortly after the user roams to the New York location. In this scenario the phones in the New York site will all fail-over to the SRST router in that site. The roaming/moved phone will also register to the New York SRST router because its SRST reference was updated based on the device mobility roaming sensitive settings. In this scenario, the local New York devices will register to the SRST router with five-digit extensions just as they do to Unified CM, and as a result the roaming phone still has a directory number of 51234. To reach the roaming phone from all other sites and from the PSTN, the number 408 555 1234 will be routed to the San Jose PSTN gateway to which this particular DID is anchored. Because the New York site is disconnected from the San Jose site, any such calls will be routed to the users' voicemail boxes since they will be unreachable at their desk phones. Likewise, calls internally within the local failed site will have to be dialed using five-digit abbreviated dialing or based on the configured digit prefixing as defined by the **dialplan-pattern** and **extension-length** commands within the SRST router. In either case, local callers will have to be understand the required dialing behavior for reaching the local roaming device by abbreviated dialing. In some cases this may be simply five-digit dialing or it may be that users have to dial a special digit prefix to reach the local roaming phone. The same logic applies to outbound dialing from the moved or roaming phone in New York because its dialing behavior might have to be altered in order to reach local extensions using abbreviated dialing. Outbound dialing to the PSTN from the local roaming device should remain the same, however.

Device Mobility Related Settings

The parameters under these settings will override the device-level settings only when the device is roaming within a Device Mobility Group. The parameters included in these settings are:

- Device Mobility Calling Search Space
- AAR Calling Search Space
- AAR Group
- Calling Party Transformation CSS

The device mobility related settings affect the dial plan because the calling search space dictates the patterns that can be dialed or the devices that can be reached.

Device Mobility Group

Device Mobility Group, as explained earlier, defines a logical group of sites with similar dialing patterns (for example, sites having the same PSTN access codes and so forth). With this guideline, all sites have similar dialing patterns in the site-specific calling search spaces. Sites having different dialing behavior are in a different Device Mobility Group. As illustrated in Figure 25-6, the San Jose and RTP sites' Device Mobility Info, Device Pools, and Physical Locations are different; however, all of these have been assigned to the same Device Mobility Group US_dmg because the required dialing patterns and PSTN access codes are the same between the two locations. On the other hand, the London site is assigned to a separate Device Mobility Group EUR_dmg due to the fact that the required dialing patterns and PSTN access codes there are different than those of the US sites. A user roaming within a Device

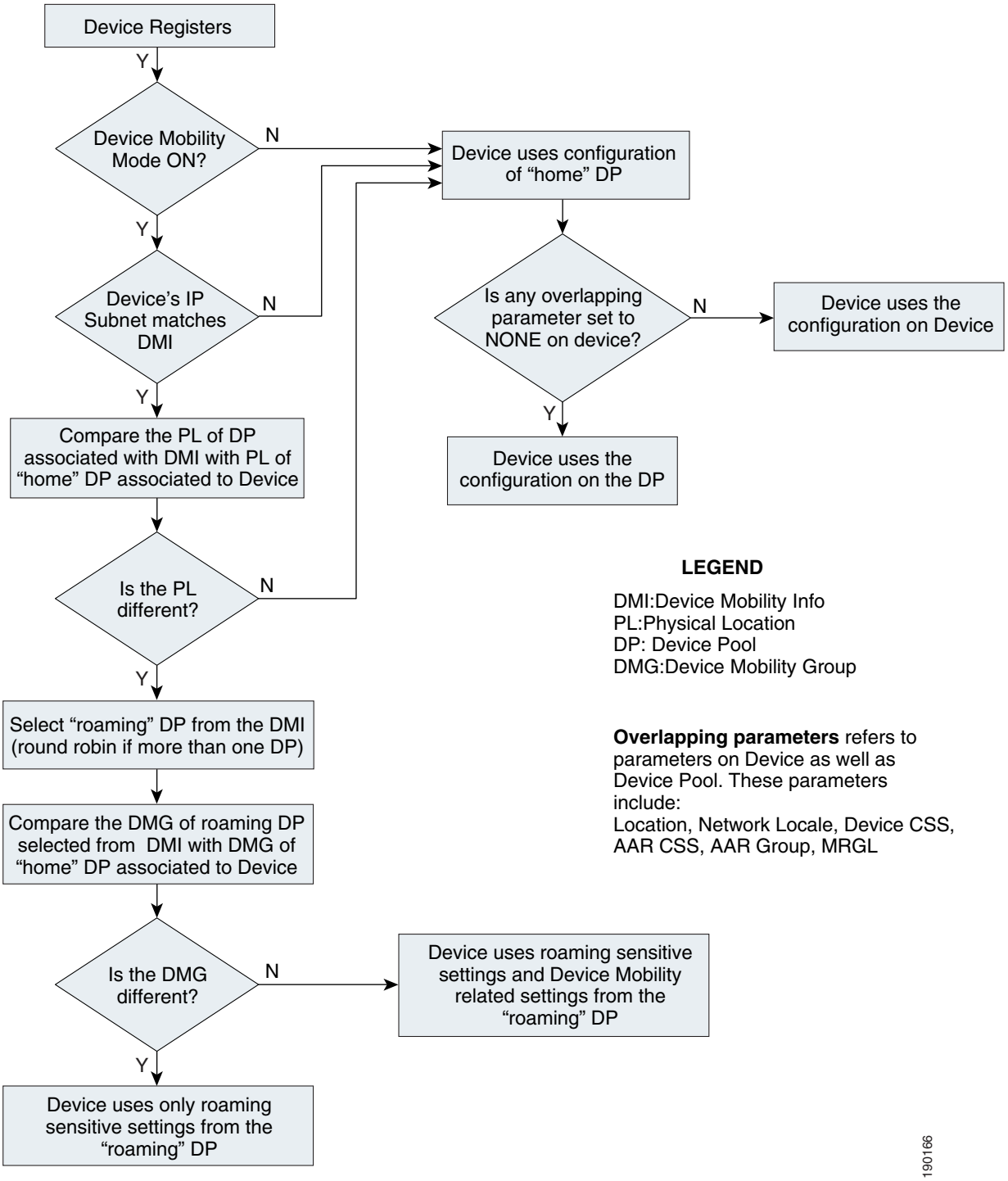
Mobility Group may preserve his dialing behavior at the remote location even after receiving a new calling search space. A user roaming outside the Device Mobility Group may still preserve his dialing behavior at the remote location because he uses his home calling search space.

However, if a Device Mobility Group is defined with sites having different dialing patterns (for example, one site requires users to dial 9 to get an outside line while another site requires users to dial 8 to get an outside line), then a user roaming within that Device Mobility Group might not preserve his same dialing behavior at all locations. A user might have to dial digits differently at different locations after receiving a new calling search space at each location. This behavior can be confusing for users, therefore Cisco recommends against assigning sites with different dialing patterns to the same Device Mobility Group.

Device Mobility Operation

The flowchart in Figure 25-8 represents the operation of the Device Mobility feature.

Figure 25-8 Operation of the Device Mobility Feature



The following guidelines apply to the Device Mobility feature:

- If the overlapping parameters listed in Figure 25-8 have the same configurations on the device as well as the device pool, then these parameters may be set to NONE on the device. These parameters must then be configured on the device pool. This practice can greatly reduce the amount of configuration because the devices do not have to be configured individually with all the parameters.
- Define one physical location per site. A site may have more than one device pool.
- Define sites with similar dialing patterns for PSTN or external/off-net access with the same Device Mobility Group.
- A "catch-all" Device Mobility Info with IP subnet 0.0.0.0 may be defined for all non-defined subnets, depending on the company policy. This Device Mobility Info may be used to assign a device pool that can restrict access or usage of the network resources. (For example, the device pool may be configured with a calling search space NONE that will block any calls from the device associated with this device pool while roaming.) However, by doing so, administrators must be aware of the fact that this will block all calls, even 911 or other emergency calls. The calling search space may be configured with partitions that will give access only to 911 or other emergency calls.

Dial Plan Design Considerations

When using the Device Mobility feature, the dialing behavior of the phone depends on the roaming (or home) location of a phone. As discussed earlier, the device mobility related settings within the device pool affect the call flow behavior because the calling search space dictates the reachability of destination patterns within Unified CM. This section discusses several dial plan approaches for Device Mobility.

For detailed explanations of various dial plan approaches, see the chapter on Dial Plan, page 9-1.

Device Mobility Considerations for Building Classes of Service

Typically, a mobile user should have the same calling privileges while he is roaming as he would have at his home location. The chapter on Dial Plan, page 9-1, discusses two approaches for building classes of service: Traditional Approach, page 25-23, and Line/Device Approach, page 25-23.

Traditional Approach

With the traditional approach, both path selection and class of service are determined by the device-level calling search space. With the line/device approach, path selection is determined by the device-level calling search space and class of service is determined by the line-level calling search space. For all deployments, the line/device approach is recommended for building classes of service. In particular with deployments utilizing Device Mobility, it is important to use the line/device approach because this approach ensures that all calls made by a mobile device will use the roaming site or local gateway rather than the home site gateway. While the traditional approach can certainly be used, this chapter covers only the recommended line/device approach. For a general discussion of the traditional approach, see the chapter on Dial Plan, page 9-1.

Line/Device Approach

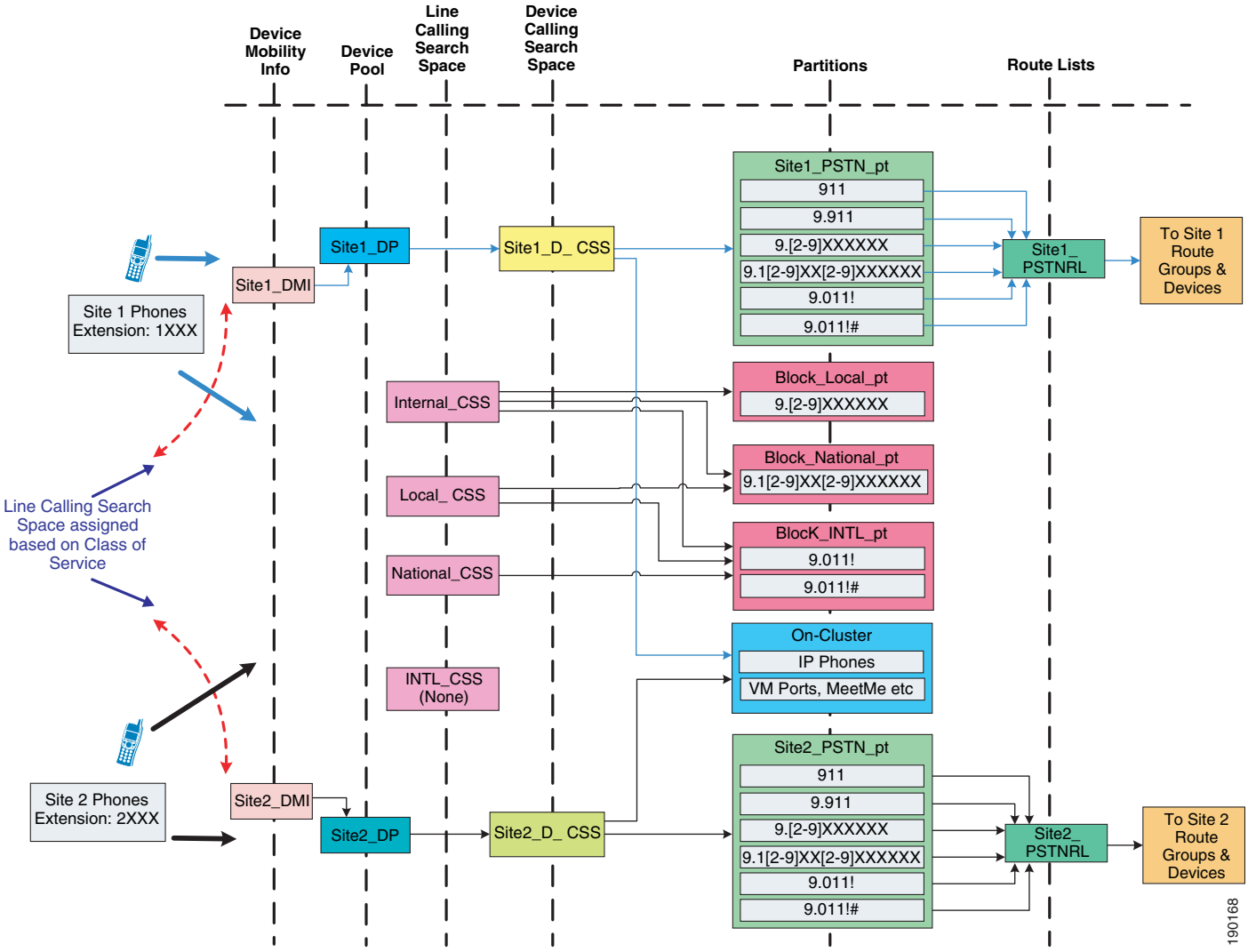
Unified CM concatenates the line and device calling search spaces for a given IP phone. The following key concepts apply to the line/device approach:

- The device calling search space provides call routing information.
- The line calling search space provides class-of-service information.

With the Device Mobility feature, the device calling search space is dynamically associated to the phone based on its location. The key concept of the line/device remains the same when using Device Mobility. The line calling search space provides the class-of-service information, while the roaming or home device calling search space that is selected provides the call routing information.

Figure 25-9 shows an example of building classes of service with the line/device approach when using Device Mobility in a cluster.

Figure 25-9 Line/Device Approach to Building Classes of Service



Cisco recommends using the line/device approach for building classes of service. This model has significant advantages when using Device Mobility because it greatly reduces the number of device pools needed, as indicated by the following formula:

Total device pools = (Number of sites)

The following design considerations apply to this approach:

- The calling search space on the phone device can be configured to NONE. The calling search space configuration on the device pool will be assigned to the phone device. This method can greatly reduce the amount of configuration because you do not have to configure the phones individually with a device calling search space.

- There is no restriction on having the same classes of service or calling privileges for all mobile users. Because the classes of service are defined using the line calling search space, a mobile user keeps the same class of service while roaming.
- A mobile user may have both Device Mobility and Extension Mobility enabled in his profile.

Choosing a Dial Plan Model

As discussed in the chapter on Dial Plan, page 9-1, there are three main approaches for the dial plan model:

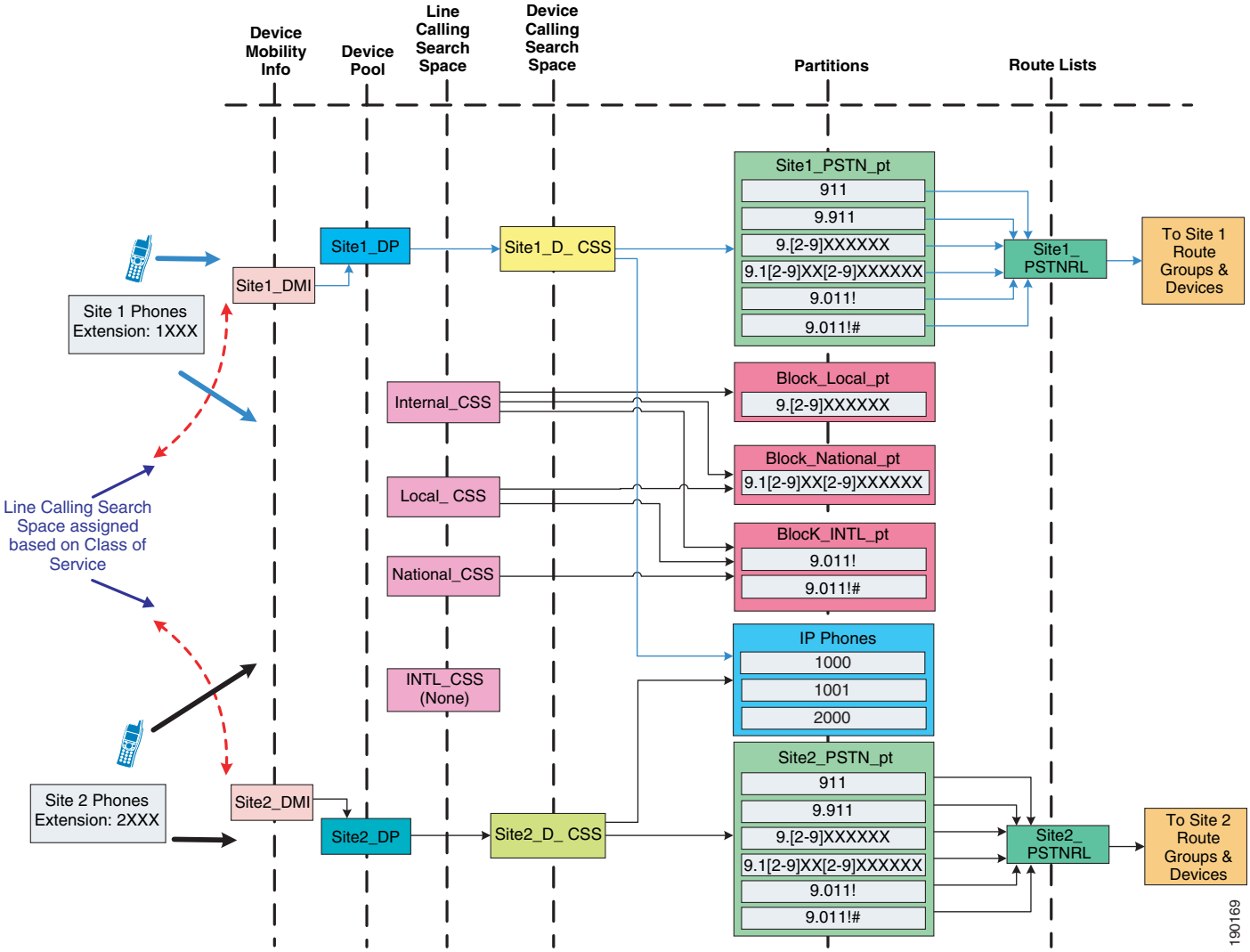
- Uniform on-net dialing
- Variable length on-net dialing with partitioned addressing
- Variable length on-net dialing with flat addressing

The following sections present various dial plan models combined with an approach for building classes of service.

Uniform On-Net Dialing Using the Line/Device Approach

Figure 25-10 shows a uniform on-net dial plan for Device Mobility.

Figure 25-10 Uniform On-Net Dial Plan for Device Mobility



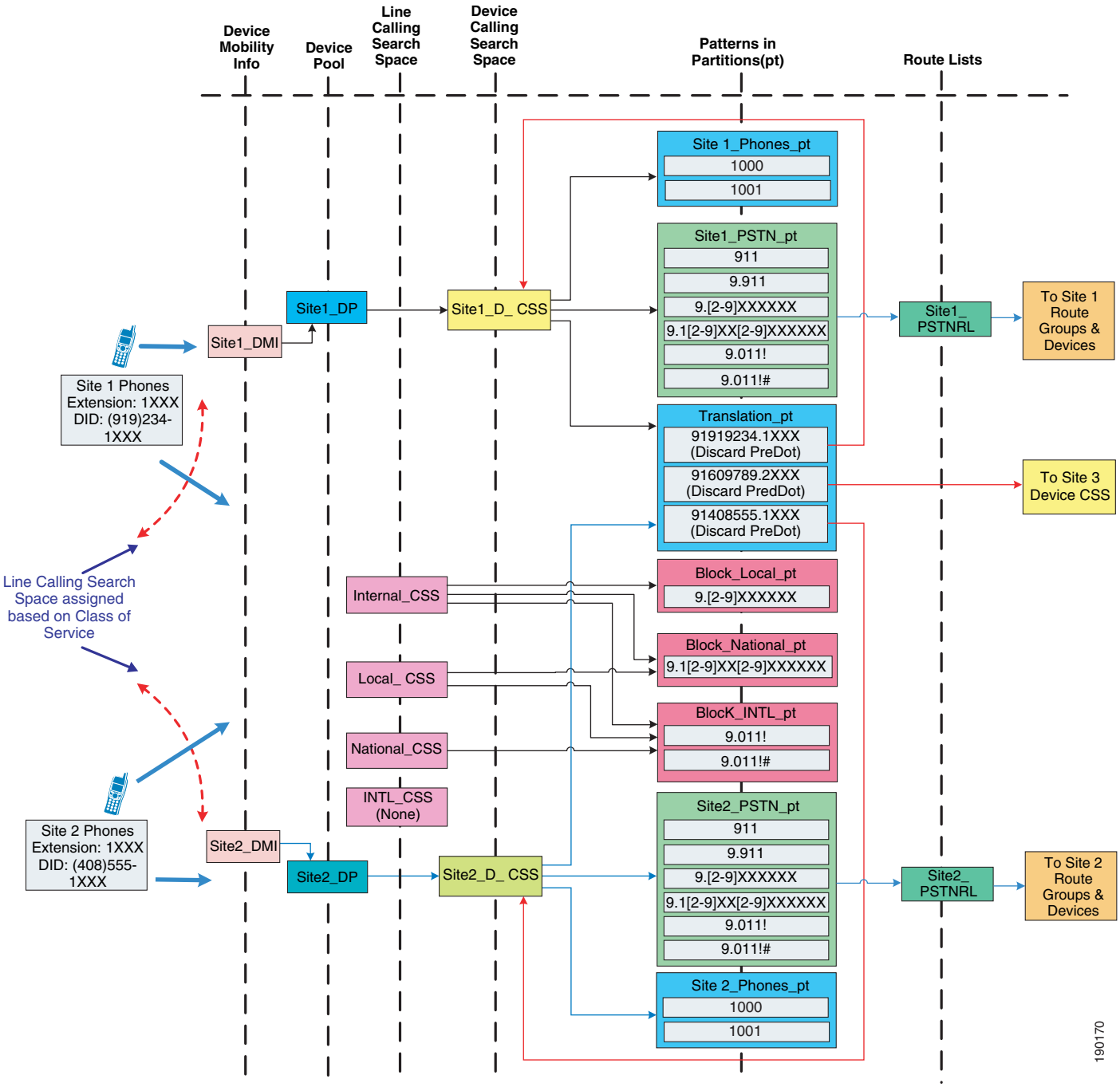
This is the most basic dial plan model, and it has the following characteristics:

- Mobile users can use abbreviated dialing (four digits for the example in Figure 25-10) from any location.
- Abbreviated speed dialing for internal extensions continues to work on the mobile user's phone in roaming locations.
- Mobile users use a "roaming" calling search space when they are at a remote location. Cisco recommends having the same access codes for PSTN calls at all sites. If the PSTN access codes are not the same, users must learn the different access codes.

Variable Length On-Net Dialing with Partitioned Addressing Using the Line/Device Approach

Figure 25-11 shows a variable-length on-net dial plan with partitioned addressing for Device Mobility.

Figure 25-11 Variable-Length On-Net Dial Plan with Partitioned Addressing for Device Mobility



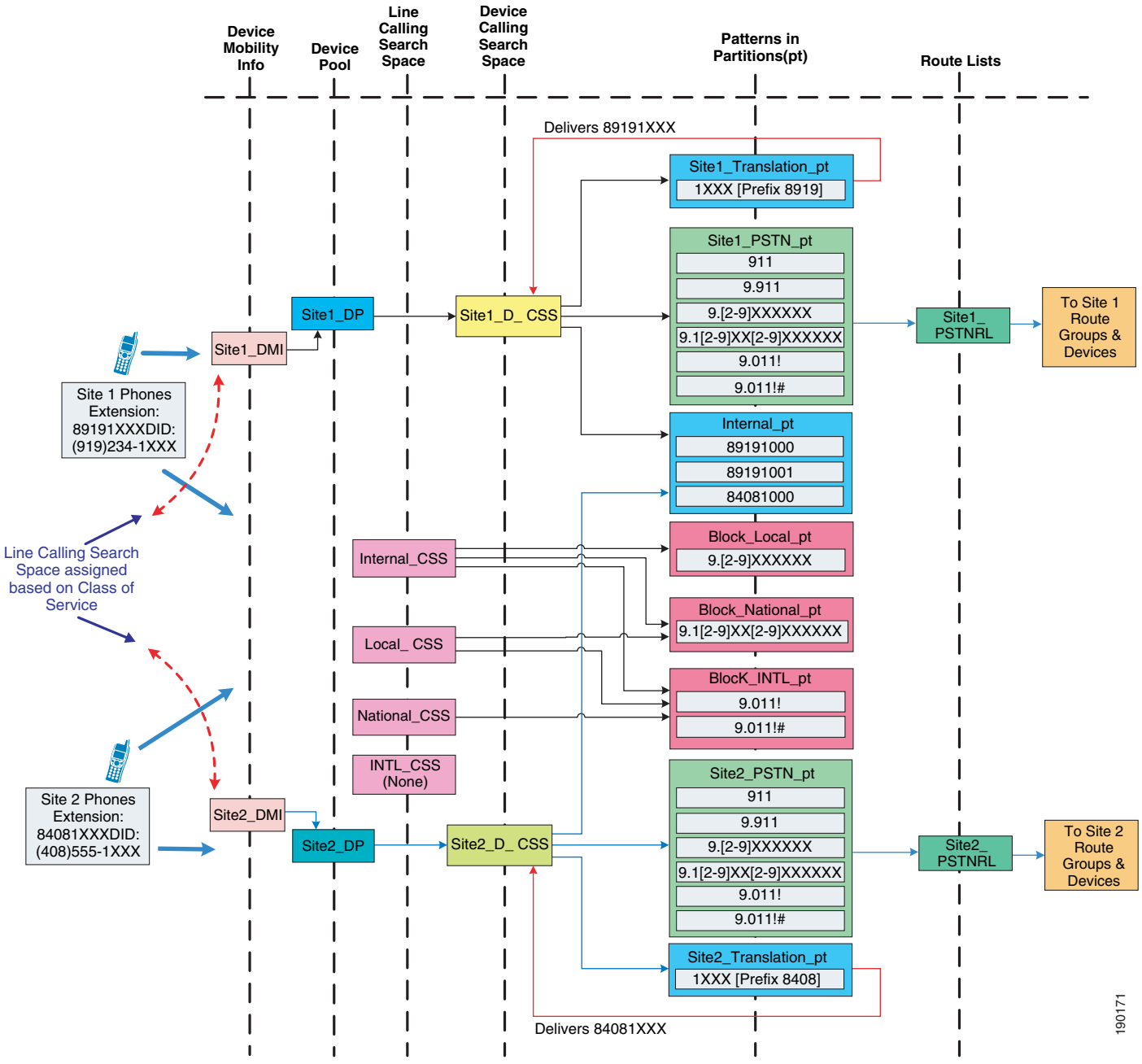
The following design considerations apply to the dial plan model in Figure 25-11:

- Calls might be routed to the wrong destination when mobile users use abbreviated dialing from a roaming location. For the example in Figure 25-11, assume that mobile user 1 in Site 1 with extension 1000 moves to Site 2. If user 1 dials 1001 with the intention of calling a person in Site 1, the call will be routed to extension 1001 in Site 2 instead. If this behavior is not desired, consider defining each site as a Device Mobility Group. As shown in Figure 25-8, when devices roam, if the Device Mobility Group of the "home" device pool is different from the Device Mobility Group defined by the "roaming" device pool of the Device Mobility Info, then only the roaming sensitive settings from the "roaming" device pool are applied. This means that the Device Mobility calling search space that is not a roaming sensitive setting will not be used, and instead the "home" calling search space (as defined at the device level setting or the device pool setting of the phone) would be used when the roaming phone makes a call. This means that for the example shown in Figure 25-11, when user 1 dials extension 1001 while in Site 2, the call will be routed using the "home" site calling search space, resulting in the call being routed to extension 1001 in Site 1. However, in this call scenario WAN bandwidth would be consumed. Further, for any external PSTN calls dialed by user 1 in this example, the roaming phone would also use the home gateway and also consume WAN bandwidth because the "home" site calling search space is used.
- Additional device calling search spaces may be configured for roaming users with access only to the PSTN and translation partitions. This configuration will need at least one additional device pool and calling search space per site. Thus, *N* sites will need *N* device pools and *N* calling search spaces. However, this configuration will not require defining each site as a Device Mobility Group.
- Abbreviated speed dials should not be used. Cisco recommends configuring speed dials in a universal way that enables the users to use speed dials at any location. For example, users may configure speed dials using E.164 numbers or using site codes and access codes.
- Overlapping extensions at multiple sites might cause problems when a roaming user registers to a remote SRST gateway. For the example in Figure 25-11, assume that mobile user A in Site 1 with extension 1000 moves to Site 2. Also assume that the WAN link at Site 2 goes down, causing the phones to register to an SRST gateway at Site 2. An incoming call on the SRST gateway for extension 1000 will be routed to actual extension 1000 in Site 2 as well as to the mobile user with extension 1000. Thus, calls might not be routed properly. This issue can be avoided by using unique extensions throughout the network.

Variable Length On-Net Dialing with Flat Addressing Using the Line/Device Approach

Figure 25-12 shows a variable-length on-net dial plan with flat addressing for Device Mobility.

Figure 25-12 Variable-Length On-Net Dial Plan with Flat Addressing for Device Mobility



The following design considerations apply to the dial plan model in Figure 25-12:

- Mobile users cannot use abbreviated dialing after roaming to another site because calls might be routed to the wrong destination. If this behavior is not desired, consider defining each site as a Device Mobility Group. However, users must be aware that, for any external PSTN calls, the mobile phone continues to use the home gateway and therefore consumes WAN bandwidth.
- Additional device calling search spaces may be configured for roaming users with access only to the PSTN and internal phones partitions. This configuration will need at least one additional device pool and calling search space per site. Thus, *N* sites will need *N* device pools and *N* calling search spaces. However, this configuration will not require defining each site as a Device Mobility Group.
- Mobile users registered with a remote SRST gateway have unique extensions. However, mobile users must be aware that no PSTN user can call them when they are registered to a remote SRST gateway.

Multisite Enterprise Mobility High Availability

Multisite enterprise mobility features and solutions should be configured and deployed in a redundant fashion in order to ensure high availability of mobility functionality. High availability considerations for wired phone moves, wireless roaming, and EM in multisite mobility deployments are similar to those for campus mobility deployments. Just as with campus environments, redundant network ports, wireless cell coverage, and Unified CM nodes handling extension mobility logins and logouts should be provided to ensure highly available services.

Similarly, it is important to consider high availability of the Device Mobility feature. Because Device Mobility is natively integrated within Unified CM, the failure of a cluster node should have no impact on the functionality of Device Mobility. Device pool, Device Mobility Info, Device Mobility Group, and all other configurations surrounding Device Mobility are preserved if there is a failure of the publisher node or a call processing (subscriber) node. Additionally, if there is a call processing node failure, affected phones will fail-over to their secondary call processing node or SRST reference router as usual based on the Unified CM Group construct.

Capacity Planning for Multisite Enterprise Mobility

As for Device Mobility scalability considerations, there are no specific or enforced capacity limits surrounding this feature and the various configuration constructs (device pools, device mobility groups, and so forth). For more information on general system sizing, capacity planning, and deployment considerations, see the chapter on Unified Communications Design and Deployment Sizing Considerations, page 29-1.

Design Considerations for Multisite Enterprise Mobility

All campus enterprise mobility design considerations apply to multisite enterprise mobility deployments as well (seeDesign Considerations for Campus Enterprise Mobility, page 25-12). The following additional design recommendations apply specifically to multisite mobility environments:

- Ensure that all critical services (device registration, PSTN connectivity, DNS, DHCP, and so forth) are deployed at each site in a multisite deployment so that failure of the connection between the site and other sites does not disrupt critical operations. In addition, ensure that a sufficient number of physical network ports and wireless LAN APs are available at each site to support movement of devices and required call capacity.

- In situations in which sites with different dialing patterns (for example, sites having different PSTN access codes) are configured in the same Device Mobility Group, roaming users might have to dial numbers differently based on their location, which can be confusing. For this reason, Cisco recommends assigning sites with similar dialing patterns (for example, sites having the same PSTN access codes) to the same Device Mobility Group. Doing so ensures that roaming users can dial numbers the same way at all sites within the Device Mobility Group.
- The Device Mobility settings from the "roaming" device pool are applied only when users roam within the same Device Mobility Group; therefore, avoid roaming between different Device Mobility Groups because the resulting call routing behavior will cause originated calls from the moved phone to be routed using the "home" or device-configured calling search space. This can lead to unnecessary consumption of WAN bandwidth because the call might be routed through a different site's gateway rather than the local "roaming" gateway.
- Define only one physical location per site. This ensures that device mobility is engaged only in scenarios in which a user is roaming between sites. For roaming within the same site, the concerns that mandate Device Mobility (for example, WAN bandwidth consumption, codec selection, and call admission control) are not present because low-speed links typically are not deployed within a single site.
- In failover scenarios, "roaming" phones will utilize the SRST reference/gateway as dictated by the "roaming" device pool's roaming sensitive settings. Therefore, in these situations the "roaming" phone is unreachable from the PSTN due to the fact that the DID for this phone is anchored in another location's PSTN gateway. Furthermore, for outbound calls from the "roaming" phone, dialing behavior might have to be altered for things such as PSTN access codes, and speed dials configured on the phone might not be usable.
- While the general recommendation is to always use the line/device approach to the dial plan, it is especially important when deploying Device Mobility because it allows different classes of service or calling privileges for each mobile user. With the line/device approach, the classes of service are defined using the line calling search space of the device, which stays the same when roaming and allows a mobile user to keep the same class of service while roaming.
- If your system requires the ability to use abbreviated dialing or to use speed dials that rely on abbreviated dialing, Cisco recommends using the Uniform On-net dial plan model because it will ensure that abbreviated dialing (direct or through speed dials) continues to work even when the mobile user's phone is in a roaming location. Abbreviated dialing is still possible with this dial plan model because all extensions or directory numbers are unique across all sites, and therefore abbreviated dialing can be used universally due to the fact that there are no overlapping extensions.
- If your system uses a Variable Length On-net dial plan model (with either partitioned addressing or flat addressing), Cisco recommends configuring speed dials in a universal way so that a single unique extension can be reached when called. By configuring speed dials using full E.164 numbers or using site or access codes, you can enable roaming users to use the same speed dials at any location.
- If Device Mobility is enabled for users who on occasion access the enterprise network through a VPN connection, Device Mobility Info (DMI) for VPN attached phones should contain IP subnets distributed or owned by the VPN concentrators to ensure that "roaming" to a VPN location results in appropriate dynamic Device Mobility configuration changes. Be sure to associate the DMI with the same device pool that is used for any devices co-located with the VPN concentrators.

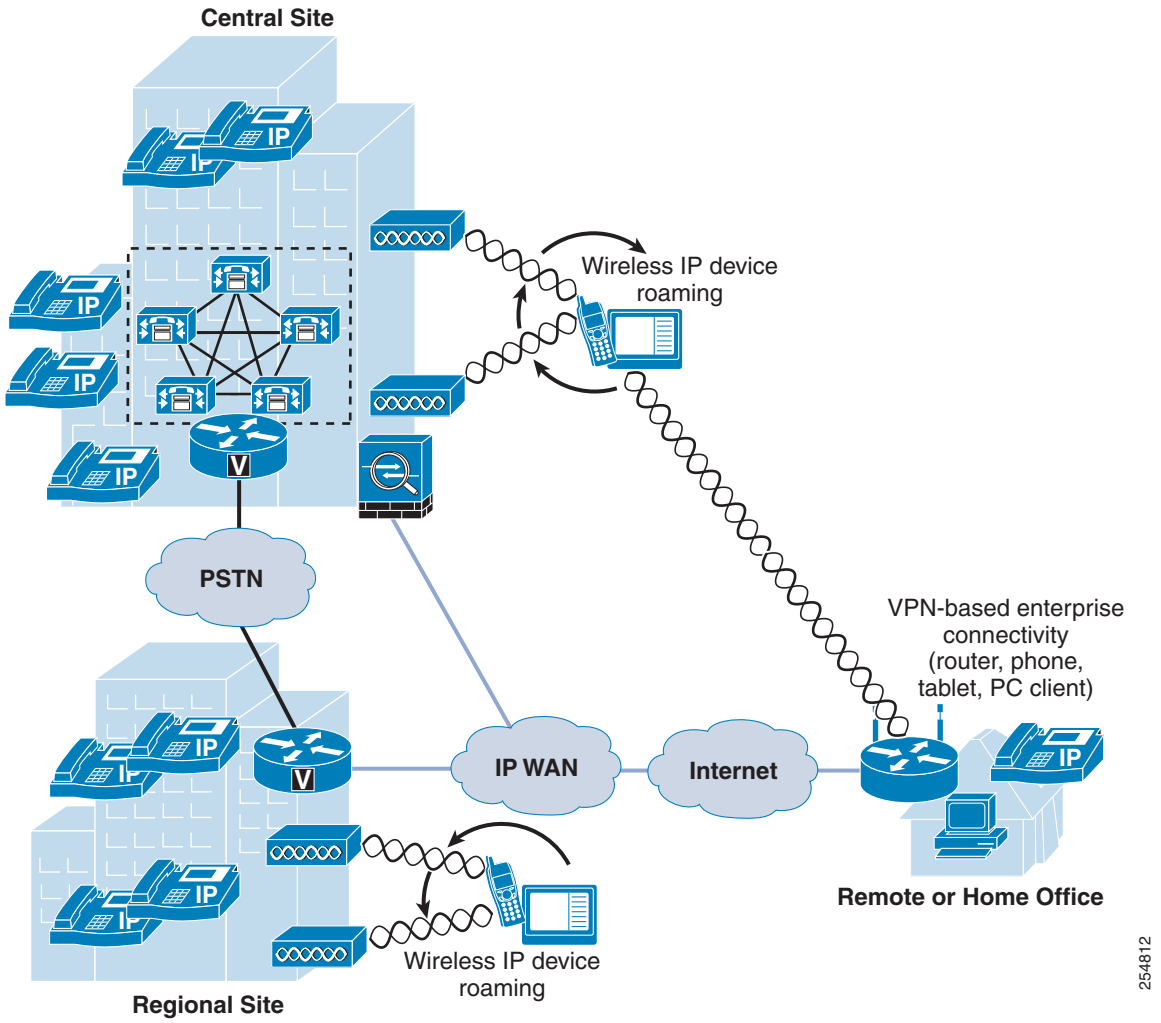
Remote Enterprise Mobility

Remote enterprise mobility refers to mobile users in locations remote from the enterprise but still attached to the enterprise network infrastructure through secure connections over the public Internet. Mobility here deals with the placement of endpoint devices in these remote locations and the movement of users, and in some cases their mobile devices, between the enterprise and these locations either frequently or on occasion.

Remote Enterprise Mobility Architecture

As illustrated in Figure 25-13, the remote enterprise mobility architecture is based on a remote physical location, typically an employee home office but also any remote location capable of secure connection back to the enterprise over the Internet. These remote sites typically consist of an IP network with connections for a user's computer, telephone, and other equipment or endpoints. In some cases this IP network may be behind an enterprise controlled and configured VPN router that provides a secure tunnel between the remote location and the enterprise network. In other cases, the remote site IP network is connected to the Internet through a user-provided router, and user computer or endpoint devices must use software-based VPN client capabilities to create secure connections back to the enterprise network. Wireless connectivity may also be provided in the remote location to allow wireless attachment of the user's computer or endpoint. When wireless connectivity is provided at the remote location, wireless phones may be moved from the enterprise network to the home office, allowing users to leverage wireless enterprise devices or mobile phones within the remote location to make and receive calls.

Figure 25-13 Remote Enterprise Mobility Architecture



Types of Remote Enterprise Mobility

Remote enterprise mobility deployments focus predominately on supporting remote users as opposed to supporting regular user or device movement. Certainly users may regularly move with or without an endpoint device between the enterprise location or locations and the remote site; however, the predominate purpose of these deployments is to support remote connectivity for enterprise users. Remote site mobility typically involves two main types of remote connectivity: router-based secure connectivity and client-based secure connectivity. Both types support remote site secure connectivity and both can accommodate various endpoint devices that can be moved between the remote site and the enterprise, including dual-mode mobile phones, wireless IP phones and tablets, and even wired IP phones.

Client-Based Secure Remote Connectivity

Wireless and wired IP phones and software-based PC telephony clients can be connected to remote site locations, as shown in Figure 25-13. These devices and endpoints are responsible for creating secure VPN connections back to the enterprise VPN head-end termination concentrator.

Examples of these types of devices include wirelessly attached dual-mode phones and clients using VPN client or application capabilities such as the Cisco Jabber for iPhone and Android clients (see Dual-Mode Phones and Clients, page 25-66), Cisco Mobile 8.5 Nokia client (see Direct Connect Mobile Clients, page 25-102), wired Cisco Unified IP Phones such as the Cisco Unified IP Phone 7965 that uses a built-in VPN client, and personal computers running software-based telephony clients such as Cisco IP Communicator that uses a software-based VPN client for connectivity to the enterprise network.

Router-Based Secure Remote Connectivity

On the other hand, remote site connectivity can be handled through router-based secure VPN tunnels. In these types of scenarios the deployed remote site router, which may be able to provide wireless network connectivity as well, is responsible for setting up and securing a VPN tunnel back to the enterprise network. This in effect extends the enterprise network boundary to the remote site location. The advantage of this type of connectivity is that a wider range of devices and endpoints may be deployed in the remote site because these devices are not responsible for providing secure connectivity and therefore do not require special software or configuration. Instead, these devices simply connect to the remote site network and leverage the secure VPN IP path from the remote site router to the enterprise VPN head-end.

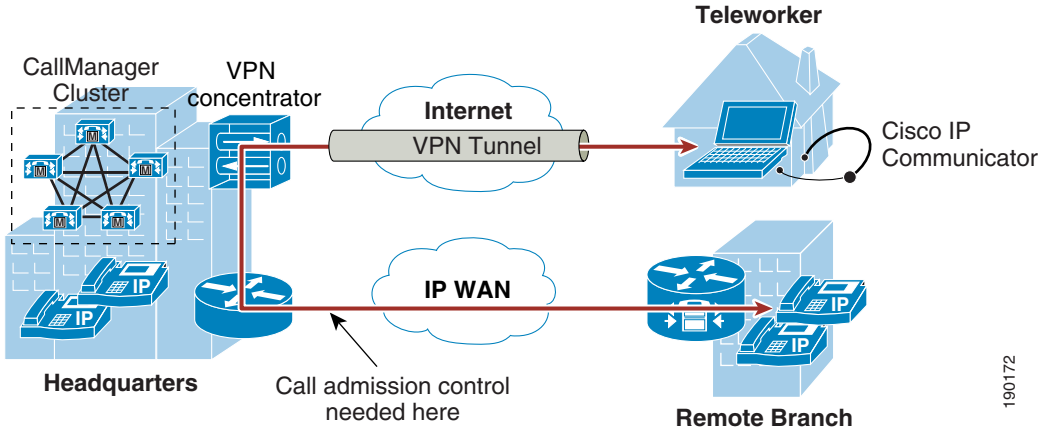
An example of this type of route-based remote site connectivity is the Cisco Virtual Office solution.

Device Mobility and VPN-Based Remote Enterprise Connectivity

Whether you are deploying client-based or router-based secure remote connectivity, the Device Mobility feature may be used to ensure that call admission control and codec are correctly negotiated for endpoint devices and that the appropriate enterprise site PSTN gateway and media resources are utilized. Based on the IP address of the endpoint device as received over the VPN connection, Unified CM will dynamically determine the location of the device.

Figure 25-14 shows an example of client-based secure remote connectivity where a Cisco IP Communicator software phone is running on a remote site computer. This software-based IP phone is connected through a client-based VPN back to the enterprise and registered to Unified CM.

Figure 25-14 Client-Based VPN Connection for Remote Site Cisco IP Communicator



The following design guidelines pertain to enabling the Device Mobility feature for user devices at a remote site connected to the enterprise through a VPN connection:

- Configure Device Mobility Info (DMI) with the IP subnets distributed or owned by the VPN concentrators.
- Associate the DMI with the same device pool that is used for devices co-located with the VPN concentrators. However, parameters such as calling privileges, network locale, and so forth, must be taken into consideration.
- Educate the remote site users to point to the geographically nearest enterprise VPN concentrator when making client-based or router-based VPN connections.

These guidelines ensure that call admission control is correctly applied on the enterprise WAN and over the connection to the remote site.

For information on deploying a VPN, refer to the various VPN design guides available under the *Security in WAN* subsection of the Design Zone for Security, available at:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_wan_security.html

Remote Enterprise Mobility High Availability

For remote site mobility environments, it is imperative that enterprise VPN services are configured and deployed in a redundant manner within the enterprise. This ensures that both client-based and router-based secure connections are highly available. If a VPN concentrator within the enterprise fails, a new secure connection can be set up with another VPN concentrator. Device registration and voice services are highly available in this type of deployment simply by virtue of the built-in Unified CM cluster node redundancy.

Capacity Planning for Remote Enterprise Mobility

The most critical scalability consideration for remote enterprise mobility environments is VPN concentrator capacity. Administrators must deploy sufficient VPN session capacity to accommodate all remote site connectivity, whether they are client-based or router-based secure tunnel connections. Failure to provide appropriate capacity will prevent some remote sites from connecting to the enterprise, thus eliminating access to even basic telephony services. Furthermore, just as with campus and multisite enterprise mobility deployments, it is important to provide sufficient device registration capacity within the enterprise to handle all remote user devices.

Design Considerations for Remote Enterprise Mobility

Consider the following design recommendations when enabling remote site connectivity for mobile users:

- When using Device Mobility, remember to configure Device Mobility Info (DMI) with the IP subnets distributed or owned by the VPN concentrators, and assign the DMI to the same device pool that is configured for devices deployed in the same location as the VPN concentrators.
- Educate remote site users to select the nearest VPN concentrator for VPN connection.
- Ensure appropriate VPN session capacity is available in order to provide connectivity to all remote site users.

Mobility Beyond the Enterprise

With Cisco's mobile Unified Communications, mobility users can handle calls to their enterprise directory number, not only on their desk phone, but also on one or more remote phones. Mobility users can also make calls from a remote phone as if they are dialing inside the enterprise. In addition, mobility users can take advantage of enterprise features such as hold, transfer, and conference as well as enterprise applications such as voicemail, conferencing, and presence on their mobile phones. This ensures continued productivity for users even when they are traveling outside the organization.

Further, with dual-mode phones that provide connectivity to mobile voice and data provider network as well as 802.11 WLAN, users not only have the ability to leverage enterprise applications while away from the enterprise, but they can also leverage the enterprise telephony infrastructure when inside the enterprise or remotely attached to the enterprise network to make and receive calls without incurring mobile voice network per-minute charges.

Mobility functionality delivered within the Cisco Unified Mobility solution is provided through Cisco Unified Communications Manager (Unified CM) and can be used in conjunction with the Cisco Unified Mobile Communicator application and dual-mode and direct-connect client devices.

Cisco Unified Mobility provides the following mobility application functionality:

- Mobile Connect

  Mobile Connect, also known as Single Number Reach, provides Cisco Unified Communications users with the ability to be reached at a single enterprise phone number that rings on both their IP desk phone and their mobile phone simultaneously. Mobile Connect users can pick up an incoming call on either their desk or mobile phones and at any point can move the in-progress call from one of these phones to the other without interruption.

- Mid-Call Features

  Mid-call features allow a user to invoke hold, resume, transfer, conferencing, and directed call park features from their mobile phone during in-progress mobility calls. These features are invoked from the mobile phone keypad and take advantage of enterprise media resources such as music on hold and conference bridges.

- Single Enterprise Voicemail Box

  Single Enterprise Voicemail box provides mobile voicemail avoidance capabilities and ensures that any unanswered calls made to the user's enterprise number and extended to the user's mobile phone will end up in the enterprise voicemail system rather than in a mobile voicemail system. This provides a single consolidated voicemail box for all business calls and eliminates the need for users to check multiple voicemail systems for messages.

- Mobile Voice Access and Enterprise Feature Access two-stage dialing

  Mobile Voice Access and Enterprise Feature Access two-stage dialing provide mobile users with the ability to make calls from their mobile phone as if they were calling from their enterprise IP desk phone. These features provide a cost savings in terms of toll charges for long distance or international calls as well as calls to internal non-DID extensions on the system that would not normally be reachable from outside the enterprise. These two-stage dialing features also provide the enterprise with an easy way to track phone calls made by users via a uniform and centrally located set of call detail records. Furthermore, these features provide the ability to mask a user's mobile phone number when sending outbound caller ID. Instead, the user's enterprise number is sent as caller ID. This ensures that returned calls to the user are made to the enterprise number, thus resulting in enterprise call anchoring.

Dual-mode phones and clients provide the ability to attach to both the mobile voice and data networks as well as to enterprise wireless networks for voice and data connectivity. This enables users to leverage both enterprise call control and mobile network call control from a single device. By leveraging the enterprise telephony infrastructure for making and receiving calls whenever possible and falling back to the mobile voice network only when enterprise connectivity is unavailable, dual-mode phones can help reduce telephony costs. Dual-mode phones and the clients that run on them also provide a handoff mechanism so that in-progress voice calls can be moved easily between the WLAN and mobile voice interfaces as a user moves in or out of the enterprise.

The Cisco Unified Mobile Communicator application includes a mobile client that provides enterprise Unified Communications features on a user's mobile phone through the use of a back-hauled data channel. The data channel is sent by means of the service provider data service over the Internet and is terminated at the Cisco Adaptive Security Appliance (ASA) and forwarded on to the Unified Mobility Advantage server, which interfaces with various applications and components within the enterprise Unified Communications infrastructure. The PSTN and mobile voice network are utilized for voice services.

Enterprise applications and features that can be integrated with the Cisco Unified Mobile Communicator application include:

- LDAP directory with Microsoft Active Directory for user authentication and directory lookups
- Voicemail with Cisco Unity or Unity Connection for message waiting indication and visual navigation of the user's enterprise voicemail box
- Conferencing and collaboration with Cisco Unified MeetingPlace for receiving conference notifications
- Presence integration with Cisco Unified Presence, allowing exchange of presence information and synchronization of buddy lists with other clients and applications such as Cisco Unified Personal Communicator

- Enterprise call log and dial-via-office with Cisco Unified Communications Manager (Unified CM) for receiving call history logs from the user's desk phone and for providing the ability to dial calls via the enterprise IP telephony infrastructure.
- Messaging for sending and receiving text messages with other Cisco Unified Mobile Communicator clients

In addition to providing the ability to integrate with various enterprise unified communication applications, Cisco Unified Mobile Communicator mobile client can be integrated with Unified Mobility to take advantage of these features including Mobile Connect and Single Enterprise Voicemail Box.

Direct connect mobile clients enable mobile phones to connect remotely to the enterprise network through the mobile data network or to connect locally through the enterprise WLAN in order to leverage voice features such as dial-via-office and voice over WLAN as well as other unified communications services such as corporate directories access, presence and instant messaging (IM). By providing similar features to Cisco Unified Mobile Communicator (dial-via-office, corporate directory access, presence, and so forth) and voice WLAN capabilities such as dual-mode phones and clients, these direct connect clients enable mobile users to remain productive whether inside or outside the enterprise by providing access to collaboration applications while at the same time enabling users to make and receive enterprise calls from their mobile devices, whether outside the enterprise over public or private Wi-Fi hot spots or the mobile data network, or inside the enterprise and over the WLAN network.

This section begins with a discussion of Unified Mobility features, functionality, and design and deployment considerations. Given the various benefits of Unified Mobility and the fact that dual-mode phones and clients can be integrated to take advantage of the features provided, this discussion paves the way for examination of dual-mode client applications such as Cisco Jabber. Following the dual-mode mobile phone client discussion, Cisco Unified Mobile Communicator is explained and direct connect mobile clients are examined. This section includes a discussion of architecture, functionality, and design and deployment implications for the following mobility applications and features:

- Cisco Unified Mobility, page 25-38
- Dual-Mode Phones and Clients, page 25-66
- Cisco Unified Mobile Communicator, page 25-87
- Direct Connect Mobile Clients, page 25-102

Cisco Unified Mobility

Cisco Unified Mobility refers to the native mobility functionality within the Cisco Unified Communications Manager (Unified CM) and includes the Mobile Connect, Mobile Voice Access, and Enterprise Feature Access features.

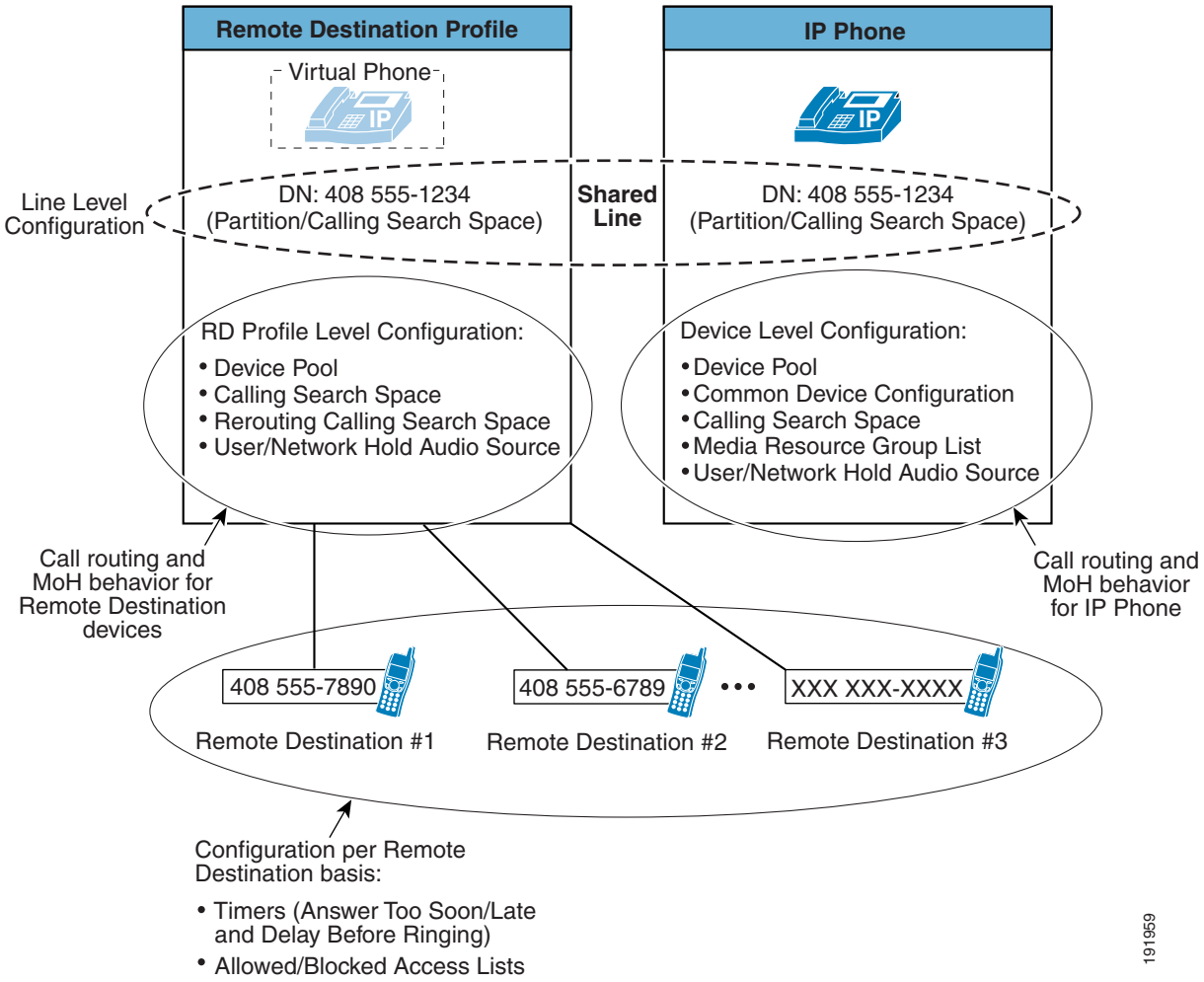
Unified Mobility functionality depends on the appropriate configuration of Unified CM. For this reason, it is important to understand the nature of this configuration as well as the logical components.

Figure 25-15 illustrates the configuration requirements for Unified Mobility. First, as for all users, a mobility user’s enterprise phone is configured with appropriate line-level settings such as directory number, partition, and calling search space. In addition, the device-level settings of the enterprise phone include parameters such as device pool, common device configuration, calling search space, media resource group list, and user and network hold audio sources. All of these line and device settings on the user’s enterprise phone affect the call routing and music on hold (MoH) behavior for incoming and outgoing calls.

Next, a remote destination profile must be configured for each mobility user in order for them to take advantage of Unified Mobility features. The remote destination profile is configured at the line level with the same directory number, partition, and calling search space as the user’s enterprise phone line. This

results in a shared line between the remote destination profile and the enterprise phone. The remote destination profile configuration includes device pool, calling search space, rerouting calling search space, and user and network hold audio source parameters. The remote destination profile should be thought of as a virtual phone whose configuration mirrors the user's line-level enterprise phone settings, but whose profile-level configuration combined with the line-level settings determines the call routing and MoH behavior that the user's remote destination phone will inherit. The user's enterprise directory number, which is shared between the remote destination profile and the enterprise phone, allows calls to that number to be extended to the user's remote destination.

Figure 25-15 Cisco Unified Mobility Configuration Architecture



As further shown in Figure 25-15, a mobility user can have one or more remote destinations configured and associated with their remote destination profile. A remote destination represents a single PSTN phone number where a user can be reached. A user can have up to 10 remote destinations defined. Call routing timers can be configured for each remote destination to adjust the amount of time a call will be extended to a particular remote phone, as well as the amount of time to wait before extending the call and the amount of time that must pass before a call can be answered at the remote phone. Mobility users can also configure filters for each remote destination to allow or deny calls from certain phone numbers to be extended to that remote phone.

Note Cisco Business Edition supports a maximum of four remote destinations per mobility user.

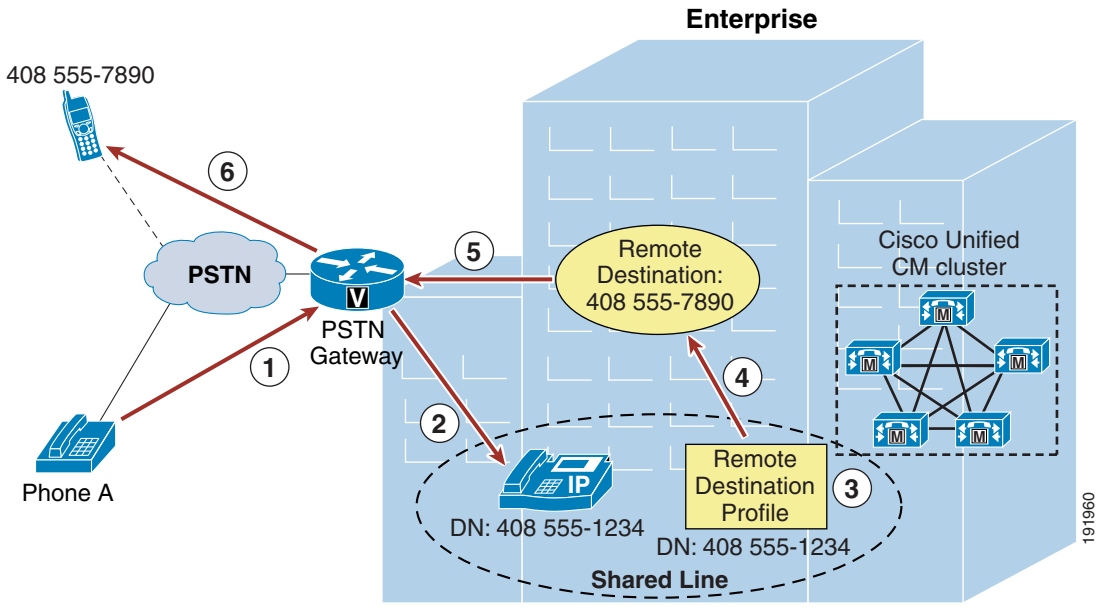
Mobile Connect

The Mobile Connect feature allows an incoming call to an enterprise user to be offered to the user's IP desk phone as well as up to 10 configurable remote destinations. Typically a user's remote destination is their mobile or cellular telephone. Once the call is offered to both the desktop and remote destination phone(s), the user can answer at any of those phones. Upon answering the call on one of the remote destination phones or on the IP desk phone, the user has the option to hand off or pick up the call on the other phone.

Mobile Connect Functionality

Figure 25-16 illustrates a basic Mobile Connect call flow. In this example, Phone A on the PSTN calls a Mobile Connect user's enterprise directory number (DN) 408-555-1234 (step 1). The call comes into the enterprise PSTN gateway and is extended through Unified CM to the IP phone with DN 408-555-1234 (step 2), and this phone begins to ring. The call is also extended to the user's Remote Destination Profile, which shares the same DN (step 3). In turn, a call is placed to the remote destination associated with the user's remote destination profile (in this case 408-555-7890) (step 4). The outgoing call to the remote destination is routed through the PSTN gateway (step 5). Finally the call rings at the remote destination PSTN phone with number 408 555-7890 (step 6). The call can then be answered at either phone.

Figure 25-16 Mobile Connect



Typically a Mobile Connect user's configured remote destination is their mobile phone on a mobile voice or cellular provider network; however, any destination reachable by means of the PSTN can be configured as a user's remote destination. Furthermore, a Mobile Connect user can have up to 10 remote

destinations configured, so an incoming call could potentially ring as many as 10 PSTN phones as well as the user's desk phone. Once the call is answered at the desk phone or at a remote destination phone, any other call legs that have been extended to ring additional remote destinations or the desk phone (if not answered at the desk phone) will be cleared. If the incoming call is answered at the remote destination, the voice media path will be hairpinned within the enterprise PSTN gateway utilizing two gateway ports. This utilization must be considered when deploying the Mobile Connect feature.

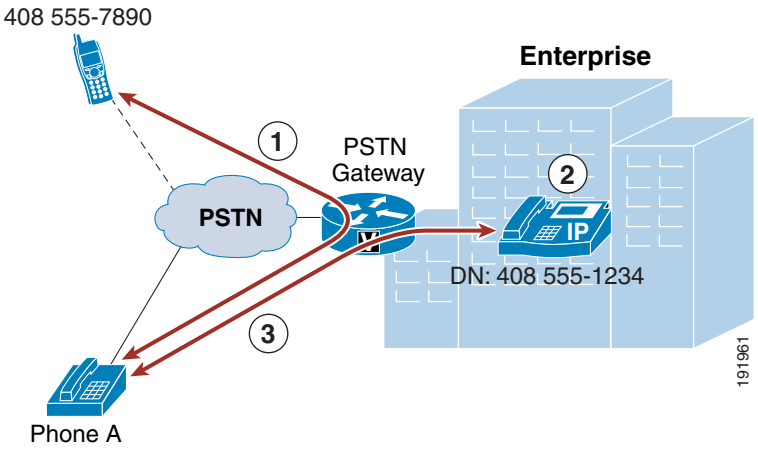
Note Mobility users on a Cisco Business Edition system can have a maximum of four remote destinations.

Note In order for Mobile Connect to work as in Figure 25-16, ensure that the user-level Enable Mobility check box under the End User configuration page has been checked and that at least one of the user's configured remote destinations has the Enable Mobile Connect check box checked.

Desk Phone Pickup

As illustrated in Figure 25-17, once a user answers a Mobile Connect call at the remote destination device (step 1: in this case, 408 555-7890), at any point the user can hang up the call at the remote destination and pick it up again at their desk phone by simply pressing the Resume softkey on the desk phone (step 2: at DN 408 555-1234 in this case). The call resumes between the original caller at Phone A and the desk phone (step 3).

Figure 25-17 Desk Phone Pickup



Desk phone pickup can be performed whenever an enterprise-anchored call is in progress at a configured remote destination phone and that phone hangs up the call.

Note An enterprise-anchored call refers to any call that has at least one call leg connected through an enterprise PSTN gateway and that originated either from a remote destination to an enterprise DID or from Mobile Connect, Mobile Voice Access, Enterprise Feature Access, or Intelligent Session Control.

The option to pick up or resume the call at the desk phone is available for a certain amount of time. For this reason, it is good practice for the Mobile Connect user to ensure that the calling phone hangs up before the remote destination phone is hung up. This ensures that the call cannot be resumed at the desk

phone by someone else. By default, the call remains available for pickup at the desk phone for 10 seconds after the remote destination phone hangs up; however, this time is configurable and can be set from 0 to 30000 milliseconds on a per-user basis by changing the Maximum Wait Time for Desk Pickup parameter under the End User configuration page. Desk phone pickup can also be performed after invoking the mid-call hold feature at the remote destination phone. However, in these cases, the Maximum Wait Time for Desk Pickup parameter setting has no effect on the amount of time the call will be available for pickup. A call placed on mid-call hold will remain on hold and be available for desk phone pickup until manually resumed at either the remote or desktop phone.

Another method for performing desk phone pickup is to use the mid-call session handoff feature. This mid-call feature is invoked by manually keying *74, the default enterprise feature access code for session handoff, which in turn generates a DTMF sequence back to Unified CM. When this feature is invoked, Unified CM sends a new call to the user's enterprise desk phone. Once this new call is flashing or ringing at the desk phone, the user then must answer the call to complete the session handoff.

The benefit of this desk phone pickup method over other methods (such as hanging up the call at the mobile phone or using the mid-call hold feature) is that the conversation between the user and the far-end phone is maintained throughout the handoff process. Once the *74 sequence has been keyed, the user can continue the conversation because the handoff call is sent to the user's desk phone. When the user answers the call at the desk phone, the call legs are shuffled so that the call leg to the far-end is connected to the new call leg created at the desk phone, thus resulting in an uninterrupted or near-instantaneous cut-through of the audio path. The original call leg at the mobile device is subsequently cleared.

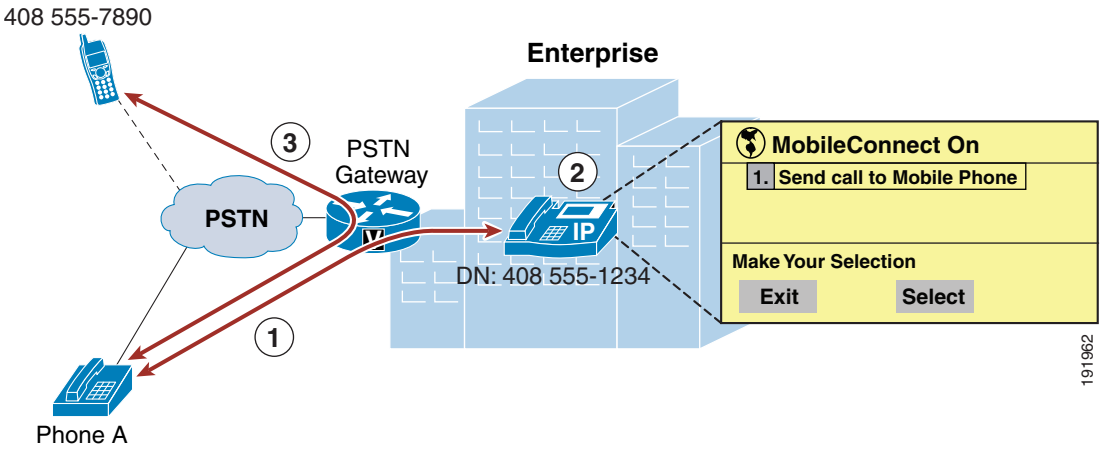
Unlike the hang-up method for invoking desk phone pickup, where the end-user’s Maximum Wait Time for Desk Pickup setting determines how long the call will be available for pickup at the desk phone, with session handoff the Session Handoff Alerting Timer service parameter determines the amount of time the call will ring or flash at the desk phone before the handoff call is cleared. The default handoff alerting time is 10 seconds. Further, with session handoff, any call forward settings configured on the desk phone do not get invoked. As a result, the handoff feature does not forward to voicemail or any other call-forward destination. If a call is not answered by the end of Session Handoff Alerting Timer period, then the call is cleared and the Remote In Use state is removed from the user's desk phone line. However, in this scenario the original call is maintained at the mobile phone.

For additional information about session handoff and other mid-call features, see Mid-Call Features, page 25-43.

Remote Destination Phone Pickup

Figure 25-18 illustrates Mobile Connect remote destination phone pickup functionality. Assuming Phone A calls the Mobile Connect user's enterprise DN 408 555-1234 and the call is answered at the user's desk phone and is in progress (step 1), the user must push the Mobility softkey. Assuming the Mobile Connect feature is enabled for this phone and remote destination pickup is available, the user presses the Select softkey (step 2). A call is generated to the user's remote destination phone (in this case, 408 555-7890), and the remote phone begins to ring. Once the call is answered at the remote phone, the call resumes between Phone A and the Mobile Connect user's remote phone with number 408 555-7890 (step 3).

Figure 25-18 Remote Destination Phone Pickup



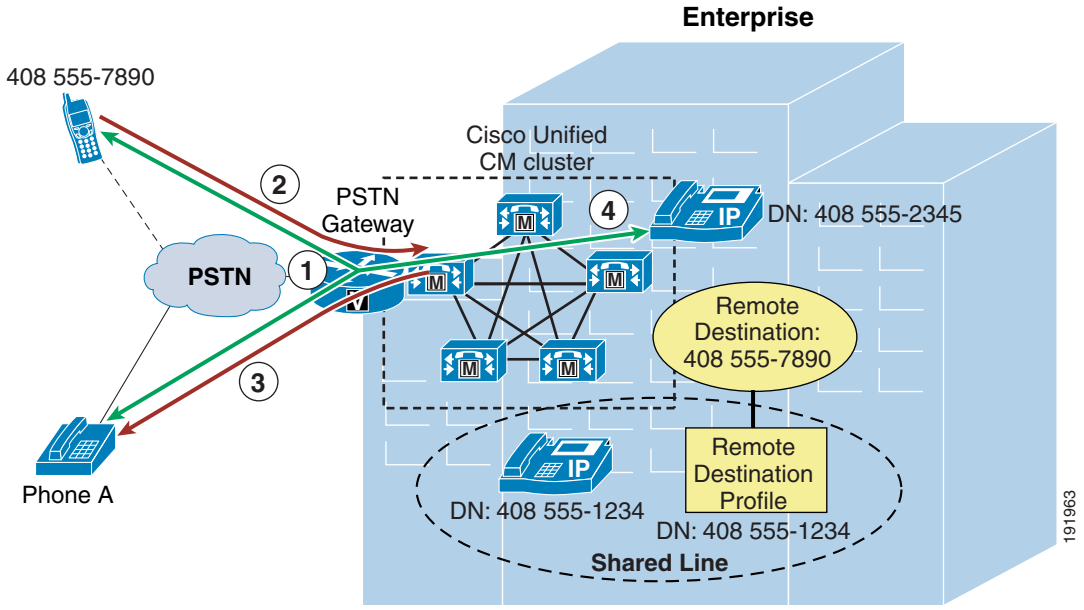
When a Mobile Connect user has multiple remote destinations configured, each remote destination will ring when the Select softkey is pressed, and the user can answer the desired phone.

Note In order for remote destination phone pickup to work as in Figure 25-18, ensure that at least one of the user's configured remote destinations has the Mobile Phone check box checked. In addition, the Mobility softkey must be configured for all mobility users by adding the softkey to each user's associated desk phone softkey template. Failure to check the Mobile Phone check box and to make the Mobility softkey available to mobility users will prevent the use of remote destination phone pickup functionality.

Mid-Call Features

As illustrated in Figure 25-19, once a user answers a Mobile Connect call at the remote destination device (step 1: in this case, 408 555-7890), the user can invoke mid-call features such as hold, resume, transfer, conference, directed call park, and session handoff by sending DTMF digits from the remote destination phone to Unified CM via the enterprise PSTN gateway (step 2). When the mid-call feature hold, transfer, conference, or directed call park is invoked, MoH is forwarded from Unified CM to the held party (step 3: in this case, Phone A). In-progress calls can be transferred to another phone or directed call park number, or additional phones can be conferenced using enterprise conference resources (step 4).

Figure 25-19 Mobility Mid-Call Feature



Mid-call features are invoked at the remote destination phone by a series of DTMF digits forwarded to Unified CM. Once received by Unified CM, these digit sequences are matched to the configured Enterprise Feature Access Codes for Hold, Exclusive Hold, Resume, Transfer, Conference, and Session Handoff, and the appropriate function is performed.

Note To enable the Directed Call Park mid-call feature, you must configure Cisco Unified CM with directed call park numbers and call park retrieval prefixes.

Note In order to perform the transfer, conference, and directed call park mid-call features, a second call leg is generated by the remote destination phone to a system-configured Enterprise Feature Access DID that answers the call, takes user input (including PIN number, mid-call feature access code, and target number), and then creates the required call leg to complete the transfer, conference, or directed call park operation.

With the mid-call session handoff feature, MoH is not forwarded to the far-end because the far-end is never placed on hold. Instead, the original audio path is maintained until the mobile user answers the handoff call at the desk phone. Once the call is answered, the call legs are shuffled at the enterprise gateway and the audio path is maintained.

Mid-call features are invoked by manually keying the feature access codes and entering the appropriate key sequences. Table 25-2 indicates the required key sequences for invoking mid-call features.

Table 25-2 Manual Mid-Call Feature Key Sequences

Mid-Call Feature	Enterprise Feature Access Code (default)	Manual Key Sequence
Hold	*81	Enter: *81
Exclusive Hold	*82	Enter: *82
Resume	*83	Enter: *83
Transfer	*84	1. Enter: *82 (Exclusive Hold) 2. Make new call to Enterprise Feature Access DID. 3. On connect, enter: <*PIN_number*> # *84 # <*Transfer_Target/DN*> # 4. Upon answer by transfer target (for consultive transfer) or upon ringback (for early attended transfer), enter: *84
Directed Call Park	N/A	1. Enter: *82 (Exclusive Hold) 2. Make new call to Enterprise Feature Access DID. 3. On connect, enter: <*PIN_number*> # *84 # <*Directed_Call_Park_Number*> # *84 # **Note** To retrieve a parked call, the user must use Mobile Voice Access or Enterprise Feature Access Two-Stage Dialing to place a call to the directed call park number. When entering the directed call park number to be dialed, it must be prefixed with the appropriate call park retrieval prefix.
Conference	*85	1. Enter: *82 (Exclusive Hold) 2. Make new call to Enterprise Feature Access DID. 3. On connect enter: <*PIN_number*> # *85 # <*Conference_Target/DN*> # 4. Upon answer by conference target, enter: *85
Session Handoff	*74	1. Enter: *74 2. Answer at the desk phone upon ring and/or flash.

Note Media resource allocation for mid-call features such as hold and conference is determined by the Remote Destination Profile configuration or, in the case of dual-mode phones and Unified Mobile Communicator, the device configuration. The media resource group list (MRGL) of the device pool configured for the Remote Destination Profile or the mobile client device is used to allocate a conference bridge for the conferencing mid-call feature. The User Hold Audio Source and Network Hold MoH Audio Source settings of the Remote Destination Profile or the mobile client device, in combination with the media resource group list (MRGL) of the device pool, is used to determine the appropriate MoH stream to be sent to a held device.

Mobile Voicemail Avoidance with Single Enterprise Voicemail Box

An additional consideration with Unified Mobility Mobile Connect is mobile voicemail avoidance. The single enterprise voicemail box feature ensures that all unanswered enterprise business calls end up at the enterprise voicemail system. This prevents a user from having to check multiple mailboxes (enterprise, mobile, home, and so forth) for unanswered calls to their enterprise phone number. To implement this feature, the system relies on a set of timers (one per remote destination) in conjunction with system call-forward timers. The purpose of these timers is to ensure that, when and if a call is forwarded to a voicemail box on ring-no-answer, the call is forwarded to the enterprise voicemail box rather than any remote destination voicemail box. These timers, in conjunction with other system forward-no-answer timers, should be configured to avoid non-enterprise voicemail systems as follows:

- Ensure the system forward-no-answer time is shorter at the desk phone than at the remote destination phones.

  To do so, ensure that the global Forward No Answer Timer field in Unified CM or the No Answer Ring Duration field under the individual phone line is configured with a value that is less than the amount of time a remote destination phone will ring before forwarding to the mobile voicemail system. In addition, the Delay Before Ringing Timer parameter under the Remote Destination configuration page can be used to delay the ringing of the remote destination phone in order to further lengthen the amount of time that must pass before a remote destination phone will forward to its own mobile voicemail box. However, when adjusting the Delay Before Ringing Timer parameter, take care to ensure that the global Unified CM Forward No Answer Timer (or the line-level No Answer Ringer Duration field) is set sufficiently high enough so that the mobility user has time to answer the call on the remote destination phone. The Delay Before Ringing Timer parameter can be set for each remote destination and is set to 4000 milliseconds by default.

- Ensure that the remote destination device stops ringing before the incoming call is forwarded to the mobile voicemail system.

  You can accomplish this with the Answer Too Soon and Answer Too Late timers for each remote destination. First the Answer Too Soon Timer parameter under the Remote Destination configuration page should be configured with a value that is more than the amount of time it takes a call extended to a powered-off or out-of-range mobile phone to be forwarded to the mobile voicemail system. By default this timer is set 1,500 milliseconds (or 1.5 seconds). If the call is answered before the Answer Too Soon Timer expires, the system will disconnect the call leg to the remote destination. This ensures that calls forwarded immediately to the mobile voicemail system are not connected, but those answered by the user after ring-in are connected.

  Next configure the Answer Too Late Timer parameter under the Remote Destination configuration page with a value that is less than the amount of time a remote destination phone will ring before forwarding to its voicemail box. By default this timer is set to 19,000 milliseconds (or 19 seconds). If the call is not answered before this timer expires, the system will disconnect the call leg to the remote destination. This ensures that the remote destination phone stops ringing before the call is forwarded to the mobile voicemail system.

Note Incoming calls to a remote destination that are manually diverted by the mobility user can end up in the mobile voicemail box if the manual divert occurs after the Answer Too Soon timer has expired. To prevent this from happening, mobility users should be advised to ignore or silence the ringing of incoming calls they wish to divert to voicemail. This will ensure that unanswered calls always end up in the enterprise voicemail system.

Note In most deployment scenarios, the default Delay Before Ringing Timer, Answer Too Late Timer, and Answer Too Soon Timer values are sufficient and do not need to be changed.

Enabling and Disabling Mobile Connect

The Mobile Connect feature can be enabled or disabled by using one of the following methods:

- Cisco Unified CM Administration or Cisco Unified CM User Options pages

  An administrator or user unchecks the Mobile Connect box to disable, or checks the Mobile Connect box to enable, the feature. This is done per remote destination.

- Mobile Voice Access or Enterprise Feature Access

  A Mobility-enabled user dials into the Mobile Voice Access or Enterprise Feature Access DID and, after entering appropriate credentials, enters the digit 2 to enable or 3 to disable. With Mobile Voice Access, the user is prompted to enable or disable Mobile Connect for a single remote destination or all of their remote destinations. With Enterprise Feature Access, the user can enable or disable Mobile Connect only for the remote destination device from which they are calling.

- Desk phone Mobility softkey

  The user presses the Mobility softkey when the phone is in the on-hook state and selects either Enable Mobile Connect or Disable Mobile Connect. With this method, Mobile Connect is enabled or disabled for all of the user's remote destinations.

- Mobile Clients

  Users with a mobile device running Cisco Unified Mobile Communicator or direct connect mobile clients can toggle the Mobile Connect feature status by changing the Mobile Connect or Single Number Reach setting to Enable or Disable under the client configuration settings. This will enable or disable Mobile Connect for the Cisco Unified Mobile Communicator or direct connect mobile client mobility identity only.

Access Lists for Allowing or Blocking Mobile Connect Calls

Access lists can be configured within Cisco Unified CM and associated to a remote destination. Access lists are used to allow or block inbound calls (based on incoming caller ID) from being extended to a mobility-enabled user's remote destinations. Furthermore, these access lists are invoked based on the time of day.

Access lists are configured for mobility-enabled users as either blocked or allowed. Access lists contain one or more members or filters consisting of a specific number or number mask, and the filters are compared against the incoming caller ID of the calling party. In addition to containing specific number strings or number masks for matching caller ID, access lists can also contain a filter for incoming calls where the caller ID is not available or is set to private. A blocked access list contains an implicit "allow all" at the end of the list so that calls from any numbers entered in the access list will be blocked but calls from all other numbers will be allowed. An allowed access list contains an implicit "deny all" at the end of the list so that calls from any numbers entered in the access list will be allowed but calls from all other numbers will be blocked.

Once configured access lists are associated with a configured Ring Schedule under the Remote Destination configuration screen, the configured Ring Schedule in combination with the selected access list provides time-of-day call filtering for Mobile Connect calls on a per-remote-destination basis. Access lists and Ring Schedules can be configured and associated to a remote destination by an administrator using the Cisco Unified CM Administration interface or by an end user using the Cisco Unified CM User Options interface.

Mobile Connect Architecture

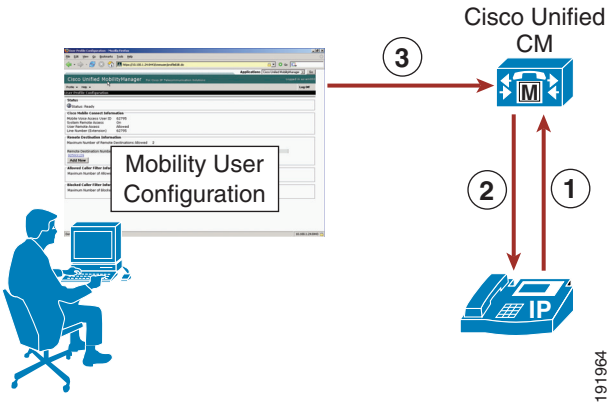
The architecture of the Mobile Connect feature is as important to understand as its functionality. Figure 25-20 depicts the message flows and architecture required for Mobile Connect. The following sequence of interactions and events can occur between Unified CM, the Mobile Connect user, and the Mobile Connect user's desk phone:

1. The Mobile Connect phone user who wishes to either enable or disable the Mobile Connect feature or to pick up an in-progress call on their remote destination phone pushes the Mobility softkey on their desk phone (see step 1 in Figure 25-20).
2. Unified CM returns the Mobile Connect status (On or Off) and offers the user the ability to select the Send Call to Mobile Phone option when the phone is in the Connected state, or it offers the user the ability to enable or disable the Mobile Connect status when the phone is in the On Hook state (see step 2 in Figure 25-20).
3. Mobile Connect users can use the Unified CM User Options interface to configure their own mobility settings via the web-based configuration pages at

   http://<*Unified-CM_Server_IP_Address*>/ccmuser/

   where <*Unified-CM_Server_IP_Address*> is the IP address of the Unified CM publisher server (see step 3 in Figure 25-20).

Figure 25-20 Mobile Connect Architecture



High Availability for Mobile Connect

The Mobile Connect feature relies on the following components:

- Unified CM servers
- PSTN gateway

Each component must be redundant or resilient in order for Mobile Connect to continue functioning fully during various failure scenarios.

Unified CM Server Redundancy

The Unified CM server is required for the Mobile Connect feature. Unified CM server failures are non-disruptive to Mobile Connect functionality, assuming phone and gateway registrations are made redundant using Unified CM Groups.

In order for Mobile Connect users to use the Unified CM User Options web interface to configure their mobility settings (remote destinations and access lists), the Unified CM publisher server must be available. If the publisher is down, users will not be able to change mobility settings. Likewise, administrators will be unable to make mobility configuration changes to Unified CM; however, existing mobility configurations and functionality will continue. Finally, changes to Mobile Connect status must be written by the system on the Unified CM publisher server; if the Unified CM publisher is unavailable, then enabling or disabling Mobile Connect will not be possible.

PSTN Gateway Redundancy

Because the Mobile Connect feature relies on the ability to extend additional call legs to the PSTN to reach the Mobile Connect users' remote destination phones, PSTN gateway redundancy is important. Should a PSTN gateway fail or be out of capacity, the Mobile Connect call cannot complete. Typically, enterprise IP telephony dial plans provide redundancy for PSTN access by providing physical gateway redundancy and call re-routing capabilities as well as enough capacity to handle expected call activity. Assuming that Unified CM has been configured with sufficient capacity, multiple gateways, and route group and route list constructs for call routing resiliency, the Mobile Connect feature can rely on this redundancy for uninterrupted functionality.

Mobile Voice Access and Enterprise Feature Access

Mobile Voice Access (also referred to as System Remote Access) and Enterprise Feature Access two-stage dialing are features built on top of the Mobile Connect application. Both features allow a mobility-enabled user who is outside the enterprise to make a call as though they are directly connected to Unified CM. This functionality is commonly referred to as Direct Inward System Access (DISA) in traditional telephony environments. These features benefit the enterprise by limiting toll charges and consolidating phone billing directly to the enterprise rather than billing to each mobile user. In addition, these features allow the users to mask their mobile phone or remote destination numbers when sending outbound caller ID. Instead, the user's enterprise directory number is sent as caller ID. This ensures that returned calls to the user are made to the enterprise number, thus resulting in enterprise call anchoring. These features also enable mobile users to dial internal extensions or non-DID enterprise numbers that would not normally be reachable from outside the enterprise.

Mobile Voice Access is accessed by calling a system-configured DID number that is answered and handled by an H.323 or SIP VoiceXML (VXML) gateway. The VoiceXML gateway plays interactive voice response (IVR) prompts to the Mobile Voice Access user, requesting user authentication and input of a number to be dialed via the user phone keypad.

Enterprise Feature Access functionality includes the previously discussed mid-call transfer and conference features as well as two-stage dialing functionality. Two-stage dialing works the same way as Mobile Voice Access, but without the IVR prompts. The system-configured Enterprise Feature Access DID is answered by Unified CM. The user then uses the phone keypad or Smart Phone softkeys to input authentication and the number to be dialed. These inputs are received without prompts.

With both the Mobile Voice Access and Enterprise Feature Access two-stage dialing features, once the call to the input number is connected, users can invoke mid-call features or pick up the call on their desk phones just as with a Mobile Connect calls. This is possible because the call is anchored at the enterprise gateway.

Mobile Voice Access IVR VoiceXML Gateway URL

The Mobile Voice Access feature requires the Unified CM VoiceXML application to reside on the H.323 or SIP gateway. The URL used to load this application is:

http://<*Unified-CM-Publisher_IP-Address*>:8080/ccmivr/pages/IVRMainpage.vxml

where <*Unified-CM-Publisher_IP-Address*> is the IP address of the Unified CM publisher node.

Mobile Voice Access Functionality

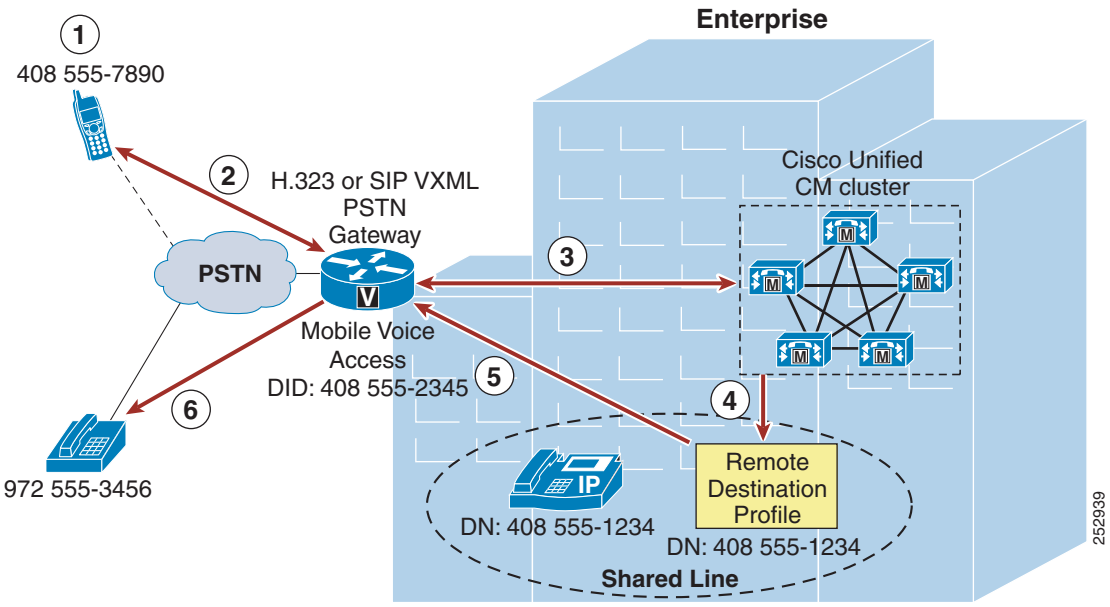
Figure 25-21 illustrates a Mobile Voice Access call flow. In this example, the Mobile Voice Access user on PSTN phone 408 555-7890 dials the Mobile Voice Access enterprise DID DN 408-555-2345 (step 1).

The call comes into the enterprise PSTN H.323 or SIP gateway, which also serves as the VoiceXML gateway. The user is prompted via IVR to enter their numeric user ID (followed by the # sign), PIN number (followed by the # sign), and then a 1 to make a Mobile Voice Access call, followed by the phone number they wish to reach. In this case, the user enters 9 1 972 555 3456 as the number they wish to reach (followed by the # sign) (step 2).

Note If the PSTN phone from which the Mobile Voice Access user is calling is configured as a Mobile Connect remote destination for that user and the incoming caller ID can be matched against this remote destination by Unified CM, the user does not have to enter their numeric user ID. Instead they will be prompted to enter just the PIN number.

In the meantime, Unified CM has forwarded IVR prompts to the gateway, the gateway has played these prompts to the user, and the gateway has collected user input including the numeric ID and PIN number of the user. This information is forwarded to Unified CM for authentication and to generate the call to 9 1 972 555 3456 (step 3). After authenticating the user and receiving the number to be dialed, Unified CM generates a call via the user's Remote Destination Profile (step 4). The outbound call to 972 555-3456 is routed via the PSTN gateway (step 5). Finally, the call rings at the PSTN destination phone with number 972 555-3456 (step 6).

Figure 25-21 Mobile Voice Access



Note In order for Mobile Voice Access to work as in Figure 25-21, ensure that the system-wide Enable Mobile Voice Access service parameter is set to True and that the per-user Enable Mobile Voice Access check box on the End User configuration page is also checked.

Note The Mobile Voice Access feature relies on the Cisco Unified Mobile Voice Access Service, which must be activated manually from the Unified CM Serviceability configuration page. This service can be activated on the publisher node only.

Mobile Voice Access Using Hairpinning

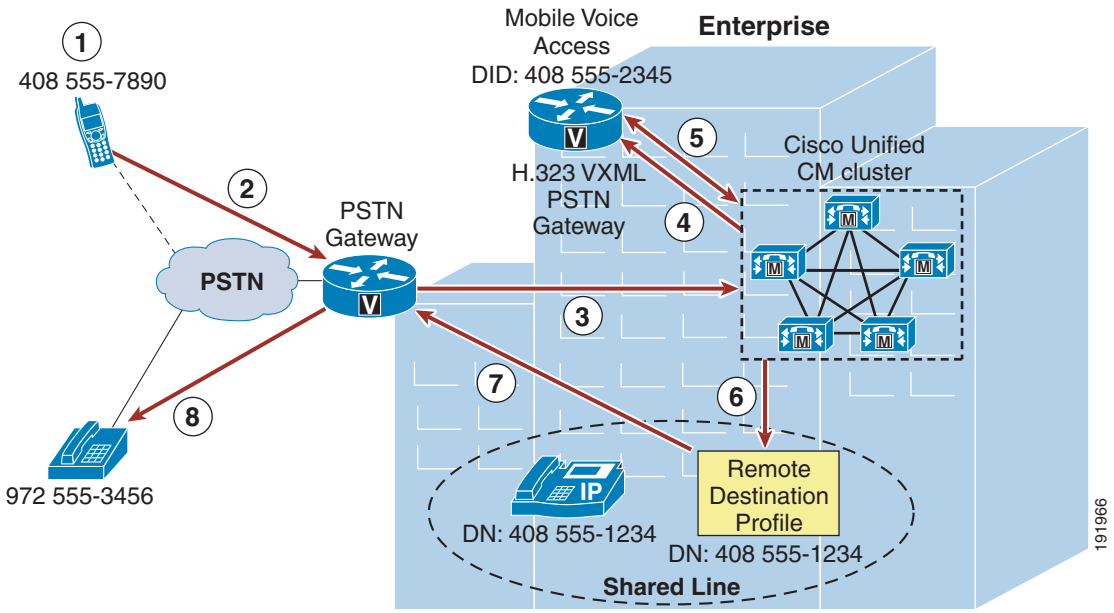
In deployments where the enterprise PSTN gateways are not using H.323 or SIP, Mobile Voice Access functionality can still be provided using hairpinning on a separate gateway running H.323. Mobile Voice Access using hairpinning relies on off-loading the VoiceXML functionality to a separate H.323 gateway. Figure 25-22 illustrates a Mobile Voice Access call flow using hairpinning. In this example, just as in the previous example, the Mobile Voice Access user on PSTN phone 408 555-7890 dials the Mobile Voice Access enterprise DID DN 408-555-2345 (step 1). The call comes into the enterprise PSTN gateway (step 2) and is forwarded to Unified CM for call handling (step 3). Unified CM next routes the inbound call to the H.323 VoiceXML gateway (step 4). The user is then prompted by IVR to enter their numeric user ID, PIN, and then a 1 to make a Mobile Voice Access call, followed by the phone number they wish to reach. Again the user enters 9 1 972 555 3456 as the number they wish to reach (followed by the # sign).

Note When using Mobile Voice Access with hairpinning, users calling into the system will not be identified automatically by their caller ID. Instead, users will have to key in their remote destination number manually prior to entering their PIN. The reason the user is not automatically identified is that, for hairpinning deployments, the PSTN gateway must first route the call to Unified CM to reach the

hairpinned Mobile Voice Access gateway. Because the call is routed to Unified CM first, the conversion of the calling number from a mobile number to an enterprise directory number occurs prior to the call being handled by the Mobile Voice Access gateway. This results in the Mobile Voice Access gateway being unable to match the calling number with a configured remote destination, and therefore the system prompts the user to enter their remote destination number. This is unique to hairpinning deployments; with normal Mobile Voice Access flows, the PSTN gateway does not have to route the call to Unified CM first in order to access Mobile Voice Access because the functionality is available on the local gateway.

In the meantime, the H.323 VoiceXML gateway collects and forwards the user input to Unified CM and then plays the forwarded IVR prompts to the PSTN gateway and the Mobile Voice Access user. Unified CM in turn receives user input, authenticates the user, and forwards appropriate IVR prompts to the H.323 VoiceXML gateway based on user input (step 5). After receiving the number to be dialed, Unified CM generates a call using the user's Remote Destination Profile (step 6). The outbound call to 972 555-3456 is routed through the PSTN gateway (step 7). Finally, the call rings at the PSTN destination phone with number 972 555-3456 (step 8).

Figure 25-22 Mobile Voice Access Using Hairpinning



Note When deploying Mobile Voice Access in hairpinning mode, Cisco recommends configuring the Mobile Voice Access DID at the PSTN gateway and the Mobile Voice Access Directory Number within Cisco Unified CM (under **Media Resources > Mobile Voice Access**) as different numbers. A translation pattern within Unified CM can then be used to translate the called number of the Mobile Voice Access DID to the configured Mobile Voice Access directory number. Because the Mobile Voice Access directory number configured within Unified CM is visible to the administrator only, translation between the DID and directory number will be invisible to the end user and there will be no change in end-user dialing behavior. This is recommended in order to prevent mobility call routing issues in multi-cluster environments. This recommendation does not apply to Mobile Voice Access in non-hairpinning mode.

Note Mobile Voice Access in hairpinning mode is supported only with H.323 VXML gateways.

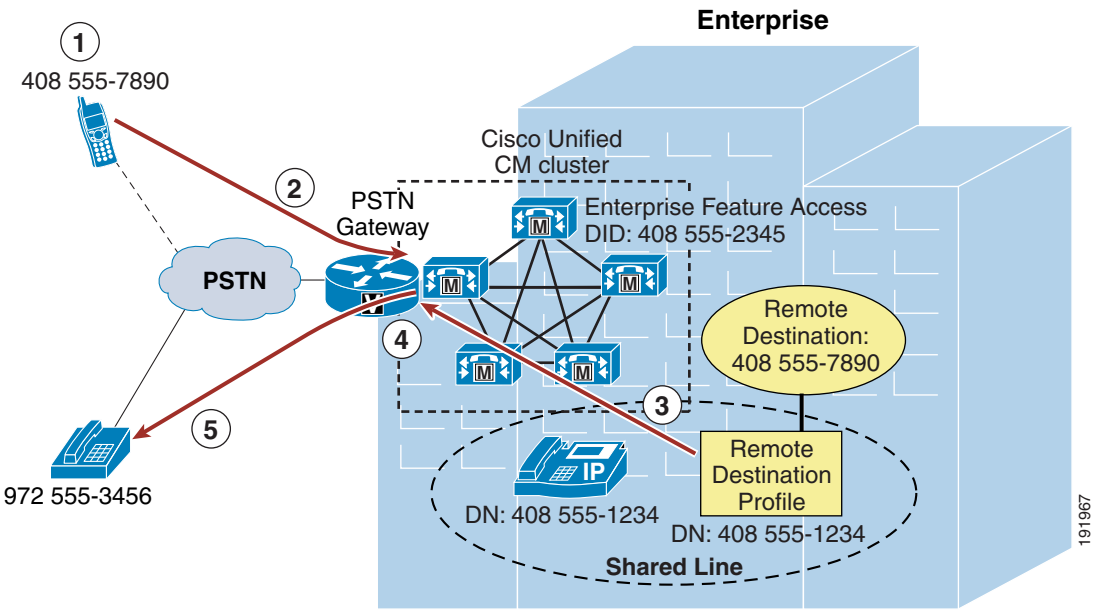
Enterprise Feature Access with Two-Stage Dialing Functionality

Figure 25-23 illustrates the call flow for Enterprise Feature Access two-stage dialing. In this example, the mobility user at remote destination phone 408 555-7890 dials the Enterprise Feature Access DID 408 555-2345 (step 1). Once the call is connected, the remote destination phone is used to send DTMF digits to Unified CM via the PSTN gateway, beginning with the user's PIN (followed by the # sign) which is authenticated with Unified CM. Next a 1 (followed by the # sign) is sent to indicate a two-stage dialed call is being attempted, followed by the phone number the user wishes to reach. In this case the user enters 9 1 972 555 3456 as the destination number (step 2).

Note Unlike with Mobile Voice Access, Enterprise Feature Access requires that all two-stage dialed calls must originate from a phone that has been configured as a remote destination in order to match the caller ID and PIN against the end-user account. There is no provision within Enterprise Feature Access in which the mobility user can enter their remote destination number or ID to identify themselves to the system. Identity can be established only via the combination of incoming caller ID and entered PIN.

Next the outgoing call is originated via the user's remote destination profile (step 3), and the call to PSTN number 972 555-3456 is routed via the enterprise PSTN gateway (step 4). Finally, the call rings the PSTN phone (step 5: in this case, 972 555-3456). As with Mobile Voice Access, the voice media path of each Enterprise Feature Access two-stage dialed call is hairpinned within the enterprise PSTN gateway utilizing two gateway ports.

Figure 25-23 Enterprise Feature Access Two-Stage Dialing Feature



Note In order for Enterprise Feature Access two-stage dialing to work as in Figure 25-23, ensure that the system-wide Enable Enterprise Feature Access service parameter is set to True.

Desk and Remote Destination Phone Pickup

Because Mobile Voice Access and Enterprise Feature Access functionality is tightly integrated with the Mobile Connect feature, once a Mobile Voice Access or Enterprise Feature Access two-stage dialed call has been established, the user does have the option of using Mobile Connect functionality to pick up the in-progress call on their desk phone by simply hanging up the call on the originating phone and pushing the Resume softkey on their desk phone or by using the mid-call hold feature. In turn, the call can then be picked up on the user's configured remote destination phone by pressing the Mobility softkey and selecting Send Call to Mobile Phone.

Enabling and Disabling Mobile Connect

In addition to providing users of Mobile Voice Access and Enterprise Feature Access with the ability to make calls from the PSTN as though they are within the enterprise, the functionality provided by Mobile Voice Access on the H.323 or SIP VoiceXML gateway and provided by Enterprise Feature Access also gives users the ability to remotely enable and disable their Mobile Connect functionality for each remote destination via their phone keypad. Rather than entering a 1 to make a call, users enter a 2 to turn the Mobile Connect feature on and a 3 to turn the Mobile Connect feature off.

If a user has more than one remote destination configured when using Mobile Voice Access, they are prompted to key in the remote destination phone number for which they wish to enable or disable the Mobile Connect feature. When using Enterprise Feature Access, a user can enable or disable Mobile Connect only for the remote destination phone from which they are calling.

Note When the Enable Mobile Voice Access service parameter is set to False, resulting in an inability to make two-stage dialed calls, Mobile Voice Access still provides users with the ability to enable and disable mobile connect remotely. As long as the Mobile Voice Access Directory Number has been configured on the system, the user's account has been enabled for Mobile Voice Access, and the Cisco Unified Mobile Voice Access service is running on the publisher, a calling user can still enable or disable Mobile Connect.

Mobile Voice Access and Enterprise Feature Access Number Blocking

Administrators might want to prevent users of Mobile Voice Access and Enterprise Feature Access two-stage dialing from dialing certain numbers when using these features. In order to restrict or block calls to certain numbers when using these features for off-net calls, a comma-separated list of those numbers can be configured in the System Remote Access Blocked Numbers service parameter field. Once this parameter is configured with blocked numbers, those numbers will not be reachable from a user's remote destination phone when using Mobile Voice Access or Enterprise Feature Access features. Numbers that administrators might want to block can include emergency numbers such as 911. When configuring blocked numbers, ensure they are configured as they would be dialed by an enterprise user, with appropriate prefixes or steering digits. For example, if an emergency number is to be blocked and the emergency number is dialed by system users as 9911, then the number configured in the System Remote Access Blocked Numbers field should be 9911.

Access Numbers for Mobile Voice Access and Enterprise Feature Access

While the Unified CM system allows the configuration of only a single Mobile Voice Access Directory Number, this does not preclude the use of multiple externally facing numbers that can access these internally configured numbers. For example, consider a system deployed in the US in New York with a remote site in San Jose as well as an overseas site in London. Even though the system may have the Mobile Voice Access directory number configured as 555-1234, the gateways at each location can be configured to map a local or toll-free DID number to this Mobile Voice Access directory number. For example, the gateway in New York may have DIDs of +1 212 555 1234 and +1 800 555 1234, which both map to the Mobile Voice Access number, while the gateway in San Jose has a DID of +1 408 666 5678 and the gateway in London has a DID of +44 208 777 0987, which also map to the Mobile Voice Access number of the system.

The Unified CM system does permit the configuration of multiple Enterprise Feature Access Numbers so that location-specific system access numbers can be configured for each geographic location of the deployment. This enables local or toll-free Enterprise Feature Access two-stage dialing functionality for all users regardless of geographic location.

By acquiring multiple local or toll-free DID numbers, system administrators can ensure that two-stage dialed calls will always originate as a call into the system that is either local or toll-free, thus providing further reductions in telephony costs.

Remote Destination Configuration and Caller ID Matching

When authenticating users for Mobile Voice Access and Enterprise Feature Access two-stage dialing functionality as well as the DTMF-based mid-call features Transfer and Conference, the caller ID of the calling remote destination phone is matched against all remote destinations configured within the system. Matching of this caller ID depends on a number of factors, including how the remote destination numbers are configured, whether digit prefixing is required to include PSTN steering digits on the system, and whether the Matching Caller ID with Remote Destination parameter is set to Partial or Complete Match.

To control the nature of this matching, consider the following two approaches.

Using Digit Prefix Mechanism

With this approach, remote destinations are configured just as the caller ID would be presented from the PSTN. For example, if the caller ID from the PSTN for a remote destination phone is presented as 4085557890, then this number should be configured on the Remote Destination configuration page. In order to route Mobile Connect calls appropriately to this remote destination, it is then necessary to use a digit prefixing mechanism to prefix necessary PSTN access codes and other required digits. For example, if 9 is required to reach the PSTN when dialing calls and a 1 is required for dialing long distance, then digit prefixing must be configured to add the 9 and 1 to the beginning of the dial string. Digit prefixing is facilitated by using translation patterns, route patterns, or route list constructs within the Unified CM system. Alternatively, Application Dial Rules may be used to provide digit prefixing. When using this approach, the Matching Caller ID with Remote Destination parameter should be left at the default setting of Complete Match.

Note Not only are Application Dial Rules applied to Mobile Connect, Mobile Voice Access, and Enterprise Feature Access calls, but they are also applied to calls made with Cisco WebDialer, Cisco Unified CM Assistant, Cisco Unified Personal Communicator, and Cisco Jabber applications. For this reason, exercise care when configuring these rules to ensure that dialing behavior across all applications is as expected.

Using Partial Caller ID Matching

With this approach, remote destinations are configured as they would be dialed from the system to the PSTN. For example, if the number for the remote destination is 14085557890 and PSTN access from the system requires a 9, then this number should be configured on the Remote Destination configuration page as 914085557890. This approach precludes the need for configuration of a digit prefixing mechanism on the system, but it requires that the Matching Caller ID with Remote Destination service parameter be set to Partial Match and that the Number of Digits for Caller ID Partial Match be set to the appropriate number of consecutive digits that should be matched against the remote destination caller ID. For example, if the caller ID for a remote destination is 14085557890 and the remote destination is configured as 914085557890, then the Number of Digits for Caller ID Partial Match would ideally be set to 10 or 11. In this example, this parameter could be set to a lower number of digits; however, always take care to ensure that enough consecutive digits are matched so that all configured remote destinations in the system are matched uniquely. If there is no exact match and more than one configured remote destination number is matched when using partial caller ID matching, the system treats this as if there is no matching remote destination number, thus requiring the user to enter their remote destination number/ID manually in the case of Mobile Voice Access before providing their PIN. With Enterprise Feature Access, there is no mechanism for the user to enter their remote destination number; therefore, when using this functionality, take care to ensure that only unique matches occur.

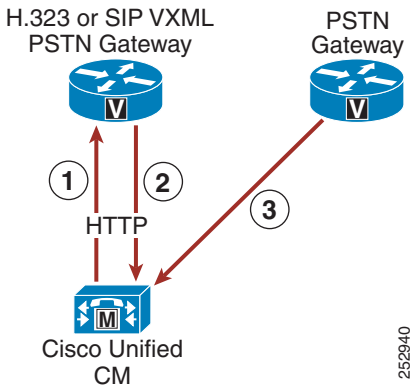
Note If the PSTN service provider sends variable-length caller IDs, using partial caller ID matching is not recommended because ensuring a unique caller ID match for each inbound call might not be possible. In these scenarios, using complete caller ID matching is the preferred method.

Mobile Voice Access and Enterprise Feature Access Architecture

The architecture of the Mobile Voice Access and Enterprise Feature Access feature is as important to understand as their functionality. Figure 25-24 depicts the message flows and architecture required for Mobile Voice Access and Enterprise Feature Access. The following sequence of interactions and events can occur between Unified CM, the PSTN gateway, and the H.323 or SIP VXML gateway:

1. Unified CM forwards IVR prompts and instructions to the H.323 or SIP VXML gateway via HTTP (see step 1 in Figure 25-24). This provides the VXML gateway with the ability to play these prompts for the inbound Mobile Voice Access callers.
2. The H.323 or SIP VXML gateway uses HTTP to forward Mobile Voice Access user input back to Unified CM (see step 2 in Figure 25-24).
3. The PSTN gateway forwards DTMF digits in response to user or Smart Phone key sequences from the remote destination phone for Enterprise Feature Access two-stage dialing and mid-call features (see step 3 in Figure 25-24).

Figure 25-24 Mobile Voice Access and Enterprise Feature Access Architecture



Note While Figure 25-24 depicts the H.323 or SIP VoiceXML gateway as a separate box from the PSTN gateway, this is not an architectural requirement. Both VoiceXML functionality and PSTN gateway functionality can be handled by the same box, provided there are no requirements for the PSTN gateway to run a protocol other than H.323 or SIP. An H.323 or SIP gateway is required for Mobile Voice Access VoiceXML functionality.

High Availability for Mobile Voice Access and Enterprise Feature Access

The Mobile Voice Access and Enterprise Feature Access features rely on the same components and redundancy mechanisms as the Mobile Connect feature (see High Availability for Mobile Connect, page 25-48). Unified CM Groups are necessary for PSTN gateway registration redundancy. Likewise, PSTN physical gateway and gateway connectivity redundancy should be provided. Redundant access between the PSTN and the enterprise is required for remote destination phones to access Mobile Voice Access and Enterprise Feature Access features in the event of a gateway failure. However, while physical redundancy can and should be provided for the H.323 or SIP VoiceXML gateway, there is no redundancy mechanism for the Cisco Unified Mobile Voice Access service on Unified CM. This service can be enabled and run on the publisher node only. Therefore, if the publisher node fails, Mobile Voice Access functionality will be unavailable. Enterprise Feature Access and two-stage dialing functionality have no such dependency on the publisher and can therefore provide equivalent functionality to mobility users (without the IVR prompts).

Designing Cisco Unified Mobility Deployments

The Cisco Unified Mobility solution delivers mobility functionality via Cisco Unified CM. Functionality includes Mobile Connect, Mobile Voice Access, and Enterprise Feature Access. When deploying this functionality it is important to understand dial plan implications, guidelines and restrictions, and performance and capacity considerations.

Dial Plan Considerations for Cisco Unified Mobility

In order to configure and provision Unified Mobility appropriately, it is important to understand the call routing behavior and dial plan implications of the remote destination profile configuration.

Remote Destination Profile Configuration

When configuring Unified Mobility, you must consider the following two settings on the Remote Destination Profile configuration page:

- Calling Search Space

  This setting combines with the directory number or line-level calling search space (CSS) to determine which partitions can be accessed for mobility dialed calls. This affects calls made by the mobility user from the remote destination phone, including Mobile Voice Access and Enterprise Feature Access two-stage dialing as well as calls made in conjunction with mid-call transfer and conferencing features. Ensure that this CSS, in combination with the line-level CSS, contains all partitions that need to be accessed for enterprise calls originating from a user's remote destination phone.

- Rerouting Calling Search Space

  This setting determines which partitions are accessed when calls are sent to a user's remote destination phone. This applies to all Mobile Connect calls. When a call to a user's enterprise directory number is also sent via Mobile Connect to a user's remote destination, this CSS determines how the system reaches the remote destination phone. For this reason, the CSS should provide access to partitions with appropriate route patterns and gateways for reaching the PSTN or mobile voice network.

When configuring the Remote Destination Profile Rerouting CSS, Cisco recommends that the route patterns within this CSS point to a gateway that is in the same call admission control location as the gateway used to route the inbound call to the user's desk phone. This ensures that a call admission control denial due to insufficient bandwidth between two locations will not occur when routing calls out to the remote destination. Further, because subsequent call admission control checks after the initial Mobile Connect call is routed will not result in a denial if there is insufficient WAN bandwidth, routing the inbound and outbound call legs out a gateway or gateways in the same call admission control location ensures that subsequent desk phone or remote destination pickup operations during this call will not require call admission control, which could result in WAN bandwidth oversubscription.

Likewise, when configuring the Remote Destination Profile CSS for outbound Mobile Voice Access or Enterprise Feature Access 2-Stage dialing call routing, Cisco recommends that the route patterns within this calling search space point to a gateway that is in the same call admission control location as the gateway that handles the inbound call leg to the Mobile Voice Access or Enterprise Feature Access DID. This ensures that a call admission control denial due to insufficient bandwidth will not occur during initial outbound call routing to the dialed number. However, be aware that a subsequent desk phone pickup can result in WAN bandwidth oversubscription if the desk phone is in a different call admission control location than the gateway through which the Mobile Voice Access or Enterprise Feature Access DIDs are reached.

Finally, because inbound PSTN calls to the mobility-enabled user will always come in their home location gateway based on the DID of their enterprise desk phone, in situations where the mobility-enabled user has moved call admission control locations either due to an Extension Mobility login at another site or due to the physical movement of the user's desk phone to another call admission control location, pointing to an outbound gateway that is located in the same call admission control location with the gateway that the inbound call came in on will not be possible in most cases. For this reason, Cisco recommends avoiding scenarios or deployments in which mobility-enabled users use extension mobility to log on to phones in call admission control locations outside their home location or physically move devices between call admission control locations. If these types of scenarios are not avoided or minimized, there is an increased potential for call leg failures due to call admission control denial or WAN oversubscription due to desk phone or remote destination pickup activity.

Automatic Caller ID Matching and Enterprise Call Anchoring

Another aspect of the Unified Mobility dial plan that is important to understand is the system behavior with regard to automatic caller ID identification for inbound calls from configured remote destination phones. Whenever an inbound call comes into the system, the presented caller ID for that call is compared against all configured remote destination phones. If a match is found, the call will automatically be anchored in the enterprise, thus allowing the user to invoke mid-call features and to pick up in-progress calls at their desk phone. This behavior occurs for all inbound calls from any mobility user's remote destination phone, even if the inbound call is not originated as a mobility call using Mobile Voice Access or Enterprise Feature Access.

Note Automatic inbound caller ID matching for configured remote destination numbers is affected by whether the Matching Caller ID with Remote Destination service parameter is set to Partial or Complete Match. See Remote Destination Configuration and Caller ID Matching, page 25-55, for more information about this setting.

In addition to automatic enterprise call anchoring, inbound and outbound call routing must also be considered when a configured remote destination phone is calling into the enterprise. Inbound call routing for calls from configured remote destinations occurs in one of two ways, depending on the setting of the service parameter Inbound Calling Search Space for Remote Destination. By default, this service parameter is set to **Trunk or Gateway Inbound Calling Search Space**. With the service parameter set to the default value, inbound calls from configured remote destinations will be routed using the Inbound Calling Search Space (CSS) of the PSTN gateway or trunk on which the call is coming in. If, on the other hand, the parameter Inbound Calling Search Space for Remote Destination is set to the value **Remote Destination Profile + Line Calling Search Space**, inbound calls coming from remote destinations will bypass the Inbound CSS of the PSTN gateway or trunk and will instead be routed using the associated Remote Destination Profile CSS (in combination with the line-level CSS).

Given the nature of inbound call routing from remote destination phones, it is important to make sure that calling search spaces are configured appropriately in order to provide access for these inbound calls to any partitions required for reaching internal enterprise phones, thus ensuring proper call routing from remote destination phones.

Note Incoming calls that do not come from a configured remote destination phone are not affected by the Inbound Calling Search Space for Remote Destination service parameter because they will always use the trunk or gateway inbound CSS.

Outbound call routing for Mobile Voice Access or Enterprise Feature Access calls always uses a concatenation of the Remote Destination Profile line CSS and device-level CSS, therefore it is important to make sure that these calling search spaces are configured appropriately in order to provide access to any route patterns necessary for off-net or PSTN access, thus ensuring proper outbound call routing from remote destination phones.

Intelligent Session Control

The Intelligent Session Control feature enables automatic call anchoring for enterprise-originated calls made directly to configured remote destination numbers. Normally, mobility call anchoring is dependent exclusively on calls made to or on behalf of a user's enterprise number. The system already anchors externally originated calls made by dial-via-office or enterprise two-stage dialing because these call are routed as internal calls. With the Intelligent Session Control feature enabled, the system will also anchor internally originated calls made directly to configured remote destinations.

This feature is enabled by setting the Reroute Remote Destination Calls to Enterprise Number service parameter to True. By default, this service parameter is set to False and the feature is disabled. When the feature is enabled, not only will the system route the call to the dialed remote destination by way of the PSTN, but it will also automatically anchor the call inside the enterprise gateway. By anchoring these types of calls, the system enables the called mobile user to invoke mid-call features and desk phone pickup or session handoff.

As an example, assume that the Intelligent Session Control feature has been enabled and that a mobility-enabled user has a remote destination number configured as 408 555 1234, which corresponds to their mobile number. If another system user dials the mobility-enabled user's remote destination number (408 555 1234) from their desk phone, the system will route the call through the PSTN to the remote destination and will simultaneously anchor the call in the enterprise gateway. Once the call is set up and anchored, the called mobility-enabled user now has the ability to invoke mid-call features such as hold, transfer, and conference, as well as the ability to perform a desk phone pickup or session handoff.

Taking this same example and assuming instead that the Intelligent Session Control feature is disabled, then when a system user dials the mobility-enabled user’s remote destination directly from a desk phone inside the enterprise, the call will still be routed to the called remote destination through the PSTN; however, the call will not be anchored. As a result, the mobile user would not be able to invoke mid-call hold or transfer and would have no ability to perform a desk phone pickup or session handoff.

When enabling this feature, it is important to understand the implications to dial plan configuration and call routing. To invoke the feature, the number dialed by an internal user to reach a remote destination number on the PSTN (including any required PSTN steering digits) must match the remote destination (or mobility identity) number as it is configured on the system. For example, if the remote destination number is configured on the system as 408 555 1234 but internal users must normally dial PSTN steering digits 91 in addition to the number they are calling, then rerouting and resulting enterprise call anchoring will not occur. This is because the user dialed 91 408 555 1234 to reach the remote destination on the PSTN but the remote destination was configured as 408 555 1234, so there is no match.

For this feature to function properly, matching must occur between the configured remote destination and the number that must be dialed to reach this remote destination on the PSTN. To ensure that this matching happens, set the service parameter Matching Caller ID with Remote Destination to **Partial Match**. By setting this parameter to Partial Match and then specifying the number of digits to partially match using the Number of Digits for Caller ID Partial Match service parameter, it is still possible to match the configured remote destination number with the dialed number even if it contains PSTN steering digits.

Using the previous example and assuming that system has been set to use partial match on ten digits, the dialed number 9 1 408 555 1234 can be matched to the configured remote destination 408 555 1234. This is because, with partial matching, the system attempts to match the same number of digits as specified by the Number of Digits for Caller ID Partial Match, which in this case is ten digits. The system attempts to match the two numbers by matching digits from right to left. The last ten digits of the dialed number 9 1 408 555 1234 are 408 555 1234, and these ten digits match the ten digits of the configured remote destination (408 555 1234). In this example, the resulting call is anchored in the enterprise and the called mobile user is able to invoke mid-call features and perform desk phone pickup or session handoff.

At first glance it might appear that an easier way to handle this feature would be to configure remote destination or mobility identity numbers that include any required PSTN steering digits. However, when configuring these numbers with required PSTN steering digits, if you do not also configure partial caller ID matching, the system will not be able to perform automatic caller ID matching and enterprise anchoring for inbound calls from configured remote destinations or mobility identities. In the previous example, if the remote destination number had been configured as 9 1 408 555 1234 and complete caller ID matching had been used, an inbound call from the remote destination would present caller ID of 408 555 1234 and a match would not occur, meaning the inbound call from the remote destination would not be anchored as expected.

Based on this potential for mismatch between dialed numbers for outbound calls and configured remote destination numbers for inbound calls, Cisco recommends enabling partial (rather than complete) caller ID matching when using the Intelligent Session Control feature for all deployments that require one or more steering digits to reach the PSTN. This ensures that calls made directly to the remote destination number using PSTN steering digits are still matched and anchored. On the other hand, if steering digits are not required to reach the PSTN and users are able to dial the full E.164 number to route calls to the PSTN, then Cisco recommends the complete caller ID matching setting because the remote destination is configured to match the caller ID and is the same number as dialed by internal users to reach the remote destination or mobility identity on the PSTN.

When enabling the Intelligent Session Control feature, it is also important to understand the behavior of the enterprise and remote destination lines during the reroute feature operation. On call reroute, remote destination line settings Do Not Disturb (DND), Access Lists and Time of Day call filtering, and the Delay Before Ringing Timer are ignored. All reroute calls are routed unfiltered and immediately. Enterprise desk phone line settings are also ignored or bypassed by default. However, Call Forward All settings on the enterprise desk phone line can be honored during reroute feature operation by setting the Ignore Call Forward All on Enterprise DN service parameter to False. If this parameter is set to False, on reroute operation, calls will not be routed to the remote destination if the enterprise desk phone line has a call-forward-all destination set. Instead, the call will be routed to the call-forward-all destination. By default, this service parameter is set to True, and call-forward-all settings on enterprise desk phone lines are ignored.

Caller ID Transformations

Any calls made into the cluster by configured remote destination numbers will automatically have their caller ID or calling number changed from the calling remote destination phone number to the enterprise directory number of the associated desk phone. For example, if a remote destination phone with number 408 555-7890 has been configured and associated to a user's enterprise desk phone with number 555-1234, then any call from the user's remote destination phone destined for any directory number in the cluster will automatically have the caller ID changed from the remote destination number of 408 555-7890 to the enterprise directory number of 555-1234. This ensures that the active call caller ID display and call history log caller ID reflect a mobility user's enterprise desk phone number rather than their mobile phone number, and it ensures that any return calls are made to the user's enterprise number, thus anchoring those calls within the enterprise.

Likewise, calls from a remote destination phone to external PSTN destinations and anchored in the enterprise via Mobile Voice Access or Enterprise Feature Access two-stage dialing, or those calls forked to the PSTN as a result of Mobile Connect, will also have caller ID changed from the calling remote destination phone number to the associated enterprise directory number.

Finally, in order to deliver the calling party number as an enterprise DID number rather than an enterprise directory number to external PSTN phones, calling party transformation patterns can be used. By using calling party transformation patterns to transform caller IDs from enterprise directory numbers to enterprise DIDs, return calls from external destinations will be anchored within the enterprise because they will be dialed using the full enterprise DID number. For more information about these transformations and dial plan implications, see Special Considerations for Cisco Unified Mobility, page 9-115.

Guidelines and Restrictions for Unified Mobility

The following guidelines and restrictions apply with regard to deployment and operation of Mobile Connect within the Unified CM telephony environment:

- Mobile Connect is supported only with PRI TDM PSTN connections. T1 or E1-CAS, FXO, FXS, and BRI PSTN connections are not supported. This PRI requirement is based on the fact that Cisco Unified CM must receive expeditious answer and disconnect indication from the PSTN in order to ensure full feature support. Answer indication is needed in order for Cisco Unified CM to stop ringing the desk phone and other remote destinations when a Mobile Connect call is answered at a particular remote destination. In addition, answer indication is required in order to support the single enterprise voicemail box feature. Finally, disconnect indication is required for desk phone pickup. A PRI PSTN connection will always provide answer or disconnect indication.
- Mobile Connect is also supported over SIP trunk VoIP PSTN connections as long as the Cisco IOS Unified Border Element provides the demarcation point between the Unified CM SIP trunk and the service provider trunk and as long as mid-call features (or other DTMF-dependent features) are not in use. Mid-call features are not supported over VoIP PSTN connections. A VoIP-based PSTN connection is still able to provide expeditious answer and disconnect indication to Unified CM due to the end-to-end signaling path provided by VoIP-based PSTN connections.
- Mobile Connect can support up to two simultaneous calls per user. Any additional calls that come in are automatically transferred to the user's voicemail.
- Mobile Connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Mobile Connect features are disabled for that call.
- Mobile Connect services do not extend to video calls. A video call received at the desktop phone cannot be picked up on the cellular phone.
- The Unified CM Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with Mobile Voice Access or Enterprise Feature Access.
- Remote destinations must be Time Division Multiplex (TDM) devices or off-system IP phones on other clusters or systems. You cannot configure IP phones within the same Unified CM cluster as remote destinations.

For additional guidelines and restrictions, refer to the information on Cisco Unified Mobility in the latest version of the *Cisco Unified Communications Manager Features and Services Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Capacity Planning for Cisco Unified Mobility

Cisco Unified Mobility supports the following capacities:

- Maximum of 15,000 mobility-enabled users per cluster with Cisco MCS 7845 server or Open Virtualization Archive (OVA) equivalent servers.
- Maximum of 10,000 mobility-enabled users per cluster with Cisco MCS-7835 or OVA equivalent servers.
- Maximum of 4,000 mobility-enabled users per cluster with Cisco MCS 7825 or OVA equivalent servers.
- Maximum of 3,750 remote destinations per MCS 7845 node or OVA equivalent server, or 15,000 destinations per cluster.
- Maximum of 2,500 remote destinations per MCS 7835 or OVA equivalent server, or 10,000 per cluster.
- Maximum of 1,000 remote destinations per MCS 7825 or OVA equivalent server, or 4,000 per cluster.

Note A mobility-enabled user is defined as a user that has a remote destination profile and at least one remote destination or a mobility identity configured.

The maximum number of supported mobility-enabled users will depend on the number of remote destinations or mobility identities configured for each user. The capacity numbers for maximum number of mobility-enabled users given above assume one remote destination or mobility identity per user. As the number of remote destinations or mobility identities per user increases, the number of supported mobility-enabled users decreases.

The above numbers are maximum capacities; however, Cisco Unified Mobility scalability and performance ultimately depend on the number of mobility users, the number of remote destinations or mobility identities each user has, and the busy hour call attempt (BHCA) rates of those users. Multiple remote destinations per user and/or high BHCA per user will result in lower capacity for Cisco Unified Mobility.

The capacity for Unified Mobility users on Cisco Business Edition systems depends exclusively on both the number of remote destinations per user and the BHCA of the users enabled for Unified Mobility, rather than on server hardware. Thus, the number of remote destinations supported on Cisco Business Edition depends directly on the BHCA of these users. The guidelines for sizing Unified Mobility for Cisco Business Edition are as follows:

- No more than 4 remote destinations can be configured per user. Given a maximum of 500 users per Cisco Business Edition system, the theoretical limit in terms of remote destinations is 2,000. However, given that the maximum BHCA per Cisco Business Edition is 3,600, it is possible that the system might not be able to support 2,000 remote destinations. Instead, BHCA calculations should be used to properly size the number of remote destinations that can be handled by the system.
- Each configured remote destination has potential BHCA implications. For every remote destination configured for a user, one additional call leg is used. Because each call consists of two call legs, one remote destination ring is equal to half (0.5) of a call. Therefore, you can use the following formula to calculate the total remote destination BHCA:

  Total remote destination BHCA = (Number of users) * (Number of remote destination per user) * (User BHCA) * 0.5

For example:

Assuming a system of 300 users at 5 BHCA each, with each user having one remote destination (total of 300 remote destinations), the calculation for the total remote destination BHCA would be:

Total remote destination BHCA = (300 users) * (1 remote destination per user) * (5 BHCA per user) * 0.5 = 750 BHCA

Total user BHCA in this example is (300 users) * (5 BHCA per user), which is 1500 total user BHCA. By adding the total remote destination BHCA of 750 to this value, we get a total system BHCA of 2250 (1500 total user BHCA + 750 total remote destination BHCA).

If other applications or additional BHCA variables are in use on the system in the example above, the capacity might be limited. (See Cisco Business Edition Capacity Planning, page 8-28, for further details.)

Note A mobility identity is configured just like a remote destination within the system, and it has the same capacity implications as a remote destination. Unlike a remote destination, however, the mobility identity is associated directly to a phone device rather than a remote destination profile. The mobility identity applies only to mobile client devices such as dual-mode phones, direct connect clients, and Cisco Unified Mobile Communicator clients.

Cisco Unified Mobility scalability and performance ultimately depends on the number of mobility users, the number of remote destinations or mobility identities each user has, and the busy hour call attempt (BHCA) rates of those users. Multiple remote destinations per user and/or high BHCA per user may result in lower capacity for Cisco Unified Mobility. For information on general Unified CM system sizing, see the chapter on Unified Communications Design and Deployment Sizing Considerations, page 29-1.

Design Considerations for Cisco Unified Mobility

Observe the following design recommendations when deploying Unified Mobility:

- Ensure that the PSTN gateway protocol is capable of out-of-band DTMF relay or allocate media termination points (MTPs) in order to covert in-band DTMF to out-of-band DTMF. When using Cisco IOS gateways for PSTN connectivity, out-of-band DTMF relay will be supported. However, third-party gateways might not support a common out-of-band DTMF method, and as a result an MTP might be required. In order to use Enterprise Feature Access Two-Stage Dialing and mid-call features, DTMF digits must be received out-of-band by Cisco Unified CM.

  Note When relying on MTP for converting in-band DTMF to out-of-band DTMF, be sure to provide sufficient MTP capacity. If heavy or frequent use of Enterprise Feature Access Two-Stage Dialing or mid-call features is anticipated, Cisco recommends a hardware-based MTP or Cisco IOS software-based MTP.

- Prior to deploying Unified Mobility, it is important to work with the PSTN provider to ensure the following:
  - Caller ID is provided by the service provider for all inbound calls to the enterprise. This is a requirement if Enterprise Feature Access Two-Stage Dialing or mid-call transfer, conference, and directed call park features are needed.

  - Outbound caller ID is not restricted by the service provider. This is a requirement if there is an expectation that mobility-enabled users will receive the caller ID of the original caller at their remote destination rather than a general enterprise system number or other non-meaningful caller ID.

Note Some providers restrict outbound caller ID on a trunk to only those DIDs handled by that trunk. For this reason, a second PRI trunk that does not restrict caller ID might have to be acquired from the provider. To obtain an unrestricted PRI trunk, some providers might require a signed agreement from the customer indicating they will not send or make calls to emergency numbers over this trunk.

Note Some providers allow unrestricted outbound caller ID on a trunk as long as the Redirected Dialed Number Identification Service (RDNIS) field or SIP Diversion Header contains a DID handled by the trunk. The RDNIS or SIP Diversion Header for forked calls to remote destinations can be populated with the enterprise number of the user by checking the Redirecting Number IE Delivery - Outbound check box on the gateway or trunk configuration page. Contact your service provider to determine if they honor the RDNIS or SIP Diversion Header and allow unrestricted outbound caller ID.

- Because mobility call flows typically involve multiple PSTN call legs, planning and allocation of PSTN gateway resources is extremely important for Unified Mobility. In cases where there are large numbers of mobility-enabled users, PSTN gateway resources will have to be increased. The following methods are recommend to minimize or reduce PSTN utilization:
  - Limit the number of remote destinations per mobility-enabled user to one (1). This will reduce the number of DS0s that are needed to extend the inbound call to the user's remote destination. One DS0 is consumed for each configured remote destination when a call comes into the user's enterprise directory number, even if the call is not answered at one of the remote destinations. Note that a DS0 per remote destination may be used for as long as 10 seconds, even if the call is not answered at the remote destination.
  - Use access lists to block or restrict the extension of calls to a particular remote destination based on incoming caller ID. Because access lists can be invoked based on the time of day, this eliminates the need for repeated updates of access lists by the end-user or the administrator.
  - Educate end-users to disable Mobile Connect when not needed, to further eliminate DS0 utilization when a call comes in for that user's enterprise number. If Mobile Connect is disabled, incoming calls will still ring the desk phone and will still forward to enterprise voicemail if the call goes unanswered.
- Due to the potential for call admission control denials resulting from insufficient WAN bandwidth between locations and the possibility that a desk phone pickup or remote destination pickup may result in a WAN bandwidth oversubscription, Cisco recommends configuring Remote Destination Profile CSS and Rerouting CSS so that route patterns within these CSSs point to gateways that are located within the same call admission control location as the gateway on which the inbound call leg comes in. For more information, see Remote Destination Profile Configuration, page 25-58.
- If you enable the Intelligent Session Control feature in deployments where PSTN steering digits must be dialed to access the PSTN, Cisco recommends setting the Matching Caller ID with Remote Destination service parameter to **Partial Match** and configuring the appropriate number of digits (Number of Digits for Caller ID Partial Match service parameter) to achieve a partial match of

configured remote destinations or mobility identities. This will ensure proper functioning of the Intelligent Session Control feature and the mobility automatic caller ID matching and anchoring features.

Dual-Mode Phones and Clients

As the prevalence of mobile users, mobile phones, and mobile carrier services continues to increase, the ability to use a single device for voice and data services both inside and outside the enterprise becomes increasingly attractive. Dual-mode phones and the clients that run on them afford an enterprise the ability to provide customized voice and data services to users while inside the enterprise and to leverage the mobile carrier network as a backup provider of general voice and data services, all by using a single mobile phone. By enabling voice and data services inside the enterprise and providing network connectivity for dual-mode phones, enterprises are able to provide these services locally at reduced connectivity costs. For example, voice over IP (VoIP) calls made on the enterprise network will typically incur less cost than those same calls made over the mobile voice network.

This section examines dual-mode phone architecture and common functions and features provided by dual-mode phones and clients, including remote secure attachment and handoff considerations related to moving an active voice call between the enterprise WLAN network and the mobile voice network. After covering general dual-mode solution architecture and features and functions, this section provides coverage of various capabilities and integration considerations for the following specific dual-mode clients:

- Cisco Mobile — A dual-mode client for the iPhone 3G mobile device, providing the ability to make VoIP calls on the enterprise WLAN network as well as to access corporate directory and voicemail services.
- Cisco Jabber — A dual-mode client for Android and iPhone mobile devices, providing the ability to make VoIP calls on the enterprise WLAN network or over private/public 802.11 WLAN hot spots or the mobile data network as well as the ability to access the corporate directory and receive enterprise voicemail message waiting indication and message count.
- Nokia Call Connect — A dual-mode client for Nokia mobile devices, providing the ability to make VoIP calls on the enterprise WLAN network or over private/public 802.11 WLAN hot spots or the mobile data network as well as the ability to access corporate directory and other applications and services.

Note End-of-Sale for the Nokia Call Connect client is July 10, 2012. There is no replacement mobile client for Nokia mobile devices. For more information, see the End-of-Sale (EoS) and End-of-Life (EoL) announcement at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7290/ps10589/end_of_life_notice_c51-696647.html.

In addition, this section discusses high availability and capacity planning considerations for dual-mode phones and clients.

Dual-Mode Phone Architecture

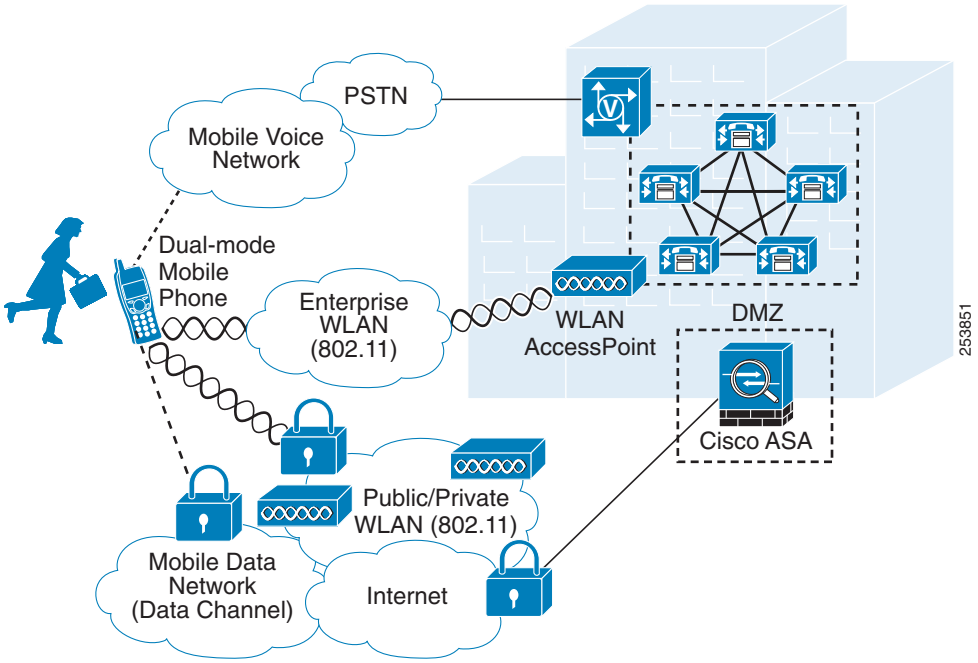
Dual-mode phones provide two physical interfaces or radios that enable the device to connect to both mobile voice and data carrier networks by means of traditional cellular or mobile network technologies and wireless local area networks (WLANs) using IEEE 802.11 standards. Dual-mode phones and the

clients that run on them enable on-premises data and voice connectivity through 802.11 WLAN as well as remote data and voice connectivity to the enterprise via public or private WLANs or over the mobile data network.

Note The use of the term *dual-mode phone* in this section refers specifically to devices with 802.11 radios in addition to the cellular radio for carrier voice and data network connectivity. Dual-mode devices that provide Digital Enhanced Cordless Telecommunications (DECT) or other wireless radios and/or multiple cellular radios are outside the scope of this section.

Figure 25-25 depicts the basic dual-mode solution architecture for incorporating dual-mode devices into a Cisco Unified Communications System. The dual-mode phone connects to the enterprise network, and then the dual-mode client registers to Cisco Unified CM as an enterprise phone. Once registered, the dual-mode device relies on the underlying enterprise Cisco IP telephony network for making and receiving calls. Only when enterprise network connectivity is unavailable, will the dual-mode phone fall back to the mobile voice network for making and receiving calls. When the dual-mode phone is connected to the enterprise network and the client is registered to Unified CM, the phone will be reachable through the user's enterprise number. Any inbound calls to the user's enterprise number will ring the dual-mode phone. If the user has a Cisco IP desk phone, then the dual-mode client registration enables a shared line instance for the user's enterprise number so that an incoming call rings both the user's desk phone and the dual-mode phone. When unregistered, the dual-mode client will not receive incoming enterprise calls at the dual-mode phone unless the user has been enabled for Cisco Unified Mobility and Mobile Connect (or single number reach) has been turned on for the user's mobile number.

Figure 25-25 Dual-Mode Phone Architecture



Note The voice quality of calls will vary depending on the Wi-Fi or mobile data network connection. Cisco Technical Assistance Center (TAC) is not able to troubleshoot connectivity or voice quality issues over mobile data networks or non-corporate Wi-Fi networks when using the secure connect feature of Cisco Jabber or the Cisco AnyConnect Secure Mobility Client.

Dual-mode phones must be capable of dual transfer mode (DTM) in order to be connected simultaneously to both the mobile voice and data network and the WLAN network. This allows the device to be reachable and able to make and receive calls on both the cellular radio and the IP interface (WLAN or mobile data) of the device. In some cases proper dual-mode client operation might not be possible if mobile voice and data networks do not support dual-connected devices.

Voice over Wireless LAN Network Infrastructure

Before considering the various dual-mode features and functions and the impact these features and functions have on the enterprise telephony infrastructure, it is critical to plan and deploy a finely tuned, QoS-enabled, and highly available WLAN network. Because dual-mode phones rely on the underlying WLAN infrastructure for carrying both critical signaling and other traffic for setting up calls and accessing various applications as well as the real-time voice media traffic, deploying a WLAN network optimized for both data and real-time voice traffic is necessary. A poorly deployed WLAN network will be subjected to large amounts of interference and diminished capacity, leading not only to poor voice quality but in some cases dropped or missed calls. This will in turn render the WLAN deployment unusable for making and receiving voice calls. Therefore, when deploying dual-mode phones, it is imperative to conduct a WLAN radio frequency (RF) site survey before, during, and after the deployment to determine appropriate cell boundaries, configuration and feature settings, capacity, and redundancy to ensure a successful voice over WLAN (VoWLAN) deployment. Each dual-mode phone device type and/or client should be tested on the WLAN deployment to ensure proper integration and operation prior to a production deployment. Using a WLAN that has been deployed and configured to provide optimized VoWLAN services (such as the Cisco Unified Wireless Network), including quality of service, will ensure a successful dual-mode phone deployment.

For more information on Voice over WLAN deployments and wireless device roaming, see Wireless Device Roaming, page 25-7.

Note While dual-mode phones and clients are capable of connecting back to the enterprise through the Internet for call control and other Unified Communications services, Cisco cannot guarantee voice quality or troubleshoot connectivity or voice quality issues for these types of connections. These types of connections include remote connections to the enterprise through public or private WLAN access points (APs) or hot spots or through the mobile data network. Cisco recommends an enterprise class voice-optimized WLAN network for connecting dual-mode phones and clients. Most public and private WLAN APs and hot spots are tuned for data applications and devices. In these cases, the AP radios are turned to maximum power, and dynamic-power control results in devices enabling maximum power on network attachment, which allows for larger client capacities. While this may be ideal for data applications that are capable of retransmitting dropped or lost packets, for voice applications this can result in very poor voice quality due to the potential for large numbers of dropped packets. Likewise, mobile provider data networks are susceptible to congestion and/or dropped connections, which can also result in poor voice quality and dropped calls.

Dual-Mode Features and Functions

Dual-mode devices provide a range of features and functions. While features and operations may vary from device to device, the common operations and behaviors described in this section apply to all dual-mode devices.

Enterprise Call Routing

Because dual-mode phones leverage the enterprise telephony infrastructure and call control services at least some of the time, it is important to understand the nature and behavior of call routing when the dual-mode device is inside the enterprise.

Inbound Call Routing

Because the dual-mode device registers to Unified CM as a user's enterprise extension with enterprise number, the dual-mode device rings when incoming calls to the system are destined for the user's enterprise number. This occurs for incoming calls originated on the PSTN or from other Unified CM clusters or enterprise IP telephony systems as well as for incoming calls originated within the Unified CM cluster by other users. If the dual-mode user has other devices or clients that are also associated to the enterprise number, these devices will also ring as shared lines; and once the call is answered at one of the devices or clients, ringing of all other devices and clients ceases.

In scenarios where a user has been enabled for Cisco Unified Mobility, and when Mobile Connect or single number reach is enabled for the user's dual-mode phone mobile number, the incoming call may also be extended to the mobility identity corresponding to the dual-mode mobile number. However, this depends on whether the dual-mode device is connected to the enterprise WLAN network or attached to the enterprise network through secure VPN and registered to Unified CM. In situations in which the dual-mode device is connected to the enterprise network directly or through a secure remote connection, an incoming call to the user's enterprise number will not be extended by Mobile Connect to the mobility identity of the dual-mode device even if Mobile Connect is turned on for this mobile number. The reason an incoming call to the enterprise number is not extended to the mobility identity of a dual-mode device when it is registered to Unified CM is that the system is aware the device is connected to the enterprise network and available. Thus, in order to reduce utilization of enterprise PSTN resources, Unified CM does not extend the call to the dual-mode device's mobile voice network interface through the PSTN. Instead, only the WLAN interface corresponding to the enterprise number is called.

Note For inbound calls to the enterprise number, the amount of time Unified CM waits for the SIP dual-mode client to respond before extending an incoming call to the mobility identity or mobile number via Mobile Connect, is determined by the SIP Dual Mode Alert Timer service parameter. By default this timer is set to 1,500 milliseconds. Cisco recommends increasing this timer to a minimum of 3,000 milliseconds to ensure that dual-mode clients have more time to respond to an inbound call on the IP interface of the device. After adjusting this global timer to 3,000 milliseconds, if users are still receiving calls at the cellular voice interface or mobility identity when the client appears to be registered, then adjust the timer upward to 4,500 milliseconds or higher. This is especially important for dual-mode client devices that are connected to the enterprise network remotely using VPN.

For situations in which the dual-mode device is not connected to the enterprise and/or not registered to Unified CM, incoming calls to the enterprise number will be extended to the dual-mode device according to the configured mobility identity, assuming that the user has been enabled for Unified Mobility and that Mobile Connect for the mobility identity is turned on. For more information on integration of dual-mode devices and clients with Unified Mobility, see Interactions Between Cisco Mobile or Cisco Jabber and Cisco Unified Mobility, page 25-79, and Interactions Between Nokia Call Connect and Cisco Unified Mobility, page 25-83.

In all cases, incoming calls made directly to the dual-mode device's mobile phone number will always be routed directly to the cellular radio of the dual-mode device on the mobile network, unless the provider network or device settings are such that calls are not extended to the device by the mobile network. This is considered appropriate behavior because these calls were not made to the user's enterprise number. These would be considered personal calls, and as such should not be routed through the enterprise.

Outbound Call Routing

For outbound calls from the dual-mode device, the interface used depends on the location and connectivity of the device at that particular time. If the dual-mode device is not connected to the enterprise and not registered to Unified CM, then calls are routed by the cellular voice radio interface to the mobile voice network as usual. However, when connected to the enterprise and registered to Unified CM, the dual-mode device should make all calls through the enterprise telephony infrastructure. If no enterprise connectivity is available or if the dual-mode client is unregistered, then outbound calling is not possible from the enterprise number, and instead callers would have to use the mobile number of the mobile device for making calls over the mobile voice network. Alternatively, users may use the two-stage dialing features provided with Cisco Unified Mobility (see Mobile Voice Access and Enterprise Feature Access, page 25-49).

In the case of some dual-mode clients, there may be a need for configuration of one or more settings in order to have the client register automatically to Unified CM when enterprise network connectivity is available. Whenever the dual-mode client is not registered to Unified CM, then outbound calls will be made using the mobile voice network rather than the enterprise network.

Dial Plan

The enterprise dial plan determines the dialing behavior of the dual-mode device when it is connected to the enterprise and registered to Unified CM. For example, if the enterprise dial plan is configured to allow abbreviated dialing to reach internal extensions, then a dual-mode device registered to Unified CM can leverage this abbreviated dialing. While it is certainly a convenience for dual-mode mobile phone users to be able to dial within the enterprise using enterprise dialing habits and leveraging abbreviated dialing as well as site-based and/or PSTN steering digits for outbound calls, it is also a somewhat unnatural dialing scheme because mobile phone users typically dial numbers for outgoing calls on their mobile phone by using full E.164 dial strings since this is what is expected by the mobile voice network for outbound calling.

The enterprise dialing experience for an end-user is ultimately up to the enterprise policies and administrator of the enterprise telephony deployment. However, for dual-mode client devices, Cisco recommends normalizing required dialing strings so that user mobile device dialing habits are maintained whether the device is connected to the enterprise network and registered to Unified CM or not. Because dialing on the mobile voice network is typically done using full E.164 (with or without a preceding '+') and mobile phone contacts are typically stored with full E.164 numbers, Cisco recommends configuring the enterprise dial plan to accommodate full E.164 or full E.164 with preceding '+' for dual-mode client devices. When the dial plan is configured within Unified CM to handle this type of outbound dialing for dual-mode phones, it is possible for users to store a single set of contacts on the phone in the E.164 format and, when dialed from these contacts or manually using the full E.164 number, calls will always be routed to the appropriate destination, whether the device is connected to the enterprise network directly or over a secure remote connection and registered to Unified CM or connected only to the mobile voice network. Configuring the enterprise dial plan in this manner provides the best possible end-user dialing experience so that users' mobile device dialing habits are maintained and they do not have to be aware of whether the device has enterprise connectivity and is registered to Unified CM.

To achieve normalized dialing from dual-mode phones, whether connected to the enterprise or just to the mobile voice network, configure the dial plan within Unified CM with the following considerations in mind:

- Ensure that the enterprise dial plan is capable of handling dial strings from dual-mode phones typically used on the mobile voice network. For example, the dial plan should be configured to handle the following strings, which might be dialed from a mobile phone to reach a particular phone through the mobile voice network: +1 408 555 1234, 408 555 1234.
- For calls destined for other enterprise numbers, systems configured for abbreviated dialing should be capable of modifying dial strings and rerouting to enterprise extensions as appropriate. For example, assuming the enterprise dial plan is based on five-digit internal dialing, the system should be configured to handle call routing to an enterprise extension so that a call made to +1 408 555 1234 or 408 555 1234 is modified and rerouted to 51234 if the call is made while the dual-mode device is registered to Unified CM.
- Ensure that all inbound calls to the enterprise destined for dual-mode devices have the calling number and/or caller ID prefixed with appropriate digits so that missed, placed, and received call history lists are in full E.164 formats. This will allow dual-mode device users to dial from call history lists without the need for editing the dial string. Instead, users will be able to select a number from the call history list to redial, whether connected to the enterprise or not. For example, if an incoming call from inside the enterprise originates from 51234 to a dual-mode user's enterprise number and the call goes unanswered, Unified CM should be configured to manipulate the calling number so that the resulting entry within the history list of the dual-mode device shows either 408 555 1234 or + 1 408 555 1234. This number can be dialed without the need for further manipulation, whether the dual-mode device is connected to the enterprise or just to the mobile voice network.

The one exception to normalized dialing for dual-mode devices is for scenarios in which some enterprise extensions or phones are reachable only internally (that is, they have no externally reachable corresponding DID number). In these situations, non-externally reachable numbers can be dialed (manually or from contacts) using abbreviated formats. Because these numbers will never be available externally and can be dialed only from inside the enterprise, some sort of enterprise-only indication should be made when storing these numbers in the contact list. Further, incoming calls from these internal-only numbers should not have the calling number modified for call history lists because these numbers may be called only inside the enterprise. Instead, calls from these extensions should be listed in all call history lists without modification so that the abbreviated dial strings can be successfully dialed only while the device is connected to the enterprise and registered to Unified CM.

Emergency Services and Dialing Considerations

Dual-mode phones do present a slight challenge when it comes to making calls to emergency service numbers such as 911, 999, and 112. Because the dual-mode device may be located inside or outside the enterprise, providing location information for a dual-mode phone and its user in the event of an emergency must be considered. Dual-mode mobile devices with cellular voice radios receive location services from their provider networks, and these location services are always available when the device is connected and typically are able to pinpoint locations far more precisely than enterprise wireless networks; therefore Cisco recommends that dual-mode device users rely on the mobile voice network for making emergency calls and determining device and user location. To ensure that dual-mode client devices rely exclusively on the mobile provider voice network for emergency and location services, these clients force all calls made to numbers configured in the Emergency Numbers field on the mobile client device configuration page to route over the mobile voice network. Further, dual-mode phone users should be advised to make all emergency calls over the mobile voice network rather than the enterprise network.

Enterprise Caller ID

When dual-mode devices are connected to the enterprise and registered to Unified CM, all calls made with the enterprise line over the WLAN or mobile data network are routed with the user's enterprise number as caller ID. This ensures that returned calls made from call history lists at the far-end are always routed through the enterprise because the return call is to the user's enterprise number. If the dual-mode user has been enabled for Cisco Unified Mobility, and Mobile Connect is turned on for the mobile number, return calls to the enterprise number would also be extended to the dual-mode device through the PSTN whenever it is not connected to the enterprise.

Mid-Call Features

When dual-mode phone clients are connected to the enterprise and registered to Unified CM as enterprise endpoints, they are able to invoke call processing supplementary services such as hold, resume, transfer, and conference, using call signaling methods as supported by Unified CM. Just as with any IP phone or client registered to Unified CM, these devices are able to leverage enterprise media resources such as music on hold (MoH), conference bridges, media termination points, and transcoders.

External Call Routing

When the dual-mode device is not connected to the enterprise and is not registered to Unified CM, it may make and receive calls only through the mobile voice network. For this reason, Unified CM has no visibility into any calls being made or received at the dual-mode mobile device while it is unregistered. The mobile number is the caller ID being sent to the network when calls are made from dual-mode phones not connected to the enterprise. This will likely result in unanswered calls being made directly back to the dual-mode device's mobile number instead of being routed back through the enterprise.

If the dual-mode phone is integrated with Cisco Unified Mobility, enterprise two-stage dialing services may be leveraged for making calls through the enterprise network even when the dual-mode device is outside the enterprise and not registered to Unified CM. Unified Mobility two-stage dialing is done using either Mobile Voice Access or Enterprise Feature Access and requires the user to dial an enterprise system access DID number and enter credentials prior to dialing the number they are calling. For more information on Unified Mobility two-stage dialing features, see Mobile Voice Access and Enterprise Feature Access, page 25-49.

Likewise, if the dual-mode phone is integrated with Unified Mobility, a user can also receive incoming calls to their enterprise number at the mobile number through Mobile Connect; can invoke mid-call features using DTMF key sequences including hold, resume, transfer, and conference; and can perform desk phone pickup to move an active call from the mobile phone to the enterprise desk phone.

Remote Secure Enterprise Connectivity

Dual-mode client devices can utilize the IP telephony infrastructure for enterprise VoIP calling even when outside the enterprise, provided they have a secure connection back to the enterprise in order to register the client with Unified CM. Remote secure connectivity for these devices requires the use of a VPN solution such as Cisco AnyConnect or the Cisco Jabber secure connect feature in order to secure the client connection over the Internet.

Voice quality and user experience for remotely attached dual-mode client devices will vary depending on the nature of the Internet-based network connection. Cisco cannot guarantee acceptable voice quality nor successful connectivity for these types of client connections. Care should be taken when relying on these types of connections for business-critical communications. In the case of unreliable or low-bandwidth Internet connections, users should be advised to make calls over the mobile voice network rather than relying on the enterprise telephony infrastructure.

Additional Services and Features

In addition to call processing or call control services, dual-mode phones and clients are capable of providing the additional features and services described in this section.

Dual-Mode Call Handoff

One very important aspect of dual-mode phone deployments is call preservation as a user moves in and out of the enterprise and network connectivity changes from the cellular voice radio to the WLAN radio, and vice versa. Because dual-mode phone users are often mobile, it is important to maintain any active call as a dual-mode user moves in or out of the enterprise. For this reason, dual-mode clients and the underlying enterprise telephony network should be capable of some form of call handoff.

There are two types of call handoff that should be accommodated by both the dual-mode client and the underlying IP telephony infrastructure:

- Hand-out

  Call hand-out refers to the movement of an active call from the WLAN or mobile data network interface of the dual-mode phone to the cellular voice interface of the dual mode phone. This requires the call to be handed out from the enterprise IP network to the mobile voice network through the enterprise PSTN gateway.

- Hand-in

  Call hand-in refers to the movement of an active call from the cellular voice interface of the dual mode phone to the WLAN or mobile data network interface of the dual mode phone. This requires the call to be handed in from the mobile voice network to the enterprise IP network through the enterprise PSTN gateway.

The handoff behavior of a dual-mode phone depends on the nature of the dual-mode client and its particular capabilities. Some dual-mode clients are capable of providing only manual handoff, while other clients are able to invoke handoff automatically based on network conditions. In manual handoff scenarios, the dual-mode users are responsible for engaging and completing the handoff operation based on their location and needs. With automatic handoff, the dual-mode client monitors the WLAN signal and makes handoff decisions based on strengthening or weakening of the WLAN signal at the client. Hand-out is engaged in the case of a weakening WLAN signal, while hand-in is engaged in the case of a strengthening WLAN signal. Automatic handoff depends on the mobile device to provide capabilities for monitoring WLAN signal strength.

Handoff operations are critical for maximizing utilization of the enterprise IP telephony infrastructure for phone calls. These operations are also necessary for providing voice continuity and good user experience so that users do not have to hang up the original call and make another call to replace it.

Corporate Directory Access

Some dual-mode clients are capable of accessing enterprise directory services, including directory lookups and personal contact lists. While this is not a required feature for dual-mode devices and clients, it does provide productivity improvements for dual-mode phone users when they are able to access corporate directory information from their mobile device.

Enterprise Voicemail Services

Many dual-mode clients are also capable of accessing enterprise voicemail services. Most dual-mode clients are capable of receiving enterprise message waiting indication whenever an unread voicemail is in the user's enterprise voicemail box and the dual-mode phone is connected to the enterprise network. Further, dual-mode clients can be used to retrieve enterprise voicemail messages. Typically enterprise voicemail messages are retrieved when the user dials the voicemail system number and navigates to their voicemail box after providing required credentials. However, some dual-mode clients provide the ability to retrieve voicemail messages from the voicemail box by downloading and displaying a list of all

messages in the voicemail box and then by selecting individual messages to be downloaded to the dual-mode phone for listening. This is sometimes referred to as visual voicemail. Both the dual-mode phone client and the enterprise voicemail system must be capable of providing and receiving message waiting indication (MWI), voicemail message information, and downloads of the messages over the network. Cisco Unity Connection supports visual voicemail through IMAP, and it can provide MWI and voicemail lists and downloads, but only if the mobile client also supports this functionality.

Dual-Mode Clients: Cisco Mobile and Cisco Jabber

This section describes characteristics and deployment considerations for Cisco Mobile and Cisco Jabber.

Cisco Mobile

Cisco Mobile is a dual-mode client for the Apple iPhone. Once the client application is downloaded from the Apple Application Store and installed on the iPhone using iTunes, the iPhone can associate to the enterprise WLAN network and register to Unified CM as a SIP enterprise phone.

To provide registration and call control services to the Cisco Mobile dual-mode iPhone client, the device must be configured within Unified CM as a **Cisco Dual Mode for iPhone** device type. Next the iPhone must be configured to access the enterprise WLAN for connectivity based on the enterprise WLAN infrastructure and security policies. Once the iPhone has been configured to access the WLAN, when the Cisco Mobile client is launched, it will register the device to Unified CM.

To integrate to Unified Mobility and to leverage handoff functionality, the mobile number of the iPhone must be configured as a mobility identity associated to the Cisco Dual-Mode for iPhone device within Unified CM.

The Cisco Mobile 8.0 client is supported on iPhone models 3G, 3GS, and 4 running firmware version 3.0.1 or later. The iPhone WLAN interface supports 802.11b and 802.11g network connectivity.

Note When deploying iPhone 3GS and 4 devices, use the Cisco Jabber for iPhone client rather than the Cisco Mobile 8.0 client. The Cisco Jabber for iPhone client provides support for multitasking or backgrounding of the application and provides a superior user experience. The iPhone 3G is supported only with Cisco Mobile 8.0.

The Cisco Mobile client not only provides dual-mode phone services but also provides directory lookup services when configured to access the enterprise Microsoft Active Directory and provides visual voicemail services when configured to access the user's voicemail box on Cisco Unity Connection.

Note When simultaneously deploying both Cisco Mobile and the Cisco Unified Mobile Communicator client for the iPhone, Cisco Mobile should not be configured to access the user's enterprise voicemail box. Instead, the Cisco Mobile client should be used for visual voicemail access because it provides more features and a superior user experience.

The Cisco Mobile client is capable of performing only manual hand-out as described in the section on Cisco Mobile and Cisco Jabber Handoff, page 25-76.

For more information about the Cisco Mobile dual-mode iPhone client, additional feature details, and supported hardware and software versions, refer to the Cisco Unified Mobile Communicator documentation available at

http://www.cisco.com/en/US/products/ps7271/tsd_products_support_series_home.html

Cisco Jabber

Cisco Jabber is a dual-mode client for Android, iPhone, and other Apple iOS mobile devices. Once the client application is downloaded from the appropriate store or market (Apple Application Store or Google Play, formerly Android Market) and installed on the Apple iOS or Android device, it can connect to the enterprise network and register to Unified CM as a SIP enterprise phone.

To provide registration and call control services to the Cisco Jabber dual-mode Android or iPhone client, the device must be configured within Unified CM as a **Cisco Dual Mode for Android** or **iPhone** device type. Next, the mobile device must be configured to access the enterprise WLAN for connectivity based on the enterprise WLAN infrastructure and security policies. Alternatively the mobile device can be connected to the enterprise network through the mobile data network or over non-enterprise WLANs. Once the mobile device has been configured to access the enterprise network, if the Cisco Jabber client is launched, it will register the device to Unified CM. To integrate to Unified Mobility and to leverage handoff functionality, the mobile number of the Android or iPhone must be configured as a mobility identity associated to the Cisco Dual-Mode for Android or iPhone device within Unified CM.

The Cisco Jabber client is supported on the following devices:

- Android

  Samsung Galaxy S International, Samsung Galaxy Tab International, and Samsung Galaxy S2. These devices must be running a minimum firmware version of 2.2.1. Although not officially supported, Cisco Jabber for Android runs on many Android devices running version 2.2 and later with various degrees of limitations depending on the device. The WLAN interfaces of most Android devices support 802.11b, 802.11g, and 802.11n network connectivity.

- Apple iOS

  iPhone 3GS, 4, and 4S; iPod Touch 3rd and 4th generation; and iPad and iPad 2. These devices must be running a minimum iOS version of 5.0. The WLAN interfaces of Apple iOS devices support 802.11b, 802.11g, and 802.11n network connectivity.

For details on the latest specific device and firmware version support, refer to the product release notes for:

- Android

  http://www.cisco.com/en/US/products/ps11678/prod_release_notes_list.html

- iPhone

  http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html

The Cisco Jabber client not only provides voice over IP (VoIP) phone services but also provides directory lookup services when configured to access the enterprise LDAP directory and provides enterprise voicemail message waiting indication (MWI) and message count or visual voicemail when integrated to Cisco Unity Connection.

The Cisco Jabber client is capable of performing only manual hand-out as described in the section on Cisco Mobile and Cisco Jabber Handoff, page 25-76.

For more information about the Cisco Jabber dual-mode Android and iPhone clients, additional feature details, and supported hardware and software versions, refer to the Cisco Jabber documentation for:

- Android

  http://www.cisco.com/en/US/products/ps11678/tsd_products_support_series_home.html

- iPhone

  http://www.cisco.com/en/US/products/ps11596/tsd_products_support_series_home.html

Cisco Mobile and Cisco Jabber Handoff

To properly deploy Cisco dual-mode clients such as Cisco Mobile and Cisco Jabber, it is important to understand the nature of handoff operations within the client. The handoff method used by the Cisco Mobile and Cisco Jabber dual-mode client depends on the **Transfer to Mobile Network** setting on the Cisco Dual-Mode for iPhone or Cisco Dual-Mode for Android device configuration page.

There are two methods of handoff, depending on the Transfer to Mobile Network setting:

- Mobility Softkey Method of Hand-Out, page 25-76

  With this method the Transfer to Mobile Network setting should be set to **Use Mobility Softkey (user receives call)**. In this type of handoff, the Unified CM system generates a call over the PSTN to the user's mobile number. This hand-out method is supported with both Cisco Mobile and Cisco Jabber dual-mode clients.

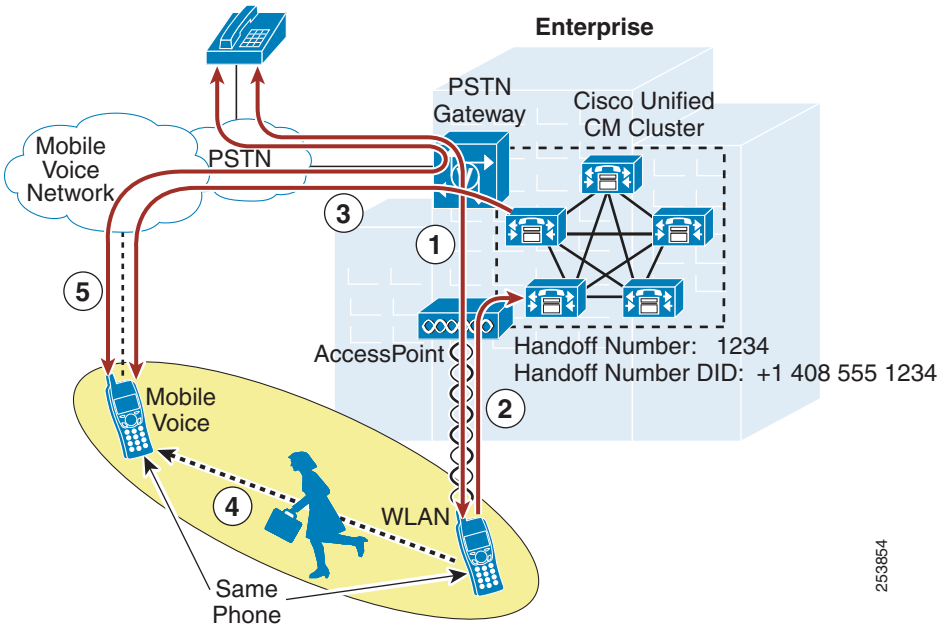
- Handoff Number Method of Hand-Out, page 25-77

  With this method the Transfer to Mobile Network setting should be set to **Use HandoffDN Feature (user places call)**. In this type of handoff, the dual-mode client generates a call over the mobile voice network to the handoff number configured within the Unified CM system. This hand-out method is supported only with iPhone dual-mode clients.

Mobility Softkey Method of Hand-Out

The operation depicted in Figure 25-26 is of an active call on an iPhone or Android dual-mode device within the enterprise being moved manually from the WLAN interface to the mobile voice network or cellular interface of the device through the enterprise PSTN gateway. As shown, there is an existing call between the dual-mode device associated to the enterprise WLAN and registered to Unified CM, and a phone on the PSTN network (step 1). Because this is a manual process, the user must select the Use Mobile Network button from the in-call menu within the Cisco Mobile or Cisco Jabber dual-mode client, which signals to Unified CM the intention to hand-out the call (step 2). Next Unified CM generates a call to the configured mobility identity number corresponding to this dual-mode device through the enterprise PSTN gateway (step 3). This call to the mobility identity is made to the mobile voice network or cellular interface of the iPhone or Android device. The user can now move out of the enterprise and away from WLAN network coverage (step 4). In the meantime, the inbound call from Unified CM is received at the mobile voice network interface, and the user must answer the call manually to complete the hand-out. Once the inbound call on the cellular interface is answered, the RTP stream that was traversing the WLAN is redirected to the PSTN gateway, and the call continues uninterrupted between the dual-mode client and the original PSTN phone with the call anchored in the enterprise gateway (step 5).

Figure 25-26 Cisco Mobile or Cisco Jabber Dual-Mode Hand-Out (WLAN-to-Mobile Voice Network): Mobility Softkey Method



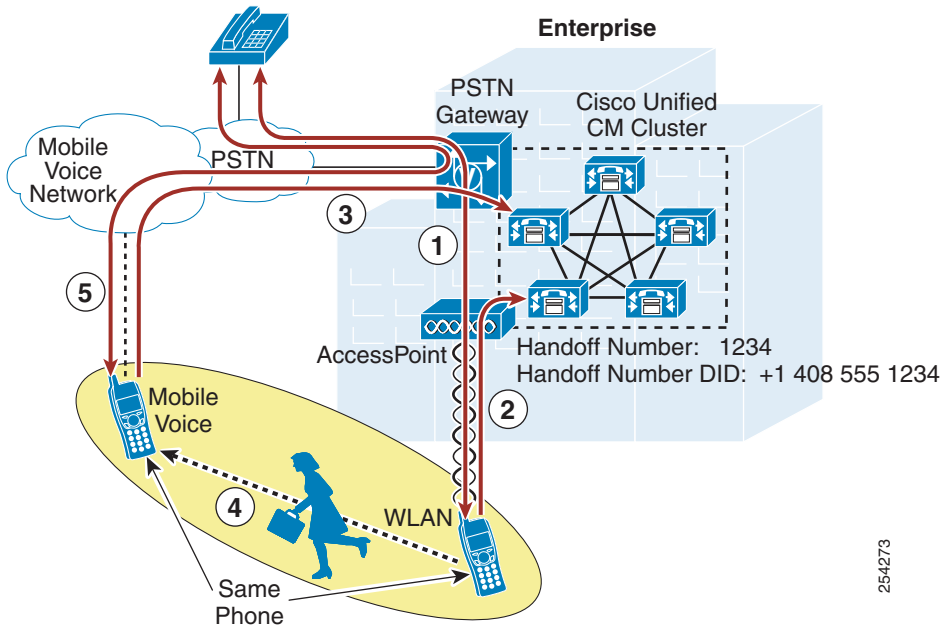
Handoff Number Method of Hand-Out

Figure 25-27 illustrates the same hand-out operation as in Figure 25-26, where an active call on an iPhone dual-mode phone within the enterprise is moved manually from the WLAN interface to the mobile voice network or cellular interface of the device through the enterprise PSTN gateway. However, in this case the Handoff Number method of hand-out is used.

Note The Handoff Number method of hand-out is supported only with iPhone dual-mode clients.

As shown in Figure 25-27, there is an existing call between the iPhone dual-mode device associated to the enterprise WLAN and registered to Unified CM, and a phone on the PSTN network (step 1). Because this is a manual process, the user must select the Use Mobile Network button from the in-call menu within the Cisco Mobile dual-mode client, which signals to Unified CM the intention to hand-out the call (step 2). Next the Cisco Mobile client automatically generates a call through the cellular interface over the mobile voice network to the configured Handoff Number within the Unified CM system (step 3). The user can now move out of the enterprise and away from WLAN network coverage (step 4). In the meantime, the inbound call from the Cisco Mobile client is received by Unified CM. Assuming the inbound calling number matches the user's configured mobility identity, the RTP stream that was traversing the WLAN is redirected to the PSTN gateway, and the call continues uninterrupted between the Cisco Mobile dual-mode client and the original PSTN phone, with the call anchored in the enterprise gateway (step 5).

Figure 25-27 Cisco Mobile Dual-Mode Hand-Out: Handoff Number Method



Note The Handoff Number method of hand-out requires that Unified CM receive an inbound calling number from the PSTN network that matches the mobility identity number configured under the Cisco Dual Mode for iPhone device attempting the hand-out. If the caller ID is not sent by the iPhone, if the PSTN provider does not send the inbound caller ID to the enterprise, or if the inbound caller ID does not match the user's configured mobility identity, the hand-out operation will fail.

Note Cisco Mobile and Cisco Jabber dual-mode clients do not support hand-in. In scenarios where an in-progress call is active between the dual-mode mobile voice network or cellular interface and an enterprise phone (or a PSTN phone with the call anchored in the enterprise gateway), the only way to move the call to the WLAN interface of the dual-mode device is to hang up the call and redial once the dual-mode client has connected to the enterprise network and registered to Unified CM.

Cisco Mobile and Jabber for iPhone Desk Phone Integration

The Cisco Mobile or Jabber iPhone Dual-Mode client enables the user to move an active or held call from the user's desk phone to the dual-mode device. This feature relies on CTI monitoring of the primary line of the user's desk phone as well as the call park feature.

The functionality provided by desk phone integration relies on active CTI monitoring of the primary line of the user's desk phone. Whenever an active or held call is sensed by the Cisco Mobile or Jabber client, it prompts the user as to whether they want to transfer the call to the dual-mode device. If the user indicates they wish to transfer the call, the desk phone automatically parks the call and the dual-mode client automatically retrieves the call from the park number.

To enable desk phone integration, ensure that the user's end-user account is assigned to a CTI-enabled user group and that the user's desk phone is enabled to allow CTI control. In addition, the CTI Control Username field on the **Cisco Dual Mode for iPhone** device must be configured with the user's end-user account userID.

Cisco Jabber for Android Desk Phone Integration

The Cisco Jabber for Android dual-mode client enables the user to move an active call from the Android device to the IP desk phone sharing a line with the dual-mode device. This feature is invoked by placing the active call on hold through the Cisco Jabber client. When the call is placed on hold, the call can be resumed at either the shared-line IP desk phone or on the Cisco Jabber client.

WLAN Design Considerations for Cisco Mobile and Cisco Jabber Dual-Mode Clients

Consider the following WLAN guidelines when deploying Cisco Mobile and Cisco Jabber dual-mode clients:

- Whenever possible, ensure that Cisco Mobile and Cisco Jabber dual-mode clients roam on the WLAN only at Layer 2 so that the same IP address can be used on the WLAN interface of the dual-mode device. In Layer 3 roaming scenarios where subnet boundaries are crossed due to device IP address changes, calls will be dropped.
- Deploy Cisco Mobile and Cisco Jabber dual-mode clients on a WLAN network where the same SSID is used across APs. Roaming between APs is much slower if SSIDs are different.
- Ensure all APs in the WLAN broadcast their SSID(s). If the SSID is not broadcast by the AP, the user may be prompted by the device to join other Wi-Fi networks or the device may automatically join other Wi-Fi networks. When this occurs the call is interrupted.

Interactions Between Cisco Mobile or Cisco Jabber and Cisco Unified Mobility

The Cisco Mobile and Cisco Jabber dual-mode clients can be integrated with Cisco Unified Mobility to leverage Cisco Mobile Connect, mid-call DTMF features, two-stage dialing, and single enterprise voicemail box mobile voicemail avoidance.

Integration with Unified Mobility requires the iPhone or Android dual-mode mobile phone number to be configured within Unified CM as a mobility identity associated with the Cisco Dual Mode for iPhone or Cisco Dual Mode for Android device. Once the mobile number is configured as a mobility identity within the system, Mobile Connect can be leveraged so that incoming calls to the user's enterprise number will be extended to the iPhone or Android dual-mode device through the mobile voice network as long as the iPhone or Android dual-mode device is not connected to the enterprise and not registered to Unified CM. In situations where the dual-mode device is connected to the enterprise and registered to Unified CM, an inbound call to the enterprise number will not be extended to the mobile voice network interface of the device. When the iPhone or Android dual-mode device is connected to the enterprise, only the WLAN or mobile data interface of the device will receive the inbound call. This prevents unnecessary consumption of enterprise PSTN gateway resources.

When not connected to the enterprise and not registered to Unified CM, the iPhone or Android dual-mode device can invoke mid-call features by means of DTMF and perform desk phone pickup for any enterprise anchored call. The dual-mode device can also leverage Mobile Voice Access and Enterprise Feature Access two-stage dialing features when making outbound calls to route these calls through the enterprise and anchor them in the enterprise PSTN gateway.

In addition to configuring a mobility identity for the iPhone or Android dual-mode device, you can configure additional mobile phone numbers or off-system phone numbers as remote destinations and associate them to the Cisco Dual Mode for iPhone or Cisco Dual Mode for Android device within Unified CM. When associating the mobility identity and additional remote destinations to the dual-mode device, you do not have to configure a remote destination profile.

For more information about the Cisco Unified Mobility feature set as well as design and deployment considerations, see Cisco Unified Mobility, page 25-38.

Cisco AnyConnect and Secure Connect

The Cisco AnyConnect mobile client and Cisco Jabber secure connect feature provide secure remote connectivity capabilities for Cisco Jabber mobile device clients, enabling connectivity over mobile data networks and non-enterprise WLANs. The Cisco AnyConnect mobile client can be downloaded from the Apple Application Store or Google Play (formerly Android Market). This client application provides SSL VPN connectivity for Apple iOS and Android mobile devices through the Cisco AnyConnect VPN solution available with the Cisco Adaptive Security Appliance (ASA) head-end.

Cisco secure connect is a Cisco Jabber mobile client feature that uses the same Cisco AnyConnect solution ASA head-end infrastructure and provides application-level SSL secure connectivity without requiring a separate Cisco AnyConnect client application. This feature enables secure connectivity for the Cisco Jabber mobile client application without securing the whole mobile device. This ensures that only Cisco Jabber traffic traverses the enterprise network while all other traffic traverses the public or private WLAN or mobile data network.

When employing VPN network connectivity for connections over the mobile data network or public or private Wi-Fi hot spots, it is important to deploy a high-bandwidth secure VPN infrastructure that adheres to the enterprise's security requirements and policies. Careful planning is needed to ensure that the VPN infrastructure provides high bandwidth, reliable connections, and appropriate session or connection capacity based on the number of users and devices using this connectivity.

For more information on secure remote VPN connectivity solutions, including Cisco AnyConnect, refer to the secure mobility documentation available at

http://www.cisco.com/en/US/products/hw/vpndevc/products.html#mobi

For information on the Cisco Jabber secure connect feature, refer to the *Cisco Jabber Secure Connect Deployment Guide*, available at

http://www.cisco.com/en/US/products/ps11678/products_implementation_design_guides_list.html

Dual-Mode Clients: Nokia Call Connect

Note End-of-Sale for the Nokia Call Connect client is July 10, 2012. There is no replacement mobile client for Nokia mobile devices. For more information, see the End-of-Sale (EoS) and End-of-Life (EoL) announcement at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7290/ps10589/end_of_life_notice_c51-696647.html.

Nokia Call Connect is a dual-mode client for Nokia mobile smart phones. Once installed on the Nokia device, the client can associate to the enterprise WLAN network and register to Unified CM as a Skinny Client Control Protocol (SCCP) enterprise phone.

To provide registration and call control services to Nokia dual-mode devices, Unified CM must support the Nokia S60 device type, which is available only after loading the Nokia-provided Cisco options package (COP) file onto Unified CM.

Once the dual-mode device has been configured within Unified CM, it is necessary to load the Nokia Call Connect client onto the Nokia device. This can be done using a computer with a USB, Bluetooth, or infrared port running the Nokia PC Suite. After the Nokia Call Connect Symbian installation system (SIS) file has been loaded on the Nokia device, the device must be configured to access the enterprise WLAN for connectivity based on the enterprise WLAN infrastructure and security policies. Once the handset has been configured to access the WLAN, when the Nokia Call Connect client is launched, it will register the device to Unified CM. To integrate the Nokia dual-mode device with Unified Mobility so the user can leverage features such as Mobile Connect, configure the Nokia mobile phone number as a mobility identity and associate it to the Nokia S60 device within Unified CM.

Note Cisco recommends configuring the Nokia Call Connect client SCCP registration setting to **Always On** to ensure that, whenever the Nokia device is associated to the enterprise WLAN network, it will attempt to register to Unified CM. Cisco also recommends setting the Nokia dual-mode phone's preferred or default call type setting to **Internet Call** to ensure that, when the Nokia Call Connect client is registered to Unified CM, the device will always attempt to route outbound calls through the WLAN interface of the dual-mode phone. These recommended settings ensure that the Nokia dual-mode phone maximizes its use of the enterprise IP telephony infrastructure for making and receiving business calls.

The Nokia Call Connect 2.2 client is supported on Nokia Symbian 3 handsets (including Nokia C7, E6, and N8) and Nokia S60 3.2 handsets (including Nokia E52, E55, E72, and E75). Nokia S60 3.1 handsets, including the E51, E61i, E63, E66, E71, and E90, are also supported but might not support advanced features such as automatic handoff. Nokia mobile phone WLAN interfaces support 802.11b, 802.11g, and in some cases 802.11n network connectivity.

The Nokia Call Connect client not only provides dual-mode phone services but also provides directory lookup services when configured to access the Unified CM directory as well as enterprise-based XML phones services like those supported on Cisco IP desk phones.

Nokia Call Connect 2.0 and later clients are capable of performing automatic hand-out and hand-in as outlined in the sections below.

For more information about the Nokia Call Connect dual-mode client, supported handsets, and software versions, and to access the latest client and COP file, refer to:

http://www.cisco.com/en/US/products/ps10589/tsd_products_support_series_home.html

Nokia Call Connect Dual-Mode Handoff

To properly deploy Nokia Call Connect dual-mode clients, it is necessary to understand the nature of the handoff operation within the Nokia dual-mode client.

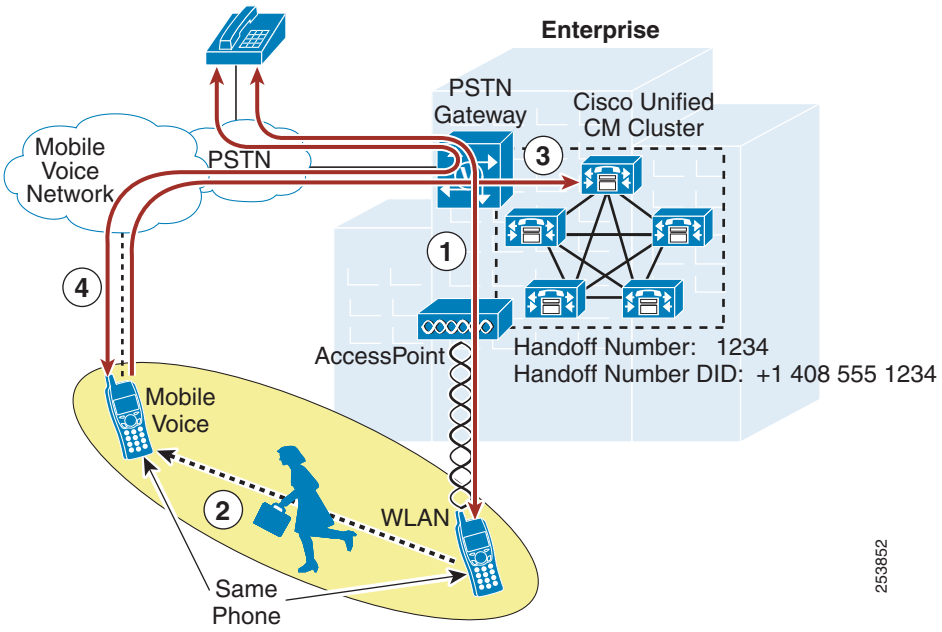
In the following examples, the handoff number is +1 408 555 1234 (this is the full E.164 handoff number). The Cellular Handover Number under the Nokia Call Connect Voice Call Continuity (VCC) settings is configured with this number.

All inbound calls are stripped to four digits by the upstream gateway, so the Handoff Number configured within Unified CM is 1234. The VoIP Handover Number is configured as 1234 under the Nokia Call Connect VCC settings.

Hand-Out (WLAN to Cellular)

Figure 25-28 shows a hand-out operation in which an active call on a Nokia dual-mode phone within the enterprise is moved from the WLAN interface to the mobile voice network or cellular interface of the device through the enterprise PSTN gateway. As shown, there is an existing call between the Nokia dual-mode device associated to the enterprise WLAN and registered to Unified CM, and a phone on the PSTN network (step 1). The Nokia dual-mode user begins to leave the enterprise (step 2), and as the WLAN signal strength drops below -78 dBm (default value for the WLAN HO threshold setting in VCC) for a period of 1,000,000 microseconds (1 second, default value for the WLAN HO hysteresis setting in VCC), a silent background call is opened to +1 408 555 1234 (the configured Cellular Handover Number in VCC and corresponding to the Handoff Number configured in Unified CM) over the mobile voice network and PSTN into the enterprise PSTN gateway and is delivered to Unified CM (step 3). Once received, the calling number is checked against all configured mobility identities on the system, and assuming a match is found, the RTP stream that was traversing the WLAN is now redirected to the PSTN gateway and the call is continued uninterrupted between the dual-mode device and the original PSTN phone with the call anchored in the enterprise gateway (step 4).

Figure 25-28 Nokia Call Connect Dual-Mode Hand-Out (WLAN-to-Mobile Voice Network)

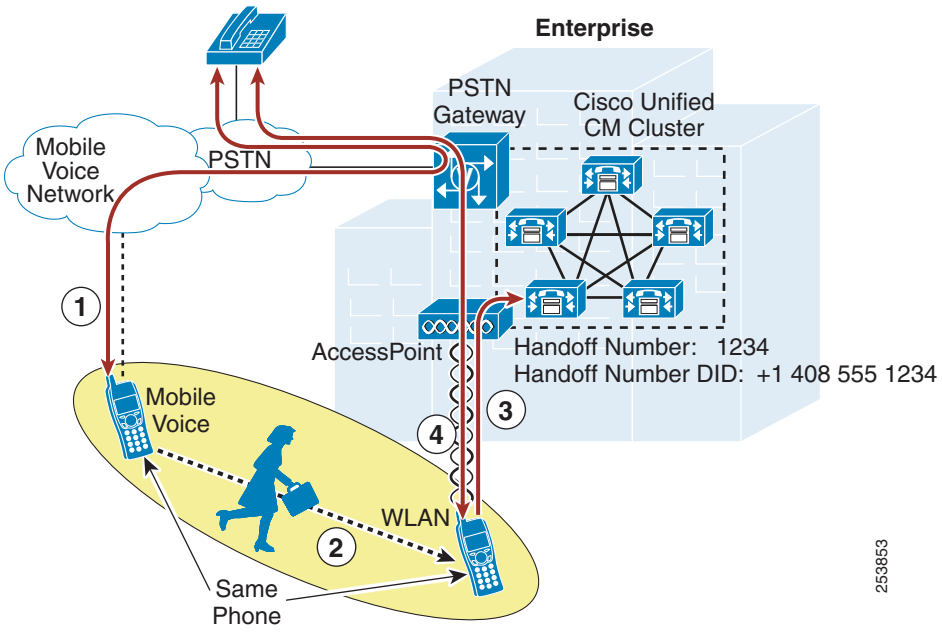


The Nokia Call Connect dual-mode client also supports manual hand-out using the Switch to Cellular or Handover to GSM in-call menu options. The availability and behavior of these manual hand-out methods depends on the device type and firmware version. For devices running firmware version 3.1 and earlier, the Switch to Cellular menu option when selected performs a blind transfer of the active call to the mobile voice network interface of the device through the enterprise PSTN gateway. For devices running firmware version 3.2 and later, the Handover to GSM menu option when selected performs a manual handoff using the Unified CM Handoff Number as shown in step 3 of Figure 25-28 without relying on WLAN handover thresholds and hysteresis VCC settings.

Hand-In (Cellular to WLAN)

Figure 25-29 depicts a hand-in operation in which an active call on a Nokia dual-mode phone outside the enterprise is moved from the mobile voice network interface to the WLAN interface of the device through the enterprise PSTN gateway. As shown, there is an existing call between the Nokia dual-mode device on the mobile voice network and a phone on the PSTN network (step 1). The Nokia dual-mode user moves into the enterprise (step 2), and the device associates in the background to the WLAN infrastructure and registers to Unified CM. After registration, the device will wait for the amount of time specified by the WLAN HO hysteresis high setting in VCC (60 seconds by default), and then a silent background call is opened to 1234 (the configured VoIP Handover Number in VCC, which corresponds to the Unified CM Handoff Number configured in Unified CM) and delivered to Unified CM (step 3). Once received, the enterprise calling number is checked against configured Nokia S60 dual-mode phones on the system, and assuming a match is found, the call that was traversing the mobile voice network/PSTN and the enterprise PSTN gateway is now redirected to the WLAN network, and the call is continued uninterrupted between the dual-mode device and the original PSTN phone (step 4).

Figure 25-29 Nokia Call Connect Dual-Mode Hand-In (Mobile Voice Network-to-WLAN)



WLAN Design Considerations for Nokia Call Connect Dual-Mode Client

Consider the following WLAN guidelines when deploying Nokia Call Connect dual-mode clients:

- Leave the **WLAN HO Threshold** setting under Voice Continuity Configuration (VCC) at default setting (73 for Nokia Call Connect 2.1 and later) unless users are experiencing delayed automatic handoff when leaving the WLAN coverage area.
- The **WLAN HO Threshold** can be adjusted lower to engage automatic handoff more quickly when users leave the WLAN coverage area.
- Adjusting the **WLAN HO Threshold** also affects trigger thresholds for roaming between WLAN Access Points (APs). Lowering the **WLAN HO Threshold** setting also lowers the AP-to-AP roaming threshold, resulting in faster AP-to-AP roaming. If users are experiencing poor voice quality on the WLAN or if AP-to-AP roaming is too slow, consider adjusting this setting lower, but be aware that automatic handoff will also engage more quickly when this value is lowered.

For more information about Nokia Call Connect VCC settings, refer to the *Nokia Call Connect for Cisco User's Guide*, available at

http://europe.nokia.com/support/download-software/nokia-call-connect-for-cisco

Interactions Between Nokia Call Connect and Cisco Unified Mobility

The Nokia Call Connect dual-mode client can be integrated with Cisco Unified Mobility to leverage Cisco Mobile Connect, mid-call DTMF features, two-stage dialing, single enterprise voicemail box, and desk phone pickup.

Integration with Unified Mobility requires the Nokia dual-mode phone mobile number to be configured within Unified CM as a mobility identity associated with the Nokia S60 device. Once the mobile number is configured as a mobility identity within the system, Mobile Connect can be leveraged so that incoming calls to the user's enterprise number will be extended to the Nokia dual-mode device through the mobile voice network as long as the Nokia dual-mode device is outside the enterprise and is not registered to

Unified CM. In situations where the Nokia dual-mode device is inside the enterprise and registered to Unified CM, an inbound call to the enterprise number will not be extended to the mobile voice network interface of the device. When the Nokia dual-mode device inside the enterprise, only the WLAN interface of the device will receive the inbound call. This prevents unnecessary consumption of enterprise PSTN gateway resources.

When outside the enterprise and not registered to Unified CM, the Nokia dual-mode device can invoke mid-call features by means of DTMF and can perform desk phone pickup for any enterprise anchored call. The Nokia Call Connect 2.1 and later client provides automation of the Cisco Enterprise Feature Access two-stage dialing feature for scenarios when the user is outside the enterprise and wishes to make outbound calls through the enterprise in order to anchor them in the enterprise PSTN gateway. For information about Enterprise Feature Access two-stage dialing, see Enterprise Feature Access with Two-Stage Dialing Functionality, page 25-53.

When the Two-Stage Dialing feature of the Nokia Call Connect client is enabled, all calls made by the device over the cellular interface will leverage the Enterprise Feature Access two-stage dialing functionality within Unified CM. The configured **Two-stage dialing no.** setting within the Nokia Call Connect client determines the number the client will dial for all outbound cellular calls. This configured number should correspond to the Enterprise Feature Access number on the Unified CM system. The configured **Two-stage dialing PIN** setting within the Nokia Call Connect client determines the authentication key sequence sent to Unified CM once the call to the Enterprise Feature Access number is connected. This configured PIN should correspond to the user's PIN as configured under the end-user account within Unified CM. The Nokia Call Connect client uses these two settings as well as the number the user dialed or selected to facilitate the two-stage dialed call.

Note Enterprise Feature Access two-stage dialing automation is available with only Nokia S60 3.2 firmware versions.

Alternatively, the Nokia dual-mode user can leverage the manual IVR-based Mobile Voice Access two-stage dialing feature to dial calls through the enterprise and anchor those calls in the enterprise gateway.

If the Nokia device is also running the Cisco Unified Mobile Communicator client, then the user should leverage the Dial-via-Office feature available with that client rather than the Enterprise Feature Access or Mobile Voice Access two-stage dialing methods because the user experience with Dial-via-Office is far superior.

In addition to configuring a mobility identity for the Nokia dual-mode device, you can configure additional mobile phone numbers or off-system phone numbers as remote destinations and associate them to the Nokia S60 device within Unified CM. When associating the mobility identity and additional remote destinations to the Nokia device, you do not have to configure a remote destination profile.

For more information about the Unified Mobility feature set as well as design and deployment considerations, see Cisco Unified Mobility, page 25-38.

High Availability for Dual-Mode Phones

Although dual-mode phones by their nature are highly available with regard to network connectivity (when connectivity to the enterprise network is unavailable, the mobile voice and data networks can be used for voice and data services), enterprise WLAN and IP telephony infrastructure high availability must still be considered.

First, the enterprise WLAN must be deployed in a manner that provides redundant WLAN access. For example, APs and other WLAN infrastructure components should be deployed so that the failure of a wireless AP does not impact network connectivity for the dual-mode device. Likewise, WLAN

management and security infrastructure must be deployed in a highly redundant fashion so that dual-mode devices are always able to connect securely to the network. Controller-based wireless LAN infrastructures are recommended because they enable centralized configuration and management of enterprise APs, thus allowing the WLAN to be adjusted dynamically based on network activity and AP failures.

Next, VPN infrastructure components, including the Cisco ASA head-end VPN or AnyConnect session terminator, should be deployed in a highly redundant fashion so that loss of a VPN session terminator does not impact or prevent remote secure enterprise connectivity for the dual-mode client device.

Next, Unified CM call processing and registration service high availability must be considered. Just as with other devices within the enterprise that leverage Unified CM for call processing services, dual-mode phones must register with Unified CM. Given the redundant nature of the Unified CM cluster architecture, which provides primary and backup call processing and device registration services, dual-mode device registration as well as call routing are still available even in scenarios in which a Unified CM server node fails.

Similar considerations apply to PSTN access. Just as with any IP telephony deployment, multiple PSTN gateways and call routing paths should be deployed to ensure highly available access to the PSTN. This is not unique to dual-mode mobile client device deployments, but is an important consideration none the less.

Capacity Planning for Dual-Mode Phones

Capacity planning considerations for dual-mode phones are the same as for other IP telephony endpoints or devices that rely on the IP telephony infrastructure and applications for registration, call processing, and PSTN access services.

When deploying dual-mode phones, it is important to consider the registration load on Unified CM as well as the Unified Mobility limits. A single Unified CM cluster is capable of handling a maximum of 40,000 device configurations and registrations. When deploying dual-mode phones, you must consider the per-cluster maximum device support, and you might have to deploy additional call processing subscriber nodes or even clusters to handle the added load.

In addition, as previously mentioned, the maximum number of remote destinations and mobility identities within a single Unified CM cluster is 15,000. Because most dual-mode devices will likely be integrated with Unified Mobility to take advantage of features such as Mobile Connect and two-stage dialing, the mobile phone number of each of these dual-mode devices must be configured as a mobility identity within the Unified CM cluster. This is necessary to facilitate integration to Unified Mobility as well as to facilitate handoff in some cases. Therefore, when integrating dual-mode phones with Unified Mobility, it is important to consider the overall remote destination and mobility identity capacity of the Unified CM cluster to ensure sufficient capacity exists. If additional users or devices are already integrated to Unified Mobility within the system, they can limit the amount of remaining remote destination and mobility identity capacity available for dual-mode devices.

CTI capacity must also be considered when deploying the Cisco Mobile or Jabber dual-mode client for iPhone with desk phone integration. Because this feature relies on CTI monitoring of the primary line of the user's desk phone, each Cisco Mobile dual-mode user enabled for desk phone integration will consume a CTI connection on the Unified CM system. This load must be considered in relation to the overall CTI capacity of the system.

Overall call processing capacity of the Unified CM system and PSTN gateway capacity must also be considered when deploying dual-mode phones. Beyond handling the actual dual-mode device configuration and registration, the system must also have sufficient capacity to handle the added BHCA impact of dual-mode phones and users. Likewise, it is critical to ensure sufficient PSTN gateway capacity is available to accommodate dual-mode devices. This is especially the case for dual-mode

devices that are integrated to Unified Mobility because the types of users that would have dual-mode devices are typically highly mobile. Highly mobile users typically generate more enterprise PSTN gateway load from mobility features such as Mobile Connect, where an incoming call to a mobile user's enterprise number generates one or more calls to the PSTN, or from two-stage dialing, where a user makes a call through the enterprise by leveraging the enterprise PSTN gateway.

The above considerations are certainly not unique to dual-mode phones. They apply to all situations in which devices and users are added to Unified CM, resulting in additional load to the overall Unified Communications System.

For more information on general system sizing, capacity planning, and deployment considerations, see the chapter on Unified Communications Design and Deployment Sizing Considerations, page 29-1.

Design Considerations for Dual-Mode Phones

Observe the following design recommendations when deploying dual-mode phones and clients:

- Dual-mode mobile devices must be capable of dual transfer mode (DTM) in order to be connected simultaneously to both the mobile voice and data network and the WLAN network so that the device is reachable and able to make and receive calls on both the cellular radio and WLAN interface of the device. In some cases, proper dual-mode client operation might not be possible if mobile voice and data networks do not support dual-connected devices.
- WLAN APs should be deployed with a minimum cell overlap of 20%. This overlap ensures that a dual-mode device can successfully roam from one AP to the next as the device moves around within a location, while still maintaining voice and data network connectivity.
- WLAN APs should be deployed with cell power level boundaries (or channel cell radius) of -67 dBm in order to minimize packet loss. Furthermore, the same-channel cell boundary separation should be approximately 19 dBm. A same-channel cell separation of 19 dBm is critical for ensuring that APs or clients do not cause co-channel interference to other devices associated to the same channel, which would likely result in poor voice quality.
- Cisco recommends using only an enterprise class voice-optimized WLAN network for connecting dual-mode phones and clients. While most dual-mode phones and clients are capable of attaching to public or private WLAN access points or hot spots for connecting back to the enterprise through the Internet for call control and other Unified Communications services, Cisco cannot guarantee voice quality for these types of connections.
- The Unified Mobility Mobile Connect feature will not extend incoming calls to the dual-mode device's configured mobility identity if the dual-mode device is connected to the enterprise and registered to Unified CM. This is by design in order to reduce utilization of enterprise PSTN resources. Because the dual-mode device registers to Unified CM, the system knows whether the device is reachable inside the enterprise; and if it is, there is no reason to extend the call to the PSTN in order to ring the dual-mode device's cellular voice radio. Only when the dual-mode device is unregistered will Mobile Connect extend incoming calls to the user's enterprise number out to the mobility identity number on the mobile voice network. The global SIP Dual Mode Alert Timer service parameter should be adjusted to a minimum of 3,000 milliseconds to ensure that calls are not prematurely or unnecessarily routed to the mobility identity.
- When deploying dual-mode phones, Cisco recommends normalizing required dialing strings so that users are able to maintain their dialing habits, whether the mobile device is connected to the enterprise or not. Because dialing on the mobile network is typically done using full E.164 (with or without a preceding '+') and mobile phone contacts are typically stored with full E.164 numbers, Cisco recommends configuring the enterprise dial plan to accommodate full E.164 or full E.164 with

preceding '+' for dual-mode phones. By configuring the enterprise dial plan in this manner, you can provide the best possible end-user dialing experience so that users do not have to be aware of whether the device is registered to the Unified CM.

- Cisco recommends that dual-mode phone users rely exclusively on the mobile voice network for making emergency calls and determining device and user location. This is because mobile provider networks typically provide much more reliable location indication than WLAN networks. To ensure that dual-mode phones rely exclusively on the mobile voice network for emergency and location services, configure the Emergency Numbers field of the dual-mode devices within Unified CM with emergency numbers such as 911, 999, and 112 in order to force these calls over the mobile voice network. Dual-mode phone users should be advised to make all emergency calls over the mobile voice network rather than the enterprise network.
- Cisco recommends the following Nokia Call Connect client configuration settings in order to maximize the dual-mode device's use of the enterprise IP telephony infrastructure for making and receiving business calls:
  - Configure the Nokia Call Connect client SCCP registration setting to **Always On** to ensure that, whenever the Nokia device is associated to the enterprise WLAN network, it will attempt to register to Unified CM.
  - Configure the Nokia dual-mode phone's preferred or default call type setting to **Internet Call** to ensure that, when the Nokia Call Connect client is registered to Unified CM, the device will always attempt to route outbound calls through the WLAN interface of the dual-mode phone.
- When deploying Cisco Mobile or Cisco Jabber Apple iOS clients with desk phone integration, the end-user account for the Cisco Mobile or Jabber user must be enabled for CTI. In addition, call park should be configured at a system level so that the desk phone can auto-park the call and Cisco Mobile or Jabber client can retrieve whenever a call is moved from the desk phone to the client. CTI overhead of this feature should be considered when sizing the overall Unified CM system.
- When deploying Cisco Mobile, Cisco Jabber for iPhone, or Cisco Jabber for Android dual-mode clients, configure the WLAN network to accommodate the following deployment guidelines:
  - Minimize roaming of Cisco Mobile, Cisco Jabber for iPhone, and Cisco Jabber for Android dual-mode devices at Layer 3 within the WLAN. Layer 3 roaming where a device IP address changes will result in longer roam times and dropped voice packets and could even result in dropped calls.
  - Configure the same SSID across all APs utilized by the Cisco Mobile and Cisco Jabber dual-mode devices within the WLAN to ensure the fastest AP-to-AP roaming.
  - Configure all WLAN APs to broadcast their SSIDs in order to prevent mid-call prompts to join other APs within the WLAN infrastructure, which could result in interrupted calls.
- For deployments of Nokia Call Connect dual-mode clients, lower the WLAN HO Threshold setting within the Nokia Call Connect client to engage automatic hand-out more quickly. However, note that lowering this setting also increases the AP-to-AP roaming speed.

Cisco Unified Mobile Communicator

Note Cisco Unified Mobile Communicator has reached End-of-Sale (EoS) and End-of-Life (EoL). Cisco Jabber is the replacement mobile client for mobile devices. For more information, see the announcement at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7290/ps7271/end_of_life_notice_c51-677140.html.

Cisco Unified Mobile Communicator is a mobility solution that provides users the ability to access and leverage Cisco Unified Communications applications from their mobile phones. The Cisco Unified Mobile Communicator and Cisco Mobile graphical clients work in conjunction with a server running the Cisco Unified Mobility Advantage software to provide a rich user interface for accessing and controlling mobile phone features and functionality. The system integrates into existing corporate LDAP directories, allowing users to use a single set of credentials across all devices. Further, all traffic between Unified Mobile Communicator and Unified Mobility Advantage is protected by the Secure Socket Layer (SSL) protocol. Unified Mobile Communicator provides the following functionality for mobile phone users:

- Access to corporate and personal directories
- Presence and buddy synchronization with the enterprise
- Visual access to corporate voicemail
- Visibility into desk phone history of missed, placed, and received calls
- Secure store-and-forward text messaging
- Reception of conference notifications
- Dial-via-office using Cisco Unified CM

Note Not all functionality listed above is available on all supported handsets or mobile operating systems.

Note Cisco Unified Mobility Advantage 7.1(3) will continue to be supported and to interoperate with Cisco Unified CM 8.*x* and other Cisco Unified Communications System 8.*x* applications All discussions and descriptions in this section are based on version 7.1(3) of the Unified Mobility Advantage server. For more details on specific hardware and software requirements for this solution, refer to the *Compatibility Matrix for Cisco Unified Mobility Advantage, Cisco Mobile, and Cisco Unified Mobile Communicator*, available at http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html.

Cisco Unified Mobile Communicator Phone Support and Data Plan Requirements

While the Cisco Unified Mobile Communicator client application runs on a variety of mobile devices, the sophisticated functionality imposes minimum device requirements that restrict the application to a set of supported phones.

Cisco Unified Mobile Communicator is designed to run on the following mobile operating systems or handsets:

- Windows Mobile 6.0 or 6.1 Standard
- Nokia Symbian and Nokia S60 Third Edition (Nokia handsets)
- Apple iPhone 3G or 3GS running firmware version 3.0.1 or later (iPhone handsets)
- Research in Motion (RIM) Blackberry (Blackberry handsets)

Note The Cisco Unified Mobile Communicator client for the iPhone and Blackberry devices is called Cisco Mobile.

Handset model support varies according to the mobile operating system (OS); however, specific handset support certification is not required. For each mobile OS, Cisco requires handsets to support a minimum set of requirements. These requirements vary per mobile OS, but the following list contains general requirements that handsets must meet in order to be supported:

- Specific version of mobile OS (varies per OS)
- Specific form factors, screen sizes, and keyboard technologies (varies per operating system)
- Installed root certificate from recognized Certificate Authority (VeriSign or GeoTrust)
- No restrictions on installing or running third-party applications

Note Actual user experience can vary between devices.

For more details on specific handset requirements, refer to the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*, available at

http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

In addition to providing a supported device, the user must also be using that device with a supported data plan. The client uses a mobile data network to communicate with the Cisco Unified Mobility Advantage Server. While the client and server use SSL to secure all data traffic, the client initiates connections to the server using the mobile data network on the port that the Unified Mobility Advantage administrator specified during installation.

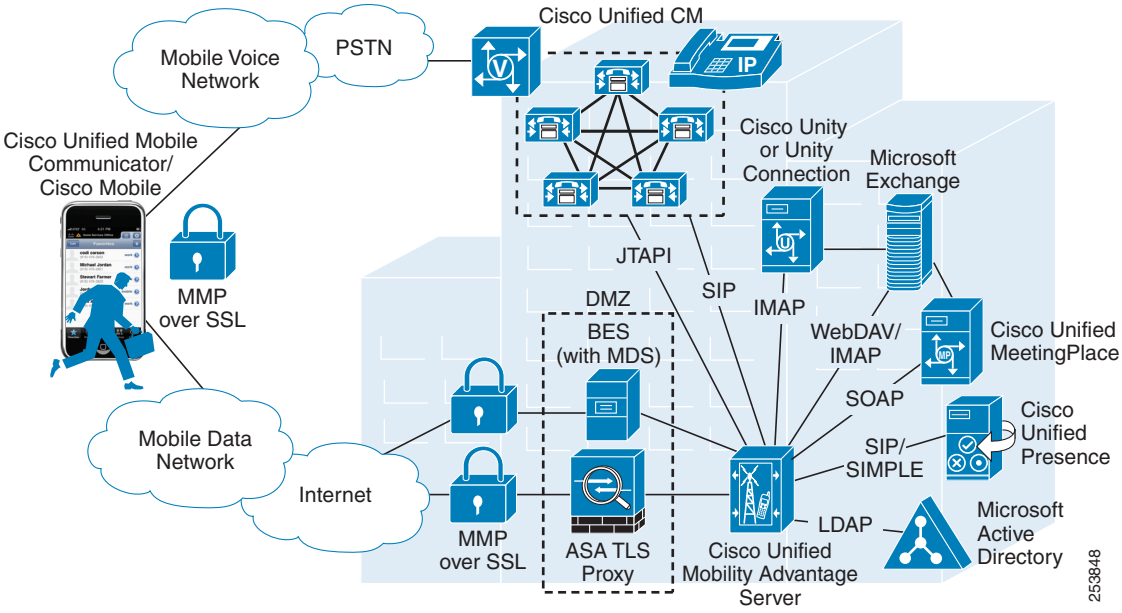
Because this may be a non-traditional port, the client requires that the mobile data network be accessed with an unrestricted plan. By contrast, many operators offer a low-end "web only" plan that allows the client to access HTTP over port 80 only. This type of plan is incompatible with Unified Mobile Communicator and will not work. Instead, the user must subscribe to a plan that allows arbitrary TCP traffic to pass from the client to any port on the server. This is sometimes referred to as a VPN plan. However, the client does not require a routable or static IP address because the Unified Mobility Advantage Server maps dynamic and translated addresses appropriately.

Because the Cisco Unified Mobile Communicator client relies on a data connection back to the enterprise for all application integration and functionality, this data connection is extremely important. The amount of bandwidth consumed by this critical connection is highly variable. Given the variable nature of these connections, Cisco highly recommends an unlimited data plan for all users rather than per-minute or per-byte plans. However, in some deployments unlimited data plans might be cost prohibitive. For bandwidth estimation and planning purposes, Cisco has found that on average most Unified Mobile Communicator users consume approximately 5.6 megabytes of bandwidth per month, provided they are not using visual voicemail functionality. Of course, bandwidth consumption will vary widely depending on end-user behavior. For example, a user who performs large numbers of directory lookups, sends many text messages, or makes large numbers of dial-via-office calls will consume considerably more bandwidth than a user who uses these features less frequently. For this reason, the average of 5.6 megabytes per month is merely a guideline. With visual voicemail, a one-minute voicemail message consumes approximately 354 kilobits, meaning that approximately two hours of visual messages will consume all of this monthly average. Therefore, it is easy to see that bandwidth requirements will be considerably higher when visual voicemail is in use.

Cisco Unified Mobile Communicator Architecture

The solution consists of three primary components: Cisco Unified Mobile Communicator, the Adaptive Security Appliance (ASA) TLS Proxy, and the Cisco Unified Mobility Advantage Server. (See Figure 25-30.) The Cisco Unified Mobility Advantage Server accesses existing Unified Communications applications and corporate systems, including as shown in Figure 25-30.

Figure 25-30 Cisco Unified Mobile Communicator Architecture



A user session is initiated when Unified Mobile Communicator starts on the mobile device. When the application starts, it prompts the user for their Microsoft Active Directory password. (Because the device is associated with the user account during provisioning, the client does not have to collect a user ID). The client then initiates an SSL connection to the ASA TLS Proxy using the mobile data network. This appears at the proxy as an inbound connection from the Internet. The protocol used over this connection is the Mobile Multiplexing Protocol (MMP). This protocol is optimized to conserve handset battery life. The MMP protocol is encapsulated in standards-based SSL packets.

Once the SSL connection is established, the ASA passes the request to the Unified Mobility Advantage Server, which then authenticates the user against the LDAP directory. The TCP connection carrying the SSL traffic is maintained by the client, allowing the server to push traffic down to the client regardless of address translation, dynamic client addresses, and so forth. Throughout the life of the client connection, the ASA TLS Proxy de-encrypts incoming packets from the client and does deep packet inspection to ensure that the packets are valid and are from the authorized client. If they are, the ASA proxy re-encrypts the packets and passes them to the Cisco Unified Mobility Advantage Server.

In addition to using the LDAP credentials for authenticating the Unified Mobile Communicator client user, the Unified Mobility Advantage Server also uses the credentials to connect to other back-end application systems. For example, the server uses this information to connect to the Microsoft Exchange server as the user, accessing their calendar, personal contacts, and conference notifications.

Whether deploying the ASA as both a TLS Proxy and firewall or deploying the ASA as simply a TLS Proxy in a DMZ and relying on some external firewall, you must configure two ports and open them on both the externally facing firewall or interface (between the Internet and the DMZ) and the internally facing firewall or interface (between the DMZ and the enterprise). A port in each of the following sets of ranges must be opened for both the external and internal firewalls:

- External Firewall Ports
  - Client Connection Port (TCP/SSL) in the range of 5400 to 5500
  - Provisioning Port (HTTP) in the range of 9000 to 9100
- Internal Firewall Ports
  - Client Connection Port (TCP/SSL) in the range of 5400 to 5500
  - Provisioning Port (HTTP) in the range of 9000 to 9100

Note The default client connection port (TCP/SSL) is 5443, and the default provisioning port (HTTP) is 9080.

Note You do not have to open the provisioning port in the firewall if you are deploying only iPhone or Blackberry handsets because these handsets do not download the Cisco Unified Mobile Communicator client over the provisioning port. For iPhone handsets, the client is downloaded from the Apple App Store; and for Blackberry handsets, the client is pushed to the handset via the Blackberry Enterprise Server (BES).

If you deploy Blackberry handsets in a Cisco Unified Mobile Communicator environment, the architecture changes slightly in that Blackberry devices running the Cisco Mobile client must connect to the Cisco Unified Mobility Advantage server through a Blackberry Enterprise Server (BES) deployed inside the enterprise. Unlike with other Cisco Unified Mobile Communicator and Cisco Mobile clients, the Blackberry client does not securely connect to the Unified Mobility Advantage server through the ASA. Instead, the secure connection between the Blackberry device and the BES server is used, and the BES server is integrated directly with the Unified Mobility Advantage server. The BES server must be deployed and configured with Mobile Data Service (MDS). As shown in Figure 25-30, both the BES server and the ASA can be integrated to the Unified Mobility Advantage server so that Blackberry and other supported mobile handsets can be deployed within the same system. For information on integrating BES with MDS directly to the Unified Mobility Advantage server for Blackberry devices, refer to the configuration guide for *Enabling Support for Clients in Cisco Unified Mobility Advantage*, available at

http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html

In a Microsoft Active Directory (AD) environment, there are no server-specific requirements for the LDAP server; any Domain Controller will work, provided it is a member of the appropriate domain. The Unified Mobility Advantage Server submits LDAP version 3 authentication and search requests to this server, and they propagate through the AD domain as expected. In an environment that contains multiple Exchange servers, the Cisco Unified Mobility Advantage Server will query AD to determine the appropriate server for each user.

Cisco Unified Mobile Communicator Features and Functionality

Cisco Unified Mobile Communicator provides users traveling outside the organization with the ability to use their mobile device to access and utilize various Unified Communications applications that reside inside the enterprise. The following enterprise applications can be integrated with the Unified Mobile Communicator solution. Each application provides the features and functionality outlined below.

For a complete list of the supported applications and versions that can integrate with the Cisco Unified Mobile Communicator solution, refer to the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*, available at

http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

LDAP Directory

The Cisco Unified Mobility Advantage server integrates with Microsoft Active Directory. This integration is required because Active Directory is used to authenticate Unified Mobile Communicator client connections. The user's Active Directory account password is never stored on the Cisco Unified Mobility Advantage server or the Unified Mobile Communicator client. In addition to providing an authentication mechanism for clients, Active Directory is also used to resolve directory lookups from the client, providing user's with the ability to search the corporate directory from their mobile device. As shown in Figure 25-30, the integration with Active Directory is via LDAP.

Cisco Unified CM

Cisco Unified Mobility Advantage Server can be integrated with Cisco Unified CM to provide desk phone call log synchronization, dial-via-office, and Unified Mobility integration. This integration requires an administrator to perform a number of configuration steps on Unified CM. For enterprise call log integration, application user accounts must be configured within Cisco Unified CM, and Unified Mobile Communicator users' desk phones must be associated to these accounts. These accounts are used by the Unified Mobility Advantage Server to monitor the desk phones of all Unified Mobile Communicator users to collect missed, received, and dialed calls. Each of these application user accounts is limited to a maximum of 250 monitored devices, and the Unified Mobility Advantage Server configuration allows a maximum of four account names, resulting in a maximum of 1,000 users. Each application user account within Cisco Unified CM must be assigned to both the Standard CTI Allow Call Monitoring group and Standard CTI Enabled group.

For dial-via-office functionality and integration with Unified Mobility, each user's Unified Mobile Communicator device must be configured as a device within Cisco Unified CM, this device must be configured with the user's enterprise number (the same directory number as the user's desk phone), and a mobility identity configured with the phone number of the user's mobile phone must be associated to this device.

For more information on integration with Unified CM, including configuration steps for enterprise call log integration, dial-via-office, and Unified Mobility integration, refer to the Cisco Unified Mobility Advantage installation and configuration documentation available at

http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html

Desk Phone Call Log Integration

Unified Mobile Communicator users with call log integration enabled are able to view call history lists (missed, placed, and received calls) from their desk phone on the Unified Mobile Communicator client.

As shown in Figure 25-30, a JTAPI connection is made between the Unified Mobility Advantage Server and Unified CM. This JTAPI connection utilizes CTI to monitor incoming and outgoing calls to the primary line of the user's desk phone. Note that call logs are synchronized only from the desk phone to the Unified Mobile Communicator client. Call logs are not synchronized from the Unified Mobile Communicator client to the desk phone.

Dial-via-Office

Dial-via-office functionality provides the ability to initiate a call from the mobile phone running the Cisco Unified Mobile Communicator client, using the Cisco Unified CM telephony infrastructure and enterprise PSTN gateway. This functionality is facilitated by SIP signaling over a SIP connection between the Unified Mobility Advantage Server and Unified CM, as shown in Figure 25-30.

Utilization of dial-via-office can be mandated by the Unified Mobility Advantage administrator for all calls made from the mobile phone by the Unified Mobile Communicator user. However, calls to configured emergency numbers or direct-dial numbers will bypass the dial-via-office mandate. Administrators may also choose to allow Unified Mobile Communicator users to decide if and when they use the dial-via-office feature. In those situations, the end-user can configure the phone to always use dial-via-office when making calls (except for calls to emergency numbers or direct-dial numbers they have configured, which are always signaled over the mobile voice network) or to prompt them on a per-call basis.

There are two types of dial-via-office supported with the Cisco Unified Mobile Communicator solution:

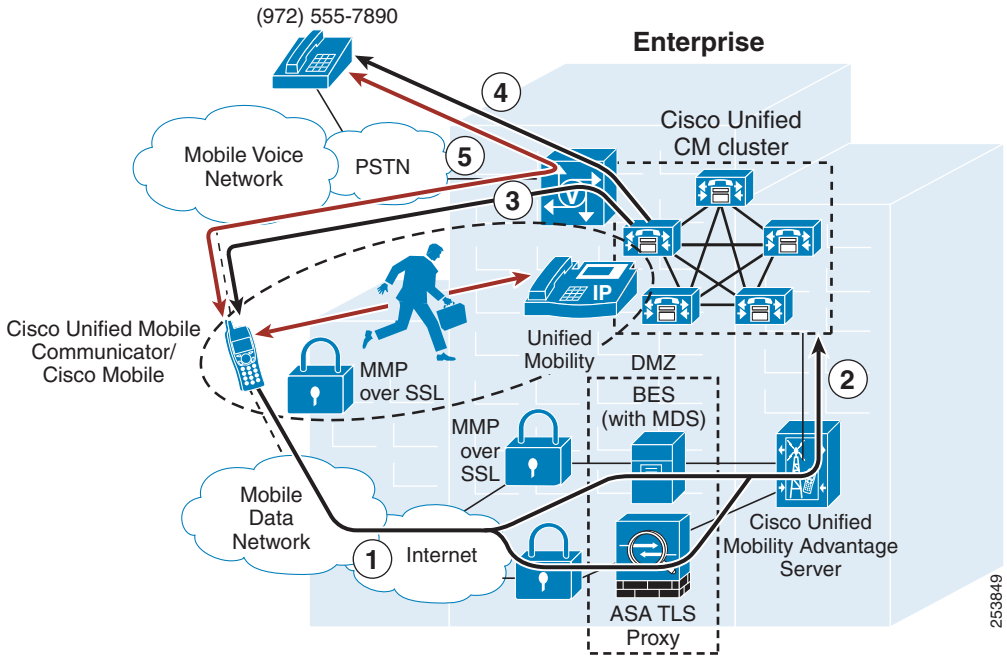
- Dial-Via-Office Reverse Callback, page 25-93
- Dial-Via-Office Forward, page 25-94

Dial-Via-Office Reverse Callback

Figure 25-31 illustrates a dial-via-office reverse callback call flow. In this example, a Unified Mobile Communicator user wishes to dial the PSTN phone 972-555-7890. The user dials the number or selects the number from a contact or directory list, which generates a SIP INVITE over the data connection to the enterprise and the Cisco Unified Mobility Advantage Server (step 1). This SIP INVITE is encapsulated in the MMP protocol and sent over the secure connection through the ASA or BES server (depending on the client type) between the client and the Cisco Unified Mobility Advantage server. The request is then forwarded by the Cisco Unified Mobility Advantage server over the SIP connection to Cisco Unified CM (step 2). Unified CM then generates a callback to the user's mobile phone number using the enterprise PSTN gateway (step 3). Once the incoming call from Unified CM is auto-answered at the mobile device, a call is extended to the number the user called or selected (step 4; in this case, 972-555-7890). Once the call is answered at the far end, the call is anchored through the enterprise PSTN gateway (step 5). Because the call is now anchored in the enterprise gateway, the user has the ability at any point during this call to use the Unified Mobility desk phone pickup feature as well as to invoke Unified Mobility mid-call features.

Note All voice or media from the user's mobile phone will always travel over the mobile voice network. Media never traverses the data connection to the enterprise. The mobile data network connection is used only for call signaling traffic and other application interactions.

Figure 25-31 Cisco Unified Mobile Communicator, Dial-via-Office Reverse Callback



In addition to having the dial-via-office reverse callback feature call back to the Cisco Unified Mobile Communicator device; users are also given the option of providing, within the Unified Mobile Communicator client configuration, an alternative number on which to be called back. For example, rather than receiving the callback on the mobile phone, the user could direct the callback to a conference room phone.

Note When invoking the dial-via-office reverse callback feature, if the callback from Unified CM is directed to a user-specified alternate number, users will have no ability to perform desk phone pickup or to invoke mid-call features for that call.

Dial-via-office reverse callback is supported for Windows Mobile, Nokia, and Blackberry mobile handsets.

Dial-Via-Office Forward

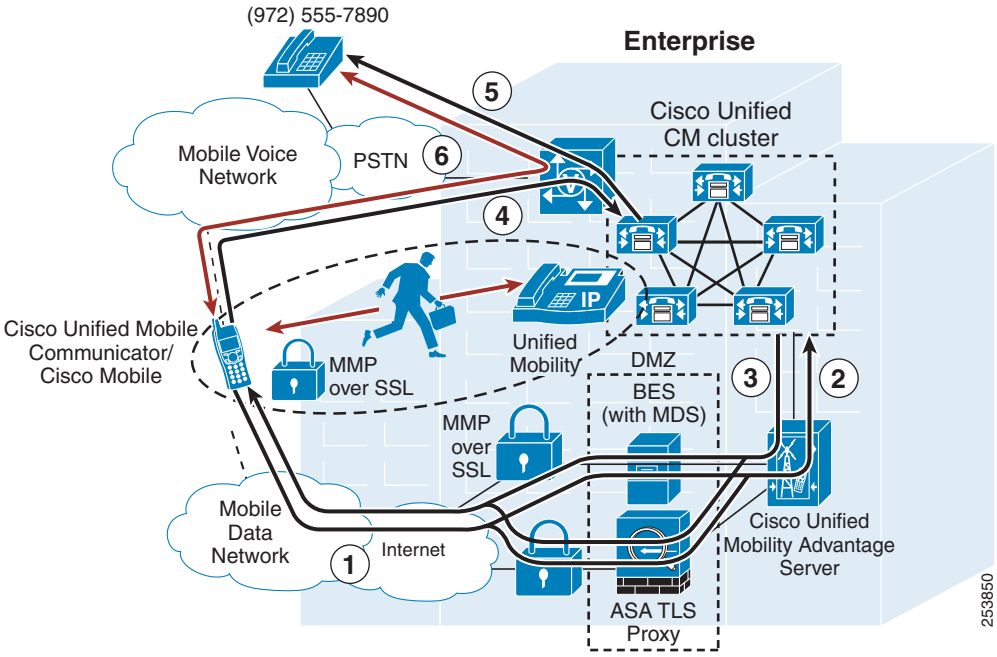
Figure 25-32 illustrates a dial-via-office forward call flow. In this example, a Unified Mobile Communicator user wishes to dial the PSTN phone 972-555-7890. The user dials the number or selects the number from a contact or directory list, which generates a SIP INVITE over the data connection to the enterprise and the Cisco Unified Mobility Advantage Server (step 1). This SIP INVITE is encapsulated in the MMP protocol and sent over the secure connection through the ASA or BES server (depending on the client type) between the client and the Cisco Unified Mobility Advantage server. The request is then forwarded by the Cisco Unified Mobility Advantage server over the SIP connection to Cisco Unified CM (step 2). Unified CM then responds back to the Cisco Unified Mobility Advantage server with the configured system-wide Enterprise Feature Access number, which is then forwarded back to the user's mobile device over the secure connection through the ASA or BES server, depending on the client type (step 3). Once the number is received at the mobile device, the Cisco Unified Mobile Communicator client automatically generates an outgoing call from the mobile device to the Enterprise Feature Access number (step 4). Once this call is received by Unified CM, the system matches the

inbound caller ID against the configured mobility identity for the user. If the inbound caller ID matches the user's configured mobility identity, a call is made by the system to the number the user dialed or selected (step 5; in this case, 972-555-7890). Once the call is answered at the far end, the call is anchored through the enterprise PSTN gateway (step 6). Because the call is now anchored in the enterprise gateway, the user has the ability at any point during this call to use the Unified Mobility desk phone pickup feature as well as to invoke Unified Mobility mid-call features.

Note In order for the dial-via-office forward call to be completed successfully, Unified CM must receive an inbound caller ID from the PSTN network that matches the mobility identity number configured for the Unified Mobile Communicator device placing the dial-via-office call. If the inbound caller ID from the PSTN is not received or does not match the user's configured mobility identity, the dial-via-office forward call will fail.

Note All voice or media from the user's mobile phone will always travel over the mobile voice network. Media never traverses the data connection to the enterprise. The mobile data network connection is used only for call signaling traffic and other application interactions.

Figure 25-32 Cisco Unified Mobile Communicator, Dial-via-Office Forward



Note If the iPhone firmware version is earlier than 3.1, then the dial-via-office forward call will require manual intervention by the user to complete the call. With iPhone firmware versions prior to 3.1, the dial-via-office call will not complete automatically. Instead the user will receive a dialog box on the client in step 3 of Figure 25-32 and must select 'Call' in order for the call to the Enterprise Feature Access number in step 4 to be generated.

In order for Cisco Unified Mobile Communicator to be able to dial the Enterprise Feature Access number sent by Unified CM for a dial-via-office forward call, the number sent must be a full E.164 number so that it can be dialed via the mobile voice network. If the number configured in the Enterprise Feature Access Directory Number field within Unified CM (under **Call Routing > Mobility Configuration**) is not a full E.164 number, the administrator should configure the Dial-via-Office Forward Service Access Number service parameter for the Cisco CallManager service with the full E.164 number that corresponds to the Enterprise Feature Access directory number configured within Unified CM. If the Dial-via-Office Forward Service Access Number service parameter is not configured, Unified CM will send the Enterprise Feature Access directory number exactly as configured. If this number is not a full E.164, the call from the Cisco Unified Mobile Communicator into the Unified CM system (step 4 of Figure 25-32) will fail, thus rendering the dial-via-office forward feature inoperable.

As an example, suppose the Enterprise Feature Access directory number is configured within Unified CM as 51234. Then in situations where the Dial-via-Office Forward Service Access Number is not configured, Unified CM will forward the Enterprise Feature Access number back to Unified Mobility Advantage as 51234, resulting in the call dialog at the Unified Mobile Communicator device to display 51234. If the user selects the Call option, the phone will attempt to call 51234 over the mobile voice network, and this call will fail. However, if the Dial-via-Office Forward Service Access Number is configured as 9195551234, then Unified CM will forward the Enterprise Feature Access number back to Unified Mobility Advantage as 9195551234. This ensures that, when the user selects the Call option, the call will be routed properly over the mobile voice network and PSTN back to the enterprise.

Dial-via-office forward is supported with Cisco Mobile, the Cisco Unified Mobile Communicator clients for the iPhone and Blackberry.

Interactions Between Nokia Call Connect and Cisco Unified Mobile Communicator

The Nokia Call Connect dual-mode client can be used in parallel with the Cisco Unified Mobile Communicator client for Nokia. When both clients are deployed, not only is the Nokia device able to leverage the enterprise IP telephony infrastructure for making and receiving calls inside the enterprise, but it is also able to leverage Unified Mobile Communicator features such as directory lookups, desk phone call log integration, presence, visual voicemail, text messaging, and dial-via-office. To integrate Nokia Call Connect dual-mode client with Unified Mobile Communicator, check the **Enable Cisco Unified Mobile Communicator** checkbox on the Nokia S60 device configuration page within Unified M.

Once configured within Unified CM, both clients can be run on the Nokia dual-mode device; however, it is important to understand the implications for the dial-via-office feature. While all other features and functions within the two clients will operate normally, the dial-via-office interaction behaves somewhat differently when the Nokia Call Connect client is installed on the same device. The dial-via-office feature within Unified Mobile Communicator will engage only for calls routed through the mobile voice network or cellular interface. For this reason, calls made by the Nokia Call Connect client through the WLAN interface will not engage dial-via-office, which is preferable behavior because the call is already being made over the enterprise IP telephony infrastructure.

However, for calls made from the mobile voice or cellular interface, the dial-via-office feature may be engaged, depending on the dial-via-office settings within the Unified Mobile Communicator client and/or the dial-via-office settings on the Cisco Unified Mobility Advantage server. If the administrator of the Unified Mobility Advantage server forces dial-via-office for users, then the Unified Mobile Communicator client will attempt to invoke dial-via-office for every call made out the cellular interface of the device. In these situations, the user should set the configuration parameter **Allow dial via office for** to **Call from this app** on the Unified Mobile Communicator client so that only calls made directly from the Unified Mobile Communicator client will attempt to invoke dial-via-office. By configuring the client this way, the user can ensure that dial-via-office will not be engaged when calls are made through the cellular interface outside of the Unified Mobile Communicator client. For example, it would be undesirable to engage dial-via-office on the Nokia device when the Nokia Call Connect client is

attempting to hand-out a call from the enterprise WLAN to the mobile voice network. During hand-out, the cellular interface of the Nokia dual-mode device calls the Unified CM Handoff Number, and having dial-via-office engage would cause additional unnecessary call legs to be created and might in fact result in a failure to hand-off the original call.

Likewise, if the administrator has allowed individual Unified Mobile Communicator users to configure their own dial-via-office settings within the client, then the users can set the client to prompt them to choose between making the call directly and using dial-via-office each time a call is attempted through the cellular interface. By setting the Unified Mobile Communicator **When dialing** setting to **Let me choose** and the **Allow dial via office for** setting to **Call from this app**, the user has maximum control over when dial-via-office will be used. In all cases, users should use dial-via-office only when the Nokia dual-mode device is outside the enterprise and not registered to Unified CM.

For more information about the Cisco Unified Mobile Communicator solution, feature set, and design and deployment considerations, see Dual-Mode Phones and Clients, page 25-66.

Unified Mobility Integration

In addition to integrating with Unified CM for call log integration and dial-via-office, Unified Mobile Communicator users may also be integrated with Unified Mobility to take advantage of Mobile Connect, thus ensuring that incoming calls to a user's enterprise number will be extended to the user's mobile phone. The integration of Cisco Unified Mobile Communicator clients with Unified Mobility is done through a configured mobility identity associated directly to the Cisco Unified Mobile Communicator device within Unified CM. The configuration settings for a mobility identity within Unified CM are the same as a remote destination. Furthermore, all of the guidelines surrounding configuration of the remote destination number and caller ID matching (see Remote Destination Configuration and Caller ID Matching, page 25-55) apply to configuration of the mobility identity number as well. Within the Unified Mobile Communicator client interface, the user has the ability to enable or disable Mobile Connect (Single Number Reach) under the General settings menu.

Cisco Unified Presence

The Unified Mobility Advantage Server can be integrated with Cisco Unified Presence so that Unified Mobile Communicator users are able to update their presence status or availability to the enterprise network. Likewise, the Unified Mobile Communicator client receives presence information for other enterprise clients within the user's buddy list, directory list, contact list, voicemail message list, and call history logs. Presence status and buddy lists are synchronized between the Unified Mobile Communicator client and the user's Cisco Unified Personal Communicator client. Unified Mobile Communicator users can manually adjust their availability within the client or rely on automatic updates to availability based on Microsoft Exchange personal calendar availability and desk phone line status. As shown in Figure 25-30, integration with Cisco Unified Presence is done using a SIP/SIMPLE connection between the Unified Mobility Advantage Server and the Cisco Unified Presence server.

Note Cisco Mobile, the Unified Mobile Communicator client for the iPhone, does not display presence status or support sending or receiving of presence status updates.

Cisco Unity and Unity Connection Voice Mail

The Unified Mobility Advantage server can be integrated with Cisco Unity (in Unified Messaging or Integrated Messaging mode) and Cisco Unity Connection voicemail systems to provide the Unified Mobile Communicator client with message waiting indication (MWI) status for the user's enterprise

voicemail box. With this integration, a user can also visually navigate their voicemail box using their mobile device. The user is able to navigate a list of all messages in the voicemail box. This list includes the following information:

- Time the message was left
- Length of the message
- Caller ID or name (if available) of the person who left the message
- Priority indication for the message
- Current presence or availability indication of the person who left the message, if that person is providing presence status to the enterprise presence infrastructure

When the user selects a message from the list, the message is downloaded by the Unified Mobile Communicator client using the data connection, and the user is able to play the message and then delete or save the message on the voicemail system. Changes to the status of a voicemail message made by the Cisco Unified Mobile Communicator client (for example, marking the message as read or deleting the message) are propagated to the voicemail system and are appropriately reflected on the user's desk phone and other clients such as Cisco Unified Personal Communicator. Voicemail messages can be navigated in any order. As shown in Figure 25-30, Unified Mobility Advantage Server integrates with Cisco Unity or Unity Connection using the IMAP protocol.

Cisco Unified MeetingPlace

The Unified Mobility Advantage Server can be integrated with Cisco Unified MeetingPlace so that Unified Mobile Communicator users can receive conference notifications or invitations to MeetingPlace meetings. These meeting notifications include the subject, the time and date, dial-in number, and meeting ID of the conference. The user can then click to call the dial-in number.

Note Click-to-join is supported only with Cisco Mobile, the Cisco Unified Mobile Communicator for the iPhone and Blackberry. For all other Cisco Unified Mobile Communicator clients, the user must manually enter the meeting ID once the call is connected.

Integration with Cisco Unified MeetingPlace is done via a direct connection from the Unified Mobility Advantage Server to the Microsoft Exchange server utilized by the conferencing system. This connection uses the web-based Distributed Authoring and Versioning (WebDAV) protocol, as shown in Figure 25-30.

In order for conference notifications to be received by Cisco Unified Mobile Communicator clients (including Cisco Mobile), the system administrator must modify the Cisco Unified MeetingPlace meeting notification email templates to include a **cump://** prefixed link in each meeting notification. The Cisco Unified Mobility Advantage server looks for this link in all meeting notifications contained within the user's Exchange mailbox. If this link is not present in a meeting notification, then notification of the meeting will not be listed or received by the client. For details surrounding the required modifications to the Cisco Unified MeetingPlace meeting notification email templates, refer to *Configuring Features in Cisco Unified Mobility Advantage: Meeting Features*, available at

http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html

Integration to MeetingPlace not only supports conference notifications but also allows the user to click-to-join a conference without the need to enter a password or meeting ID. This click-to-join functionality is facilitated by a SOAP call to the Web Services API of the MeetingPlace server, as shown in Figure 25-30.

Note Click-to-join is supported only with Cisco Mobile, the Unified Mobile Communicator clients for the iPhone and Blackberry.

In deployments where Cisco WebEx is providing web sharing capabilities for Cisco Unified MeetingPlace meetings, the iPhone Cisco Mobile client will cross-launch the Cisco WebEx Meeting Center application on the iPhone (assuming this application has already been installed on the device). For this cross-launch to work, the Cisco Unified MeetingPlace system must be successfully integrated with Cisco WebEx.

Microsoft Exchange

In addition to communicating with Microsoft Exchange for Cisco Unified MeetingPlace conferencing integration, the Cisco Unified Mobility Advantage Server also integrates with Microsoft Exchange via WebDAV to facilitate maintenance of the user's personal contact lists that are stored on Exchange. Integration with Exchange also provides the ability to update a user's presence status automatically based on their Exchange calendar availability. Microsoft Exchange is an optional component and is required only if conference notifications, personal contact lists, or calendar integration are needed.

Secure Text Messaging

In addition to the above application integrations and functionality, Unified Mobile Communicator users can also send secure text messages to one another using the Unified Mobile Communicator client. This message exchange is facilitated natively within the Cisco Unified Mobility Advantage Server. These messages are exchanged using the mobile data connection, therefore no SMS provider charges are incurred.

Note Cisco Mobile, the Unified Mobile Communicator client for the iPhone, does not support secure text messaging using the Cisco Unified Mobility Advantage server.

High Availability for Cisco Unified Mobile Communicator

The Cisco Unified Mobile Communicator client is completely reliant upon the backhauled data connection across the mobile data network to the Cisco Unified Mobility Advantage Server for application interaction and functionality. If this data connection is lost due to a failure in the mobile data network, loss of connectivity to the mobile data network, or failure of the ASA TLS Proxy, BES Server, or the Cisco Unified Mobility Advantage Server, then access to enterprise applications will be unavailable. Given any of these types of failures, users will be unable to access Unified Mobile Communicator to take advantage of the various application integrations. For example, the user would be unable to perform directory lookups, send text messages to other clients, access visual voicemail, access personal contacts, receive message waiting indication, receive conference notifications, update or synchronize buddy lists and presence information, or make calls using the dial-via-office feature.

Note Given a failure of the data connection between the Cisco Unified Mobile Communicator client and Cisco Unified Mobility Advantage or a failure of the connection between Cisco Unified Mobility Advantage and Cisco Unified CM, the client will fall back to direct dial even in cases where dial-via-office has been mandated administratively.

While the features and functions provided by Unified Mobile Communicator will be unavailable if the data connection to the enterprise is unavailable, the user will still be able to make and receive phone calls with their mobile device using the mobile voice network as usual. In addition, if the user and the mobile phone have been integrated with Unified Mobility on Unified CM, then Mobile Connect functionality as well as features such as Mobile Voice Access and Enterprise Feature Access will still be available.

Failure of enterprise applications such as Cisco Unified Presence, Cisco Unified CM, or Cisco Unity and Unity Connection can result in loss of particular functions, depending on the nature of these applications within the deployment. However, in many cases multiple adapters can be configured within the Unified Mobility Advantage Server and, assuming redundancy has also been provided for the various applications, often functionality can be maintained given an application or application server failure.

Capacity Planning for Cisco Unified Mobile Communicator

The Cisco Unified Mobility Advantage Server supports the following user capacities:

- Cisco MCS 7845-H2/I2 supports up to 1,000 Unified Mobile Communicator clients.
- Cisco MCS 7825-H4/I4 supports up to 500 Unified Mobile Communicator clients.
- Cisco MCS 7825-H2/I2 or 7825-H3/I3 supports up to 250 Unified Mobile Communicator clients.

To support more than 1,000 Unified Mobile Communicator users within a deployment, additional Unified Mobility Advantage Servers may be installed. However, Unified Mobile Communicator clients configured and associated to one Cisco Unified Mobility Advantage Server will not be able to send text messages to clients on another server.

When integrating Unified Mobile Communicator with Cisco Unified CM for enterprise call log integration, the Unified Mobility Advantage Server interacts with Unified CM CTIManager for desk phone line monitoring. For each Unified Mobile Communicator enabled for call log integration, the Cisco Unified Mobility Advantage Server generates one CTI connection to the CTIManager. Therefore, with a deployment of Unified Mobile Communicator with one fully populated Unified Mobility Advantage Server running on an MCS 7845 with call log integration enabled for all users, 1,000 CTI connections will be consumed. For this reason, when you deploy Unified Mobile Communicator with call log integration, you must consider the number of required CTI connections with regard to the following cluster-wide limits for CTI connections:

- 40,000 CTI connections per Unified CM cluster with MCS 7845-I3 or OVA equivalent servers.
- 20,000 CTI connections per Unified CM cluster with Cisco MCS 7845-H2/I2 or OVA equivalent servers.
- 10,000 CTI connections per Unified CM cluster with Cisco MCS 7835-H3/I3 or OVA equivalent servers.
- 8,000 CTI connections per Unified CM cluster with Cisco MCS 7835-H2/I2 servers.
- 4,000 CTI connections per Unified CM cluster with Cisco MCS 7825-H5/I5 or OVA equivalent servers.
- 3,600 CTI connections per Unified CM cluster with all other currently supported Cisco MCS 7825 and MCS 7835 servers.

If additional CTI connections are required for other applications, they can limit the capacity of Unified Mobile Communicator users with call log integration enabled.

Integration of Unified Mobile Communicator with Unified CM for dial-via-office and Unified Mobility functionality requires the configuration of each Unified Mobile Communicator as a Unified CM device and configuration of the mobile number as a mobility identity. Therefore, when implementing these integrations, you must also consider overall Unified CM phone and mobility-enabled user capacities.

Design Considerations for Cisco Unified Mobile Communicator

Observe the following design considerations when deploying Cisco Unified Mobile Communicator:

- For security reasons, the Cisco Unified Mobility Advantage server should be deployed behind the enterprise firewall because it is the integration point for all enterprise services and applications.
- Because the Cisco Adaptive Security Appliance (ASA) serves as a proxy server for communications between Cisco Unified Mobile Communicator clients and the Cisco Unified Mobility Advantage server, the ASA should be deployed in the enterprise DMZ.
- An SSL certificate from a Certificate Authority must be obtained. The certificate is required in order to enable encryption of data flowing between Cisco Unified Mobile Communicator clients and the Cisco Unified Mobility Advantage server.
- SSL certificates must be obtained from well-known certificate authorities VeriSign or GeoTrust because mobile phones have limited capabilities in terms of importing root certificates. Root certificates from VeriSign and GeoTrust are commonly available on most mobile handsets.
- Firewall ports in the corporate firewall must be opened to allow connectivity from the Cisco Unified Mobile Communicator clients on the Internet to the ASA in the DMZ and from the ASA in the DMZ to the Cisco Unified Mobility Advantage server in the enterprise. The following firewall ports must be opened:
  - Client connection port (SSL): a single TCP port in the range 5400 to 5500 (default port is 5443)
  - Provisioning port (HTTP): a single TCP port in the range 9000 to 9100 (default port is 9080)

  Note You do not have to open the provisioning port in the firewall if you are deploying only iPhone or Blackberry handsets because these handsets do not download the Cisco Unified Mobile Communicator client over the provisioning port. For iPhone handsets, the client is downloaded from the Apple App Store; and for Blackberry handsets, the client is pushed to the handset via the Blackberry Enterprise Server (BES).

- Microsoft Active Directory is required to authenticate Cisco Unified Mobile Communicator users. All Cisco Unified Mobile Communicator users must have a valid account within Microsoft Active Directory, otherwise authentication will fail and user will not be able to utilize features and services provided by this solution.
- Always ensure that appropriate back-end enterprise application servers have been deployed and configured appropriately based on the Cisco Unified Mobile Communicator solution features and functionality required. For a complete list of supported features and the required back-end application servers, refer to the *Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*, available at

  http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html
- If you deploy Cisco Mobile, the Unified Mobile Communicator client for the Blackberry, you must also deploy a Blackberry Enterprise Server (BES) with Mobile Data Services (MDS) and integrate it directly to the Unified Mobility Advantage server. Cisco Mobile clients on Blackberry devices do not connect to the enterprise ASA, but instead use the secure Research In Motion (RIM) mobile network operations center (NOC) and the secure connection from the NOC to the enterprise BES server before connecting to the Unified Mobility Advantage server.

- In situations where both the Nokia Call Connect dual-mode client and the Cisco Unified Mobile Communicator Nokia client are deployed on the same handset, avoid using dial-via-office whenever the dual-mode device is inside the enterprise and registered to Unified CM. Cisco recommends the following:
  - When dual-mode phones are deployed in the enterprise, the administrator of the Cisco Unified Mobility Advantage Server should not force dial-via-office by using the Dial Via Office Policy setting. Instead, the administrator should allow users to choose whether they use dial-via-office.
  - If dial-via-office is forced for Cisco Unified Mobile Communicator by the administrator of the Cisco Unified Mobility Advantage server, the user should configure the **Allow dial via office for** setting to **Call from this app** within the Unified Mobile Communicator client so that only calls made directly from within the Unified Mobile Communicator client will attempt to invoke dial-via-office. By configuring the client this way, the user can ensure that dial-via-office will not be engaged unexpectedly. If the Unified Mobile Communicator client is not in the foreground, then the user can be sure that dial-via-office will not be invoked.
  - If dial-via-office is not forced by the Unified Mobility Advantage administrator, the Unified Mobile Communicator user should set the **When dialing** setting to **Let me choose** and the **Allow dial via office for** setting to **Call from this app**. By configuring the settings in this manner, the user has maximum control over when dial-via-office will be used. In all cases, users should use dial-via-office only when the Nokia dual-mode device is outside the enterprise and not registered to Unified CM.

Direct Connect Mobile Clients

Direct connect mobile clients provide a solution that gives mobile users the ability to access and leverage Cisco Unified Communications applications from their mobile phones. Similar to the Cisco Unified Mobile Communicator solution, direct connect client applications running on mobile smart phones work in conjunction with one or more application servers within the enterprise to provide a rich user interface for accessing and leveraging enterprise voice and collaboration applications. However, unlike the Cisco Unified Mobile Communicator solution, direct connect mobile clients communicate directly with back-end application servers rather than through an intermediary server such as Cisco Unified Mobility Advantage, thus the "direct connect" moniker. Direct connect mobile clients leverage the inherent scalability and reliability of the various enterprise back-end application servers.

Direct connect mobile clients not only provide the ability to access and use collaboration applications, but they can also leverage Voice over WLAN (VoWLAN) functionality to make and receive calls, thus providing dual-mode functionality as well. With support for both dial-via-office operations and voice over WLAN calling, enterprises can drastically reduce their mobile calling costs by off-loading voice traffic from the cellular network to the enterprise data network and, barring that, providing reduced cost call routing through the enterprise by means of local toll or even toll-free system access numbers.

This section examines direct connect mobile client architecture and common functions and features provided by these clients, including dial-via-office and XMPP-based IM and presence. After covering general direct connect mobile client architecture and features and functions, this section provides coverage of various capabilities and integration considerations for the Cisco Mobile 8.5 for Nokia direct connect mobile client.

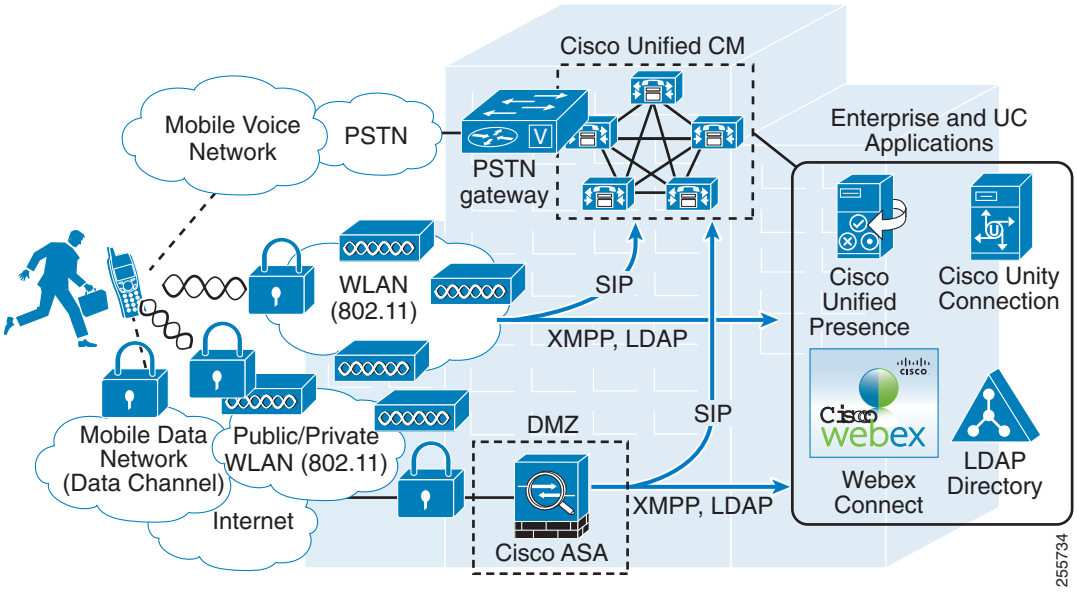
In addition, this section discusses high availability and capacity planning considerations for direct connect mobile clients.

Direct Connect Mobile Client Architecture

Direct connect mobile clients provide both remote data connectivity to the enterprise and on-premises data connectivity through wireless local area networks (WLANs) using IEEE 802.11 standards. Further voice connectivity is enabled through the mobile voice network and PSTN or through a 802.11 WLAN or the mobile data network.

Figure 25-33 depicts the basic direct connect solution architecture for connecting mobile smart phone devices into a Cisco Unified Communications System. The direct connect mobile client enables the mobile device to connect to the enterprise over the Internet using the mobile data network or a public or private Wi-Fi hot spot in order to communicate with back-end application servers such as Cisco Unified CM, the LDAP corporate directory, and Cisco Unified Presence. Further, when inside the enterprise, the device can connect to these same back-end applications and services over the enterprise WLAN.

Figure 25-33 Direct Connect Mobile Client Architecture



The direct-connect client registers to Cisco Unified CM as an enterprise phone either remotely over the mobile data network or Wi-Fi hot spot or locally once it is associated to the enterprise WLAN. Once registered, the direct connect client leverages the enterprise telephony infrastructure for making and receiving calls either through dial-via-office, where the voice path is over the mobile voice network or PSTN, or through VoWLAN. The client is also capable of leveraging SIP (and in some cases SCCP) signaling for applying supplementary call features such as hold, transfer, conference, and so forth, and for enabling/disabling Mobile Connect. When enterprise WLAN connectivity and remote data connection to the enterprise over the mobile voice network or Wi-Fi hot spot is unavailable, the mobile phone will fall back to the mobile voice network for making and receiving calls and will be able to invoke mid-call supplementary features only through DTMF feature access codes over the mobile voice network and PSTN.

When the direct connect client device is connected to the enterprise network, it will be reachable through the user's enterprise number. Any inbound calls to the user's enterprise number will ring the IP-attached device. If the user has a Cisco IP desk phone, then the direct connect client registration enables a shared line instance for the user's enterprise number so that an incoming call rings both the user's desk phone

and the mobile phone. When not connected to the enterprise network, the client device becomes unregistered and will be able to receive enterprise calls only if the user has been enabled for Unified Mobility and Mobile Connect (or single number reach) has been turned on for the mobile number.

Likewise the direct connect client allows users to access IM and presence services through XMPP and directory services through LDAP when connected to the enterprise directly or remotely.

Network Connectivity: WLAN and VPN

Direct connect mobile clients are capable of connecting to the enterprise network using both WLAN and the mobile data network. For connecting to the enterprise remotely, a VPN secure connection is typically required. To enable this network connectivity for these clients, it is critical to provide the appropriate WLAN and/or VPN infrastructure, depending on the connection method(s) the enterprise plans to leverage.

WLAN Infrastructure

When leveraging WLAN for network connectivity, it is imperative to deploy a finely tuned, QoS-enabled, and highly available WLAN network. Because the direct connect mobile clients must rely in whole or in part on the underlying WLAN infrastructure for carrying both critical signaling and real-time voice media traffic as well as data traffic for accessing various applications, deploying a WLAN network optimized for both data and real-time voice traffic is necessary. A poorly deployed WLAN network will be subjected to large amounts of interference and diminished capacity, leading not only to poor voice quality but in some cases also to dropped or missed calls. This will in turn render the WLAN deployment unusable for making and receiving voice calls. Therefore, when leveraging WLAN connectivity for deployed direct connect mobile clients, you must conduct a WLAN radio frequency (RF) site survey before, during, and after the deployment to determine appropriate cell boundaries, configuration and feature settings, capacity, and redundancy to ensure a successful Voice over WLAN (VoWLAN) deployment. As with other WLAN-enabled clients, each mobile phone device and client should be tested on the WLAN deployment to ensure proper integration and operation prior to a production deployment. Using a WLAN that has been deployed and configured to provide optimized VoWLAN services (such as the Cisco Unified Wireless Network), including quality of service, will ensure a successful direct-connect device deployment.

For more information on Voice over WLAN deployments and wireless device roaming, see Wireless Device Roaming, page 25-7.

VPN Infrastructure

When employing VPN network connectivity for connections over the mobile data network or public or private Wi-Fi hot spots, it is important to deploy a high-bandwidth secure VPN infrastructure that adheres to the enterprise's security requirements and policies. Careful planning is needed to ensure that the VPN infrastructure provides high bandwidth, reliable connections, and appropriate session or connection capacity based on the number of users and devices using this connectivity.

VPN connection types and methods vary, with options ranging from standards-based IPSec, leveraging Cisco IOS VPN or Cisco Adaptive Security Appliance (ASA), to Cisco AnyConnect and the Cisco Jabber secure connect feature, both also leveraging the Cisco ASA. The type of VPN method or client used will often depend on the mobile device or devices being deployed.

For more information on secure remote VPN connectivity solutions, including Cisco AnyConnect, refer to the secure mobility documentation available at

http://www.cisco.com/en/US/products/hw/vpndevc/products.html#mobi

For information on Cisco Jabber secure connect, refer to the *Cisco Jabber Secure Connect Deployment Guide*, available at

http://www.cisco.com/en/US/products/ps11678/products_implementation_design_guides_list.html

Note While dual-mode phones and direct connect clients are capable of connecting back to the enterprise through the Internet for call control and other Unified Communications services, Cisco cannot guarantee voice quality or troubleshoot connectivity or voice quality issues for these types of connections. These types of connections include remote connections to the enterprise through public or private WLAN access points or hot spots or through the mobile data network. Cisco recommends an enterprise-class voice-optimized WLAN network for connecting mobile client devices. Most public and private WLAN APs and hot spots are tuned for data applications and devices. In these cases, the AP radios are turned to maximum power, and dynamic-power control results in devices enabling maximum power upon network attachment, which allows for larger client capacities. While this may be ideal for data applications that are capable of retransmitting dropped or lost packets, for voice applications this can result in very poor voice quality due to the potential for large numbers of dropped packets. Likewise, mobile provider data networks are susceptible to congestion and/or dropped connections, which can also result in poor voice quality and dropped calls.

Direct Connect Mobile Client Features and Functions

Direct connect mobile clients provide a range of features and functions. While the supported features and operations may vary from client to client, the features and behaviors described in this section apply to all direct connect mobile clients.

Call Routing

Because direct connect mobile clients are capable of making and receiving calls using the enterprise telephone infrastructure, it is important to understand the nature of call routing as it pertains to direct connect mobile client behavior.

Inbound Call Routing

While the direct connect mobile clients are able to register to Unified CM to leverage both dial-via-office and VoIP calling, depending on the network connectivity, inbound call routing behavior varies slightly. When the client is connected and registered to Unified CM over the enterprise WLAN network or through secure VPN to the enterprise, the client receives inbound calls to the enterprise number (whether sourced internally or from the PSTN) just like a registered IP desk phone. If the user has a desk phone, the inbound call rings the shared line on both the mobile client device and the desk phone. On the other hand, if the client is not connected to the enterprise network directly or through a secure remote connection, then inbound calls to the enterprise number (whether sourced internally or from the PSTN) will ring the mobile number of the device provided that the user has been enabled for Cisco Unified Mobility and Mobile Connect (single number reach) is enabled for the user's direct connect client device mobile number. As with dual-mode client devices, incoming calls to the enterprise numbers are not extended to the mobile number of the direct connect client device through Mobile Connect if the client device is connected to the enterprise network and registered to Unified CM.

In all cases, incoming calls made directly to the direct connect client device's mobile phone number will always be routed directly to the device on the mobile network, unless the provider network or device settings are such that calls are not extended to the device by the mobile network. This is considered appropriate behavior because these calls were not made to the user's enterprise number. They would be considered personal calls, and as such should not be routed through the enterprise.

Outbound Call Routing

Depending on the nature of network connectivity for the direct connect mobile client device, outbound call routing behavior will be slightly different. If the device is connected to the enterprise WLAN and registered to Unified CM, then outbound calls, whether destined for internal enterprise numbers or external PSTN numbers, are routed by means of the enterprise telephony infrastructure based on the dial plan configuration within Unified CM. If instead the device is securely connected to the enterprise through the mobile data network or through a public or private Wi-Fi hot spot, then depending on the quality of the connection, outbound call routing is facilitated by either VoIP or the dial-via-office feature within Unified CM. In the case of dial-via-office, call signaling traverses the mobile data connection to the enterprise, and voice media traverses the mobile voice network and PSTN. If no enterprise connectivity is available, then outbound calling is not possible from the enterprise number, and instead calls would have to leverage the mobile number of the direct connect client device for making calls over the mobile voice network. Alternatively, users may leverage the two-stage dialing features provided with Cisco Unified Mobility (see Mobile Voice Access and Enterprise Feature Access, page 25-49).

Dial Plan

Dial-via-office and VoIP calling enable the direct connect mobile client to dial outgoing calls using enterprise dialing methods including use of abbreviated extension dialing and PSTN and inter-site steering digit dialing. However, in situations in which the dial-via-office feature or VoIP calling is not available due to lack of enterprise connectivity, enterprise dialing methods are not possible and users must dial outgoing calls using full-length E.164 number dialing as required on mobile voice networks and the PSTN.

While enterprise dialing may allow for convenience of abbreviated dialing, because of the differences between enterprise dialing and PSTN or mobile voice network dialing, normalization of required dialing patterns is recommended so that users dial the same number to reach a called destination whether they are connected to the enterprise or not. By normalizing the dial plan and dialing behavior within Unified CM for direct connect mobile client users, administrators are able to provide the best possible end-user dialing experience so that users do not have to be aware of whether the client device is connected to the enterprise and registered to Unified CM.

For more information on dial plan normalization for mobile clients, see the section on dual-mode phones and clients Dial Plan, page 25-70.

Caller ID

When direct connect mobile client devices are connected to the enterprise (directly, or through a public or private Wi-Fi hot spot or over the mobile data network) and registered to Unified CM, all calls made by dial-via-office or over the IP network will be routed with the user's enterprise number as caller ID. This ensures that returned calls made from call history lists at the far end are always routed through the enterprise because the return call is to the user's enterprise number. If the direct connect mobile client user has been enabled for Cisco Unified Mobility, and Mobile Connect is turned on for the direct connect client device mobile number, return calls to the enterprise number will also be extended to the direct connect mobile client device through the PSTN whenever the client device has no enterprise network connectivity.

Emergency Services

As with other mobility client solutions, direct connect mobile clients can present challenges when it comes to making emergency calls to public service numbers such as 911, 999, and 112. Because the direct connect mobile client device may be located inside or outside the enterprise, providing location indication in the event of an emergency must be considered. Mobile phones already receive location services from their provider networks, and these location services are always available and typically able to pinpoint locations far more precisely than enterprise wireless networks; therefore, Cisco recommends relying on the mobile voice network for making emergency calls and determining device and user

location. To ensure that direct connect mobile client devices rely exclusively on the mobile voice network for emergency and location services, Unified CM will force all calls made to numbers configured in the Emergency Numbers field on the direct connect client device configuration page to route over the mobile voice network.

External Call Routing

When the direct connect mobile client device is located outside the enterprise and has no enterprise connectivity, it may make and receive calls only through the mobile voice network. Unified CM will have no visibility to these directly dialed calls on the mobile voice network because they are not anchored in the enterprise. As a result, users will not be able to invoke enterprise mid-call features or perform desk phone pickup for these calls. In these situations, if made available by the system administrator, users can leverage Unified Mobility Enterprise Feature Access or Mobile Voice Access two-stage dialing features to anchor the calls in the enterprise.

Dial-via-Office

Dial-via-office functionality provides the ability for direct connect mobile clients to initiate calls from the mobile phone using the Cisco Unified CM telephony infrastructure and enterprise PSTN gateway. This functionality is facilitated by SIP signaling over the IP network connection between the direct connect mobile client and Unified CM. Utilization of dial-via-office can be mandated by the Unified CM system administrator, or the administrator may choose to allow users to decide whether they want to use dial-via-office or dial their calls directly over the mobile voice network. As previously mentioned, calls to emergency numbers (as configured in the Emergency Numbers field on the direct connect client device configuration page) will always be dialed directly over the mobile voice network even when dial-via-office calling has been mandated.

Dial-via-office operation and behavior is nearly identical to that described for the Cisco Unified Mobile Communicator solution (see Dial-via-Office, page 25-93), with the only difference being that the Cisco Unified Mobility Advantage server and Cisco Unified Mobile Communication client are not involved. Instead the communication for dial-via-office call setup occurs directly between the direct connect mobile client and Unified CM over the IP network connection.

Just as with the Cisco Unified Mobile Communicator solution, direct connect mobile clients can perform either Dial-via-Office Reverse Call Back (DVO-R) or Dial-via-Office Forward (DVO-F) operations.

See Dial-via-Office, page 25-93, for more information about dial-via-office call flows and operation.

Session Resumption

Beginning with Cisco Unified CM 8.5, direct connect mobile client users are able to redial Dial-via-Office Forward calls during a call set up or network failure. With Unified CM 8.5 and later releases, the system caches the last target number the user dialed for the amount of time specified in the Redial Await Timer service parameter. By default, the target number will be cached for three minutes. Given a call set up or network failure, if the user presses the redial softkey or selects the last call in the call history list of the mobile phone, the system will automatically reconnect the user to the last dialed number by means of the Dial-via-Office Forward feature, provided the Redial Await Time has not expired.

Note The Session Resumption or Dial-via-Office Forward Redial feature provided in Unified CM 8.5 and later releases may also be used with both new and existing deployments of Cisco Unified Mobile Communicator 7.*x* clients and Cisco Unified Mobility Advantage 7.1(3) that are capable of Dial-via-Office Forward. No configuration changes are required on Unified Mobile Communicator or Unified Mobility Advantage in order to leverage this feature.

Mobile Toll Bypass Optimization

In order to provide least-cost routing for dial-via-office calls, beginning with Cisco Unified CM 8.5, administrators can configure multiple enterprise feature access numbers on the system for use by the dial-via-office operation. In addition these numbers can be assigned to users through a new mobility profile configuration construct. By allowing multiple enterprise feature access numbers, the system can accommodate local access numbers for Dial-via-Office Forward calls as well as locally significant caller IDs for Dial-via-Office Reverse calls. The Dial-via-Office Forward access numbers and Dial-via-Office Reverse caller IDs can be based on geographic location of users according to assignment of geographically appropriate mobility profiles.

The Mobile Toll Bypass Optimization feature involves first configuring multiple enterprise feature access numbers on the system, each corresponding to a specific geographic location. On a globally deployed system, the administrator would provide local access numbers or DIDs for locations throughout the world based on user populations and office locations. As an example, local numbers might be configured for US cities San Jose, New York, and Miami as well as London, England, Berlin, Germany, and Tokyo, Japan.

Next these multiple access numbers are assigned to users based on configuration of mobility profiles. A mobility profile would be created for each geographic location and assigned to users in that location. For example, mobility profiles would be configured for users in San Jose, New York, Miami, London, Berlin, and Tokyo, with each profile containing the locally significant access number of DID for that particular geographic location. In this way, users in each of these locations will be able to access Dial-via-Office Forward services using a local number rather than a long distance or international number. By providing local numbers for each geographic location, cost savings can be realized due to the less expensive billing rates typically provided for local calls.

Each mobility profile is configured with up to three different numbers depending on dial plan and dial-via-office method. Under the Dial-via-Office Forward portion of each profile, the administrator may configure an Enterprise Feature Access Number and a Service Access Number. The Service Access Number and Enterprise Feature Access Number are used as a pair, with the Service Access Number serving as the E.164 form of the Enterprise Feature Access Number when it has been configured in abbreviated form. If the Enterprise Feature Access Number is configured as the full E.164 form, then the Service Access Number does not have to be configured. One or both of these numbers are used for Dial-via-Office Forward operations as the number forwarded by the system to the direct connect mobile client and, in turn, the number the client uses to call into the system to complete a Dial-via-Office Forward call. The other number that may be configured on the mobility profile is the CallBack Caller ID number under the Dial-via-Office Reverse Callback portion of each profile. This number specifies the caller ID that the Unified CM system uses when placing outbound calls to the direct connect mobile client device on the PSTN for Dial-via-Office Reverse Callback calls.

The mobility profile also contains the Mobile Client Calling Option field, which enables the system administrator to specify either Dial-via-Office Reverse or Dial-via-Office Forward when dial-via-office calls are made. This provides administrative control over the dial-via-office call direction that a mobile client uses and enables the administrator to force use of the least expensive method for making a dial-via-office call.

Mobility profiles should be assigned to users based on the location where the user will typically use the client. If a user moves between geographic locations, the administrator will have to assign the user manually to a different profile based on the new location. The system does not dynamically update the mobility profile based on a user's location.

Mobility profiles can be assigned only to mobile devices configured with mobility identities and capable of leveraging the dial-via-office feature. Direct connect mobile clients such as Cisco Mobile 8.5 for Nokia as well as the older Cisco Unified Mobile Communicator clients are devices configured with a mobility identity and capable of dial-via-office. Mobility profiles cannot be configured for regular Unified Mobility remote destinations.

Note The Mobile Toll Bypass Optimization feature provided in Unified CM 8.5 and later releases may be used with both new and existing deployments of Cisco Unified Mobile Communicator 7.*x* clients and Cisco Unified Mobility Advantage 7.1(3). No configuration changes are required on Unified Mobile Communicator or Unified Mobility Advantage in order to leverage this feature. The Unified Mobility Advantage server will automatically use the access numbers forwarded to it by Unified CM 8.5 and later releases. However, the Mobile Client Calling Option field, where the administrator can indicate Dial-via-Office Reverse or Dial-via-Office Forward, has no impact on dial-via-office call flow for Cisco Unified Mobile Communicator devices. Dial-via-office direction for Cisco Unified Mobile Communicator clients is controlled exclusively by the client itself.

Additional Services and Features

In addition to dial-via-office and VoIP call processing or call control services, direct connect mobile client are capable of providing the features and services described in this section.

XMPP-Based IM and Presence

Cisco Mobile 8.5 for Nokia and the Cisco Jabber IM direct connect mobile clients support the use of Extensible Messaging and Presence Protocol (XMPP) for enterprise IM and presence services through integration to either an on-premises Cisco Unified Presence server or an off-premises Cisco WebEx Connect cloud service. In both cases, the IM and presence capabilities of these direct connect mobile client allow the following:

- Adding users to contact or buddy lists
- Setting and propagating user presence and availability status
- Reception of presence status for a buddy or contact
- Creating and sending of instant messaging (IM) or text messages
- Reception of IM or text messages
- Escalation of an IM or text message to a voice call

A Cisco Jabber IM client is available for Apple iOS iPhone, iPod Touch, and iPad devices with a minimum Apple iOS version of 4.2. A Cisco Jabber IM client is also available for a wide range of BlackBerry devices running BlackBerry OS 4.6 and later versions.

Cisco Jabber IM enables cross-launch of the Cisco Jabber mobile client (if installed) for VoIP calling. In turn, Cisco Jabber mobile clients are able to cross-launch Cisco Jabber IM (if installed) for contact-based enterprise IM and chat.

For more information on Cisco Jabber IM clients, refer to the *Cisco Jabber IM for BlackBerry* data sheet, available at http://www.cisco.com/en/US/products/ps11763/products_data_sheets_list.html, and the *Cisco Jabber IM for iPhone* data sheet, available at http://www.cisco.com/en/US/products/ps11596/products_data_sheets_list.html.

Corporate Directory Access

Direct connect mobile clients are capable of accessing an enterprise directory for directory lookups using LDAP, provided the client device is connected to the enterprise through either a mobile data network or WLAN. While this is not a required feature for direct connect mobile clients, it does provide productivity improvements for direct connect client users when they are able to access corporate directory information from their mobile phones.

Enterprise MWI and Message Count Indication

Direct connect mobile clients are also capable of accessing enterprise voicemail services. Direct connect clients are able to receive enterprise message waiting indication (MWI) and message count, and/or access their enterprise voicemail box visually. Direct connect mobile clients must be connected to the enterprise network (through a mobile data network or WLAN) in order to receive MWI and message count indication or to access visual voicemail.

Just as with regular enterprise phones, direct connect mobile clients can also be used to retrieve enterprise voicemail messages by dialing into the voicemail system number and navigating to the appropriate voicemail box after providing required credentials.

Mobile Connect On/Off

If integrated with Unified Mobility and enabled for Mobile Connect, direct connect mobile clients are able to view Mobile Connect status and turn Mobile Connect on or off through the client settings interface. This allows users to enable or disable Mobile Connect or single number reach functionality for the direct connect mobile client device mobile number even when connected to the enterprise remotely over the mobile data network.

Direct Connect Mobile Client: Cisco Mobile 8.5 for Nokia

Note End-of-Sale for the Cisco Mobile 8.5 for Nokia client is July 10, 2012. There is no replacement mobile client for Nokia mobile devices. For more information, see the End-of-Sale (EoS) and End-of-Life (EoL) announcement at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7290/ps10589/end_of_life_notice_c51-696647.html.

Cisco Mobile 8.5 for Nokia is a direct-connect mobile client for Nokia mobile smart phones. Once installed on the Nokia device, the client can associate to either the local enterprise WLAN network or remotely to the enterprise through the mobile data network. The client registers to and communicates with Unified CM.

To provide registration and dial-via-office services to Cisco Mobile 8.5 direct connect mobile clients, Unified CM must support the appropriate Nokia S60 device type, which is available only after loading the necessary Cisco Options Package (COP) file onto Unified CM. The COP file (cmterm-nokia_s60_8.5.2v06-sccp.cop.sgn) can be found at the following location:

http://www.cisco.com/cisco/software/release.html?mdfid=281001428&release=8.5(2)&flowid=&softwareid=282074304&os=null

Once the COP file is installed and the direct connect client device has been configured within Unified CM, it is necessary to load the Cisco Mobile 8.5 for Nokia client onto the Nokia device. This can be done using a computer with a USB, Bluetooth, or infrared port. After the Cisco Mobile 8.5 Symbian installation system (SIS) file has been loaded on the Nokia device, the device must at a minimum be configured to access the local enterprise WLAN for connectivity based on the enterprise WLAN infrastructure and security policies. Additional configuration is required in order to enable remote enterprise network connectivity using a VPN.

To integrate the Cisco Mobile 8.5 Nokia device with Unified Mobility so that the user can leverage features such as Mobile Connect, configure the Nokia mobile phone number as a mobility identity and associate it to the Nokia S60 device within Unified CM.

The Cisco Mobile 8.5 client is supported on Nokia handsets running Symbian Series 60 Third Edition Feature Pack 1 (3.1) or Feature Pack 2 (3.2) firmware. Example devices include the Nokia E55, E66, E71, E72, and E75.

Nokia mobile phone WLAN interfaces typically support 802.11b and 802.11g network connectivity.

The Cisco Mobile 8.5 client not only provides dial-via-office voice services but also provides directory lookup services when configured to point to an LDAP compliant directory, and it provides XMPP-based presence and IM when integrated with Cisco Unified Presence or Cisco WebEx Connect.

For information about system requirements and supported devices, refer to the release notes for Cisco Mobile 8.5 for Nokia, available at

http://www.cisco.com/en/US/docs/voice_ip_comm/cumc/cisco_mobile/nokia/8_x/Release_Notes/Cisco_Mobile_Nokia_8_x_RN.html

For installation and configuration information for Cisco Mobile 8.5 for Nokia, refer to the administration guide available at

http://www.cisco.com/en/US/docs/voice_ip_comm/cumc/cisco_mobile/nokia/8_x/admin/Cisco_Mobile_for_Nokia_8.5_Admin_Guide.html

Co-Residency of Cisco Mobile 8.5 with Nokia Call Connect

In order to support dual-mode voice over IP (VoIP) functionality, Cisco Mobile 8.5 must be installed co-resident with the Nokia Call Connect dual-mode client on the device. The Nokia Call Connect client provides support for VoIP calling. Both clients are associated to the Nokia S60 device configuration for the Nokia device within Unified CM.

When running co-resident, the Nokia Call Connect dual-mode client behaves as previously described in the section on Dual-Mode Clients: Nokia Call Connect, page 25-80. Operation and deployment of the Nokia Call Connect dual-mode client co-resident with Cisco Mobile 8.5 is identical in operational and functional behavior to a standalone Nokia Call Connect dual-mode client installation. The same design and deployment requirements related to handoff operations and configuration must be considered. Likewise, all design recommendations and requirements covered in the section on Wireless Device Roaming, page 25-15, apply to the Nokia Call Connect client running co-resident with Cisco Mobile 8.5.

When deploying co-resident Cisco Mobile 8.5 and Nokia Call Connect clients, the Unified CM administrator should not force dial-via-office. Instead the Dial Policy parameter on the Nokia S60 device configuration page should be configured as **Let User Choose**. This gives the user maximum control over when dial-via-office will be used, thus ensuring that this feature is used only when the user is not connected to the enterprise or when voice quality over the IP network is poor.

If the administrator must force dial-via-office for Cisco Mobile 8.5, the user should configure the **Allow dial via office for** setting to **Calls from this app** within the Cisco Mobile 8.5 client so that only calls made directly from within the client application will attempt to invoke dial-via-office. By configuring the client this way, the user can ensure that dial-via-office will not be engaged unexpectedly. If the Cisco Mobile 8.5 client is not in the foreground, then the user can be sure that dial-via-office will not be invoked.

When running these two clients co-resident, consider the following:

- The Nokia Call Connect dual-mode client should be used for making and receiving VoIP calls when WLAN or mobile data network connection signal strength is strong and reliable.
- If voice quality is poor or IP connectivity is unreliable, then the Cisco Mobile 8.5 direct connect client should be used for dial-via-office calls.

In all cases, users should use dial-via-office only when the direct connect mobile client device is outside the enterprise or when voice quality over the IP network connection is poor.

Interactions Between Cisco Mobile 8.5 and Cisco Unified Mobility

The Cisco Mobile 8.5 direct connect mobile client for Nokia can be integrated with Cisco Unified Mobility to leverage Cisco Mobile Connect, mid-call DTMF features (when mobile data connection or WLAN connection is unavailable), single enterprise voicemail box, and desk phone pickup.

Integration with Unified Mobility requires the Nokia direct connect client device mobile phone number to be configured within Unified CM as a mobility identity associated with the Nokia S60 device. Once the mobile number is configured as a mobility identity within the system, Mobile Connect can be leveraged so that incoming calls to the user's enterprise number will be extended to the Nokia direct connect client device through the mobile voice network. The Mobile Connect feature can also be enabled or disabled remotely within the Cisco Mobile 8.5 client. In situations where the Nokia device is also running Nokia Call Connect dual-mode client, when the device is connected to the enterprise and registered to Unified CM, an inbound call to the enterprise number will not be extended to the mobile voice network interface of the device. When the Nokia device is connected to the enterprise, the device will receive the inbound call through the IP network. This prevents unnecessary consumption of enterprise PSTN gateway resources.

When outside the enterprise, if a public or private Wi-Fi hot spot or the mobile data network is reachable from the Nokia device and secure connectivity to the enterprise is available, the Cisco Mobile 8.5 client can use VoIP or dial-via-office for making outbound calls, depending on the quality of the enterprise connection. However, if no IP network connectivity is available, the user can still make enterprise calls by using the Unified Mobility two-stage dialing features Mobile Voice Access or Enterprise Feature Access. Further, for any enterprise anchored call (dial-via-office, two-stage dialed, or direct dialed enterprise numbers as well as Mobile Connect), users can move an active call to their desk phones by using the Move Call to Desk feature of the Cisco Mobile 8.5 client. And if enterprise connectivity is not available, mid-call features may be invoked by means of DTMF feature access codes.

In addition to configuring a mobility identity for the Nokia direct connect mobile client device, you can configure additional mobile phone numbers or off-system phone numbers as remote destinations and associate them to the Nokia S60 device within Unified CM. When associating the mobility identity and additional remote destinations to the Nokia device, you do not have to configure a remote destination profile. If existing Nokia mobile phone users are already enabled for Unified Mobility and are being migrated to Cisco Mobile 8.5, the existing remote destination profile should be removed and any configured remote destinations should be deleted and re-added directly to the Nokia S60 device. This is necessary because remote destination and mobility identities must be unique within the Unified CM system.

For more information about the Cisco Unified Mobility feature set as well as design and deployment considerations, see Cisco Unified Mobility, page 25-38.

High Availability for Direct Connect Mobile Clients

Although direct connect mobile client devices by their nature are highly available with regard to network connectivity (when connectivity to the enterprise network over WLAN or mobile data network is unavailable, the mobile voice network can be used for voice), enterprise WLAN, VPN infrastructure, and IP telephony infrastructure high availability must still be considered.

First, the enterprise WLAN must be deployed in a manner that provides redundant WLAN access. For example, APs and other WLAN infrastructure components should be deployed so that the failure of a wireless AP does not impact network connectivity for the direct connect mobile client. Likewise, WLAN management and security infrastructure must be deployed in a highly redundant fashion so that dual-mode devices are always able to connect securely to the network. Controller-based wireless LAN infrastructures are recommended because they enable centralized configuration and management of enterprise APs, thus allowing the WLAN to be adjusted dynamically based on network activity and AP failures.

Next, VPN infrastructure components, including Cisco IOS or ASA head-end VPN or AnyConnect session terminator, should be deployed in a highly redundant fashion so that loss of a VPN session terminator does not impact or prevent remote enterprise connectivity for the mobile client.

Unified CM call processing and registration service high availability must also be considered. Just as with other devices within the enterprise that leverage Unified CM for call processing services, direct connect mobile clients must register with Unified CM. Given the redundant nature of the Unified CM cluster architecture, which provides primary and backup call processing and device registration services, direct connect mobile client device registration as well as call routing is still available even in scenarios in which a Unified CM server node fails.

Similar considerations apply to PSTN access. Just as with any IP telephony deployment, multiple PSTN gateways and call routing paths should be deployed to ensure highly available access to the PSTN. This is not unique to direct connect mobile client deployments, but is an important consideration nonetheless.

Capacity Planning for Direct Connect Mobile Clients

Capacity planning considerations for direct connect mobile clients are the same as for other IP telephony endpoints or devices that rely on the IP telephony infrastructure and applications for registration, call processing, and PSTN access services.

When deploying direct connect mobile clients, it is important to consider the registration load on Unified CM as well as the Unified Mobility limits. A single Unified CM cluster is capable of handling a maximum of 40,000 device configurations and registrations. When deploying direct connect mobile client devices, you must consider the per-server maximum device support, and you might have to deploy additional call processing subscriber nodes or even clusters to handle the added load.

In addition, as discussed in Capacity Planning for Cisco Unified Mobility, page 25-63, the maximum number of remote destinations and mobility identities within a single Unified CM cluster is 15,000. Because most direct connect mobile clients will likely be integrated with Unified Mobility to take advantage of features such as Mobile Connect and desk phone pickup, the mobile phone number of each of these direct connect client devices must be configured as a mobility identity within the Unified CM cluster. This is necessary to facilitate integration to Unified Mobility as well as to facilitate handoff in some cases. Therefore, when integrating these direct connect client devices with Unified Mobility, it is important to consider the overall remote destination and mobility identity capacity of the Unified CM cluster to ensure sufficient capacity exists. If additional users or devices are already integrated to Unified Mobility within the system, they can limit the amount of remaining remote destination and mobility identity capacity available for direct connect client devices.

Overall call processing capacity of the Unified CM system and PSTN gateway capacity must also be considered when deploying direct connect mobile clients. Beyond handling the actual client device configuration and registration, the system must also have sufficient capacity to handle the added BHCA impact of these devices and users. Likewise, it is critical to ensure that sufficient PSTN gateway capacity is available to accommodate direct connect clients.

The above considerations are certainly not unique to direct connect client devices. They apply to all situations in which devices and users are added to Unified CM, resulting in additional load to the overall Unified Communications System.

For more information on general system sizing, capacity planning, and deployment considerations, see the chapter on Unified Communications Design and Deployment Sizing Considerations, page 29-1.

Design Considerations for Direct Connect Mobile Clients

Observe the following design recommendations when deploying direct connect mobile clients:

- Cisco recommends that direct connect mobile client users rely on the mobile voice network for making emergency calls and determining device and user location. This is because mobile provider networks typically provide much more reliable location indication than enterprise WLAN networks. To ensure that these client devices rely exclusively on the mobile voice network for emergency and location services, ensure that emergency numbers such as 911, 999, and 112 have been configured in the Emergency Numbers field on the direct connect client device configuration page to force all calls made to these numbers to be sent over the mobile voice network.
- When deploying direct connect mobile clients for users across geographic locations, consider using the Mobile Toll Bypass Optimization feature in order to assign location-specific system access numbers for dial-via-office. In scenarios where the dial-via-office direction impacts call cost, consider the use of the mobility profile Mobile Client Calling Option field in order to force a specific dial-via-office direction (forward or reverse).
- In deployments where both the Cisco Mobile 8.5 direct connect client and Nokia Call Connect dual-mode are deployed on the same handset, Cisco recommends the following:
  - Follow all recommendations and requirements related to voice over WLAN as outlined in the section on Wireless Device Roaming, page 25-15.
  - Follow all recommendations and requirements related to configuration and deployment of the Nokia Call Connect as outlined in the section on Dual-Mode Phones and Clients, page 25-66.
  - When dual-mode functionality is enabled, the Unified CM administrator should not force dial-via-office. Instead the Dial Policy parameter on the Nokia S60 device configuration page should be configured as **Let User Choose**.
  - If the administrator forces dial-via-office for Cisco Mobile 8.5, the user should configure the **Allow dial via office for** setting to **Calls from this app** Cisco Mobile 8.5 client so that only calls made directly from within the client application will attempt to invoke dial-via-office. By configuring the client this way, the user can ensure that dial-via-office will not be engaged unexpectedly. If the Cisco Mobile 8.5 client is not in the foreground, then the user can be sure that dial-via-office will not be invoked.
- Consider the following as it relates to making calls with the Cisco Mobile 8.5 and Nokia Call Connect clients running co-resident:
  - The Nokia Call Connect dual-mode client should be used for making and receiving voice over IP (VoIP) calls when the WLAN or mobile data connection signal strength is strong.
  - If voice quality is poor or IP network connectivity is unavailable, then the Cisco Mobile 8.5 direct connect client should be used for dial-via-office calling.