Dial Plan

Revised: November 19, 2013; OL-30952-01

The dial plan is one of the key elements of a Unified Communications and Collaboration system, and an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. Specifically, the dial plan performs the following main functions:

- Endpoint addressing

  For destinations registered with the call processing agent, addresses are assigned to provide reachability. These internal destinations include all endpoints (such as IP phones, video endpoints, soft clients and analog endpoints) and applications (such as voicemail systems, auto attendants, and conferencing systems).

- Path selection

  Depending on the calling device and the destination dialed, a path to the dialed destination is selected. If a secondary path is available, this path will also be considered if the primary path fails.

- Calling privileges

  Different groups of devices can be assigned to different classes of service, by granting or denying access to certain destinations. For example, lobby phones might be allowed to reach only internal and local PSTN destinations, while executive phones could have unrestricted PSTN access.

- Manipulation of dialed destination

  On the path from the dialing device to the dialed destination, the dial plan can apply manipulations to the dialed destination. For example, users in the US might dial 9011496901234 to reach a destination in the PSTN in Germany, while a user in France might be able to reach the same destination by dialing 000496901234. This dialed destination would need to be presented as 011496901234 to a PSTN trunk on a gateway in the US and as 00496901234 to a PSTN trunk on a gateway in France.

- Presentation of information about identities involved in the call

  During session establishment and also while in the call, on both the calling and the called device, information about the other device is displayed. Depending on call state and direction, this includes calling, diverting, alerting, and connected party information. The dial plan can define mappings that influence the format and content of information displayed.

This chapter presents information intended to guide the system designer toward a dial plan that accommodates the legacy dialing habits of telephony and video users, while also taking advantage of new functionality afforded by the increasing integration between computing technology and telephony, such as dialing from contacts, click-to-call actions from computers and smart phones, and adoption of mobility-related features. The chapter is structured to offer information about the following main areas:

- Dial Plan Fundamentals, page 14-2

  This section covers general concepts commonly used in enterprise voice and video dial plans.

- Dial Plan Elements, page 14-13

  This section introduces the various dial plan elements available in the architectural elements of an enterprise collaboration solution, including Cisco Unified Communications Manager (Unified CM) and Cisco TelePresence Video Communication Server (VCS).

- Recommended Design, page 14-53

  This section contains design guidelines related to multisite collaboration networks, endpoint addressing, and building classes of service. Also, dial plan integration between Unified CM and VCS is covered.

- Special Considerations, page 14-76

For more details, refer to the *Cisco Unified Communications Manager System Guide*, the *Cisco Unified Communications Manager Features and Services Guide*, the Cisco IOS Voice and Video Configuration guides, and other product documentation available at

http://www.cisco.com

What's New in This Chapter

Table 14-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 14-1   New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in	Revision Date
Global Dial Plan Replication (GDRP)	• Global Dial Plan Replication, page 14-46 • Dial Plan with Global Dial Plan Replication (GDPR), page 14-69 • Various other sections of this chapter	November 19, 2013

Dial Plan Fundamentals

Developing an end-to-end enterprise dial plan requires a sound understanding of a number of concepts that are independent of specific products. This section provides an overview of those concepts, including:

- Endpoint Addressing, page 14-3

- Dialing Habits, page 14-5

- Dialing Domains, page 14-6

- Classes of Service, page 14-7

Endpoint Addressing

Reachability of endpoints registered to a call processing agent, users, and applications is provided by addresses assigned to these addressable entities. In enterprise collaboration networks we differentiate between numeric addresses and alphanumeric uniform resource identifiers (URIs).

Numeric Addresses (Numbers)

Numeric addresses are represented by a sequence of digits. The call control agent does not assume, preclude, or require a special structure for numeric addresses. The decision on the structure of the numeric addresses to be used in the dial plan is part of the dial plan design process.

ITU recommendation E.164 defines the fundamental structure of numeric geographical addresses (phone numbers) to be used in the PSTN, as shown in Figure 14-1.

Figure 14-1   E.164 Format for Geographic Numbers

CC 1 to 3 digits	NSN Maximum of 15-n digits (n = number of CC digits)	
	NDC Defined by National Numbering Plan	SN Defined by National Numbering Plan
Maximum of 15 digits		

The following definitions apply to Figure 14-1:

- CC = Country Code
- NSN = National Significant Number
- NDC = National Destination Code
- SN = Subscriber Number

According to ITU recommendation E.164, the maximum length of any phone number is 15 digits. The first part of a geographic E.164 number is the country code. Country codes are between one and three digits long (country code 1 and 7 are the only single-digit country codes). The remainder of a geographic E.164 number is the national significant number (NSN). The general structure of a NSN is that the first few digits represent a national destination code (NDC), or area code, and the last digits represent the subscriber number. ITU recommendation E.164 does not define national numbering plans and thus does not prescribe the schema to be used for NSNs in specific countries. This is left to the national numbering plan authorities. A collection of documentation on various national numbering plans can be found at

http://www.itu.int/oth/T0202.aspx?parent=T0202

National numbering plans can be very different in structure. As an example, Table 14-2 compares the numbering plans used in the US and in Germany.

Table 14-2   Comparison of Numbering Plans in the US and Germany

Country Code	NSN Length	NDC Length	SN Length
1 (US)	10	3	7
49 (Germany)	3 to 13	2 to 5	4 to 11 (depending on area code)

ITU recommendation E.164 also mentions that a leading "+" should be used to indicate if an international prefix is required. Throughout this design guide we consistently use the term "E.164" to refer to E.164 numbers and "+E.164" to refer to E.164 numbers with a leading "+".

Using +E.164 numbers as numeric addresses has the benefit that these numbers by definition are unique and that it is very easy to map between +E.164 and any habitual dialing that might be required to be supported by an enterprise dial plan.

As an alternative to using unique numeric +E.164 addresses, numeric addresses following an enterprise numbering plan may also be used. Building an enterprise address plan or numbering scheme in multi-site deployments involves the definition of a typical hierarchical addressing structure with the following characteristics:

- Provides unique numeric addresses for all endpoints, users, and applications in the enterprise.
- Needs to be extensible so that the numbering scheme allows for adding new sites without having to redesign the whole numbering scheme, which would involve address reassignments for existing endpoints, users, and applications.

In a typical enterprise numbering plan, numerical addresses would consist of a site code and a site subscriber number. When designing an enterprise numbering plan, reserve enough digits for both the site code and the site subscriber number to make sure that additional sites can be added if required and enough subscriber numbers can be defined per site. Enterprise numbering plans typically are designed to be fixed length.

If or when dialing of addresses defined by an enterprise numbering plan needs to be supported directly as a dialing habit, typically a single-digit access code is selected and prefixed to the enterprise number. In that case a full enterprise numbering address would have three pieces: enterprise address access code (for example, 8), site code (for example, 496), and site subscriber number (for example, 9123); or for example, 8-496-9123.

The enterprise address access code in this case needs to be selected so that it does not cause overlap with any other dialing habit (see Dialing Habits, page 14-5).

To be able to uniquely identify an addressable entity, either all addresses have to be unique or they at least have to be unique within a defined sub-domain managed by the call processing agent. If two distinct entities need to be addressed using the same address, then the two identical addresses have to reside in disjunct addressing domains that are managed independently. With numeric addresses, this situation can occur if site-significant numeric addresses (for example, a four-digit extension) are used and two endpoints with the same site-significant address (same four-digit extension) in different sites need to be addressed by the same call control agent. Table 14-3 shows an example of this situation.

Table 14-3   Overlapping Numeric Addressing

+E.164 Number	Site (Sub-Domain)	Site DID Range	4-Digit DN (Address)
+49 690 773 3001	Frankfurt	+49 690 773 3XXX	3001
+1 408 555 3001	San Francisco	+1 408 555 3XXX	3001

In Table 14-3, two E.164 numbers result in the same site-specific four-digit directory number based on the respective site's DID range. This implies that the four-digit DNs cannot be used as numeric endpoint addresses directly.

Alphanumeric Addresses

Alphanumeric addresses based on SIP URIs can also be used to address endpoints, users, and applications. A commonly used scheme for alphanumeric addresses is simplified SIP URIs of the form *user@host*, where the left-hand side (LHS, user portion) can be alphanumeric and the right-hand side (RHS, host portion) is a domain name. The following examples represent valid alphanumeric addresses based on SIP URIs:

- bob@example.org
- bob.home-office@example.org
- bob@de.eu.example.org
- bob.ex60@example.org
- bob.vmbox@example.org
- voicemail@de.eu.example.org

All of these URIs can serve as individual alphanumeric addresses for individual endpoints, users, and applications. From the addressing perspective, any hierarchy implied by using dot-separated identifiers (bob.ex60, de.eu.example.org) does not have any impact on the decision of whether any two URIs are considered to be equivalent.

According to RFC 3261, comparison of the LHS of SIP URIs has to be case-sensitive, while the RHS has to be compared case-insensitive. According to this standardized behavior, Alice@example.com and alice@example.com are not to be considered equivalent and thus represent distinct individual addresses. In reality, using addressing schemes for endpoints, users, and applications that rely on case sensitivity of the user portion is considered bad practice because it leads to increased troubleshooting complexity. Also keep in mind that RFC 2543 (the RFC specification preceding RFC 3261) explicitly defined that SIP URIs (host and user portion) are case-insensitive. Different behaviors regarding the case sensitivity of URI equivalence are common. To avoid problems, Cisco highly recommends always using only all lowercase URIs as alphanumeric addresses.

Starting with Cisco Unified Communications Manager release 9.1 the URI lookup policy of Unified CM can be configured to be case-sensitive (default) or case-insensitive.

Dialing Habits

Dialing addresses of users, endpoints, and applications can be done using various formats. The numeric +E.164 address +496907739001, for example, could be dialed as any of the following:

- +496907739001
- 9011496907739001 from an enterprise extension in the US
- 011496907739001 from a land-line phone in the US
- 006907739001 from an enterprise extension in Germany
- 000496907739001 from an enterprise extension in Italy
- 9001 from a phone in the same office

These examples show that dialed addresses typically are interpreted in a context, and with the exception of dialing a +E.164 address directly, only the combination of dialed string and context provides proper identification of the intended destination address.

The term "dialing habit" is commonly used to refer to a given dialing behavior used to reach a given set of destinations. Examples of some "dialing habits" include:

- 9-0-1-1 plus E.164 for international destinations dialed from within the US
- 0-0 plus NSN for national calls in Germany
- 9-1 plus 10 digits for national calls in the US
- Four digits for intra-site calls in an office

A dialing habit is described by specifying both the format of the string to be dialed (address structure) and the destination address class to be reached. Examples of destination address classes typically used in enterprise dial plans include:

- On-net/intra-site
- On-net/inter-site
- Off-net/local
- Off-net/national
- Off-net/international
- Off-net/emergency
- Services (voicemail, pick-up, and so forth)

With alphanumeric dialing we typically differentiate only between fully qualified addresses and non-fully qualified addresses. Fully qualified addresses contain the user and the host portion of a SIP URI, whereas a non-fully qualified alphanumeric address represents only the user portion of the address and the host portion needs to be derived from the dialing context of the calling party. For example, dialing "bob" would be equivalent to dialing "bob@example.com" if the dialing context of the calling party defines that "@example.com" should be appended to all non-fully qualified alphanumeric addresses.

Dialing Domains

As described in the previous section, a given destination might be dialed using different strings by different users. A dialing domain specifies a group of users or devices sharing the same set of dialing habits (dialing the same strings to reach identical destinations). The concept of dialing domains is important because an enterprise dial plan has to implement the same treatment for each dialing domain. All users belonging to any given dialing domain share the same dialing treatment.

To identify dialing domains, it is important to take all dialing habits into consideration. Users in two sites in the US, even though they share the same PSTN dialing habits, would still belong to different dialing domains if we also take into account how on-net calls are placed. In a typical environment, an on-net intra-site call could be supported by dialing four digits, while an on-net inter-site call would be placed by using a dial string equivalent to the PSTN dialing habit (forced on-net would still keep the call on-net).

Figure 14-2 shows an example for this. Although endpoint 1234 in site SJC and endpoint 2001 in site RTP share the same dialing habit for national destinations (dialing 91212555600 to reach PSTN destination +1 212 555 6000) and international destinations (dialing 901149890123456 to reach PSTN destination +49 890 123456), the dialing habit to reach endpoint 1001 in site SJC is different for

endpoints in RTP than for those in SJC: endpoint 1234 in site SJC would dial 1001 while endpoint 2001 in site RTP would need to dial 914085551001. In this example, endpoints in site RTP and site SJC would belong to different dialing domains.

Figure 14-2   Dialing Domains
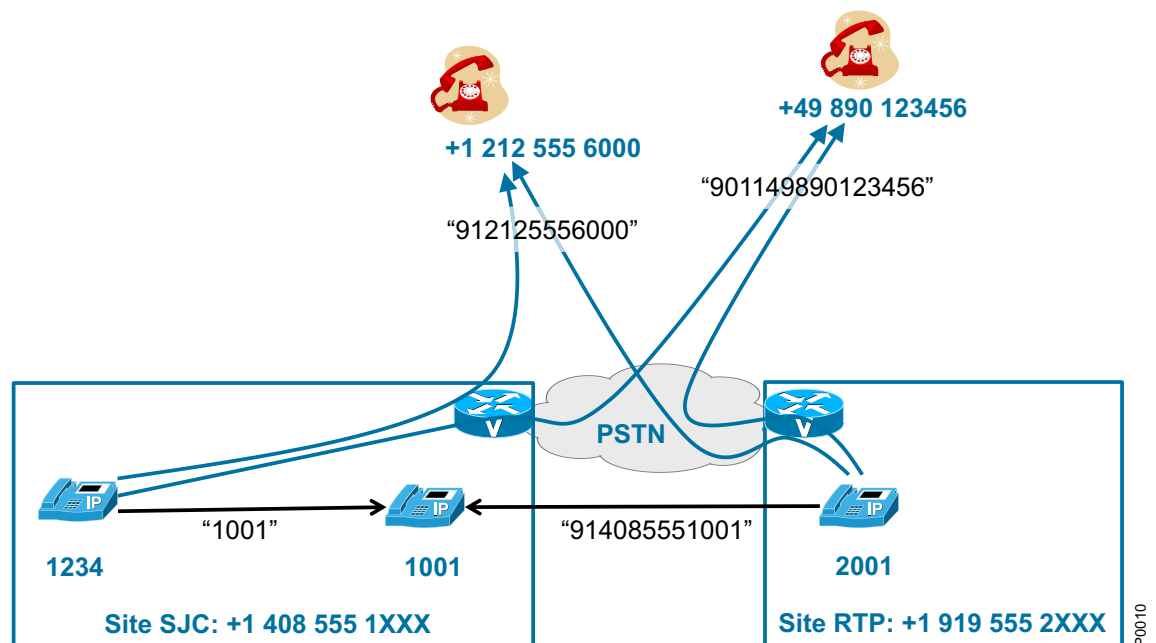
Classes of Service

Not all users, applications, and endpoints in an enterprise are allowed to reach the same set of destinations. Reasons for restricting the set of reachable destinations include cost avoidance, security considerations, and privacy. As examples, not all users might be able to place international calls, the voicemail systems might not be able to call any PSTN destination to avoid toll fraud, and only a very limited set of users might be allowed to place direct calls to the CEO of a company. The term generally used to refer to any given set of a restrictions or class of allowed destinations is *class of service*, or CoS.

Requirements for cost-driven classes of service heavily depend on the phone tariffs and the cost structure associated with them. With voice services becoming cheaper (or being available for free), the trade-off between the increased complexity associated with maintaining more classes of service and the potential savings in call costs is changing. In certain cases, for example, it might not make sense any more to differentiate between local and national calling if both call types are billed exactly the same.

The definition of a class of service might also be based on time schedules. Access to certain destinations might be allowed only at certain times.

Independent of restricting the access of certain users, devices, or applications to certain call types that incur costs, typically access to emergency services (911, 112, and so forth) has to be provided to all users at all times. Therefore, all classes of service have to allow access to emergency services at all times.

Call Routing

Routing calls involves several aspects:

- Identifying the dialing habit based on the structure of the dialed address.
- Allowing/blocking the call based on the class of service of the calling entity.
- Applying modifications to the dialed address.
- Applying modifications to the called party identification.
- Selecting a route to the called destination, establishing the call, and presenting the identity of the parties involved in the expected format. Route selection also involves selecting alternate routes if the primary route is not available for some reason.

An end-to-end enterprise dial plan needs to consider all of these aspects and is not limited only to establishing a route between the calling and called entities.

Identification of Dialing Habit and Avoiding Overlaps

The first step in the call routing process, after receiving the input from the calling entity, is to uniquely identify the dial habit used. In the case of alphanumeric dialing, this is a trivial task because in this case we typically only need to differentiate between fully qualified SIP URIs and non-fully qualified SIP URIs. This can easily be achieved through a simple lexical analysis of the dialed string.

The case of numeric dialing needs a little more attention, especially if the dialed digits are entered digit-by-digit. In this case the call control receives the destination from the calling entity digit-by-digit, and part of selecting the correct route to the destination is to determine the exact time when enough digits have been received and the call can be routed without having to wait for expiration of an inter-digit timeout.

Figure 14-3 shows some typical US dialing habits for PSTN and emergency calls. Although all of these dialing habits share the identical initial digit 9, international dialing and the first emergency dialing string can easily be distinguished as soon as the second digit (0 or 9) is dialed. As soon as the third digit is dialed, dialing 911 and dialing a national destination do not overlap any more because the North American Numbering Plan (NANP) does not allow any NPA codes (numbering plan area codes) starting with 1.

Figure 14-3   *Typical US Dialing Habits for PSTN and Emergency Calls*
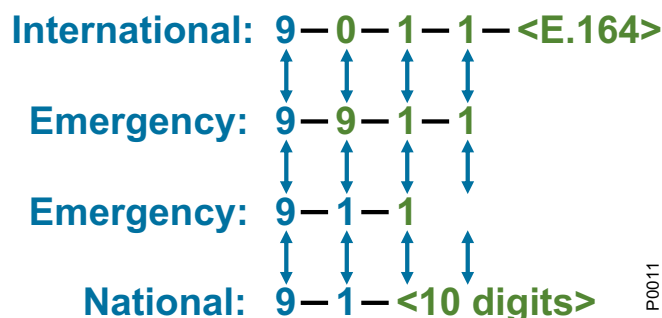
Given the PSTN dialing habit in Figure 14-3. four-digit intra-site dialing for extensions starting with 9 must be avoided because this could potentially create partial overlap. For example, extension 9113 would overlap with emergency calling, and after receiving 911 the call control would have to wait to

determine whether the caller is going to continue to dial 3 (extension 9113) or whether dialing actually was complete after 911. This would delay all emergency calls! Similarly, extensions such as 9140 would create overlaps with national PSTN calls, and calls to those extensions would be delayed.

To minimize overlaps, the first digit of a dialing habit can be defined as an access code uniquely identifying a class of destinations. The PSTN or trunk access code is a perfect example for this scheme. The most commonly used trunk access codes are 9 (US, UK, and others) and 0 (commonly used in most European countries).

As mentioned earlier, selecting non-overlapping dialing habits is key to avoiding bad user experience due to inter-digit time-outs. Typical overlaps seen in enterprise dial plans include:

- 10-digit dialing with abbreviated intra-site dialing (for example, four digits)

  NPA codes in the US can start with any digit other than 0 or 1, which means that the first few digits of 10-digit dialing would overlap with almost any abbreviated intra-site dialing.

- PSTN access code (such as 9 in the US) with abbreviated intra-site dialing

  A PSTN access code of 9 will overlap with all abbreviated intra-site dialing to extensions starting with 9.

- Abbreviated on-net inter-site dialing and abbreviated intra-site dialing

  The access code selected for the abbreviated on-net enterprise numbering plan might overlap with the range of intra-site dialing starting with the same digit. For example, using access code 8 for abbreviated on-net intra-site dialing prohibits the use of abbreviated intra-site dialing starting with 8.

Access to features such as call park numbers and voicemail also requires mapping into the set of dialing habits defined. Dialing these features should typically require only a short dialing sequence. To achieve this, either the feature access codes can be mapped into the abbreviated intra-site dialing or a dedicated feature access code needs to be defined.

Forced On-Net Routing

It is not uncommon for the dialing habits for on-net/inter-site and off-net destinations to use the same addressing structure. In this case the call control decides whether the addressed endpoint, user, or application is on-net or off-net based on the dialed address, and will treat the call as on-net or off-net, respectively.

Figure 14-4 shows an example of this forced on-net routing. All four calls in this example are dialed as 91 plus 10 digits. But while the calls to +1 408 555 2345 and +1 212 555 7000 are really routed as off-net calls through the PSTN gateway, the other two calls are routed as on-net calls because the call control identifies the ultimate destinations as on-net destinations. Forced on-net routing clearly shows that the dialing habit used to dial a specific destination does not necessarily determine how a call is routed. In this example, some calls are routed as on-net calls even though the used PSTN dialing habit seems to indicate that an off-net destination is called.

Figure 14-4   Forced On-Net Routing
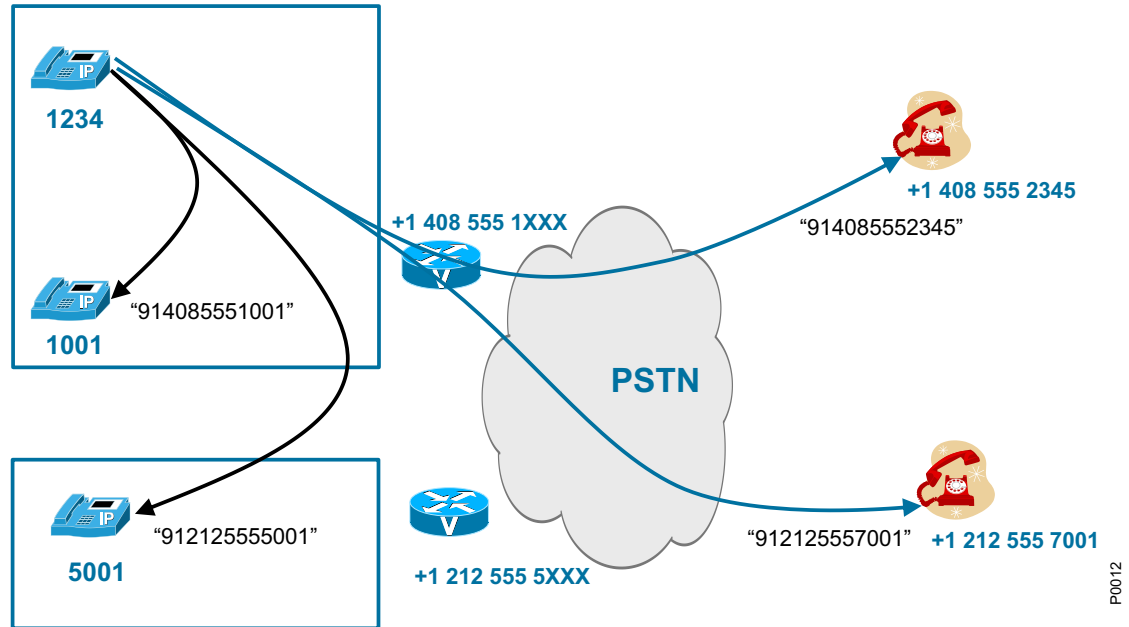
Forced on-net routing is especially important if dialing of +E.164 destinations from directories is implemented. In a normalized directory, all destinations are defined as +E.164 numbers, regardless of whether the person that the number is associated with is internal or external. In this case forced on-net routing is a mandatory requirement to avoid charges caused by internal calls routed through the PSTN.

Single Call Control Call Routing

If all endpoints are registered to a single call control, this call control has a full view of all known on-net destinations. When a user, endpoint, or application dials a destination using any of the defined dialing habits, the call control can easily determine whether the dialed destination is on-net or off-net. This might be based on the used dialing habit or on the normalized dialed address (see Forced On-Net Routing, page 14-9).

If the dialed destination is determined to be external, the call control then needs to select the correct external route to set up the call. If only one external (PSTN) connection exists, this is a trivial decision. If multiple external connections exist, the egress route selection can be based on any combination of the following factors:

- Call initiator
- Dialed destination
- Resource availability
- Resource prioritization

To be able to select an external connection based on the dialed destination, the dialed destination must be classified. As explained earlier, E.164 numbers have a hierarchical structure that implies some geographic association of numbers so that the egress connection selection could be based on a prefix-based hierarchical routing scheme that tries to select an egress point "closest" (in the sense of the geographic semantics of the E.164 number) to the destination. This behavior is called Tail End Hop Off (TEHO). When implementing Tail End Hop Off, local legal regulations have to be considered.

An interesting special case of TEHO exists if strange phone tariffs allow for cheaper national calls (for example, interstate) than local calls (in-state). In this case an egress point selection policy might be implemented that actually tries to avoid selecting an egress connection "too" close to the dialed destination. Decreasing phone charges make these kinds of routing schemes less and less useful.

In contrast to E.164 numbers, which have a clear hierarchical geographical structure with the most significant information on the left alphanumeric, SIP URIs allow addressing hierarchy in the host portion (RHS) of the URI. Depending on the domain name used as RHS, the addressing hierarchy of URIs does not necessarily allow for geographic mapping a URI to a location in the routing topology, especially if a flat URI scheme such as user@example.org is used. More interestingly, the most significant piece of a SIP URI is the right-most piece of the host portion (top level domain).

Multiple Call Control Call Routing

In larger enterprise networks, a number of call controls might be deployed. These independent call controls are interconnected using trunks. The possible topologies include hub and spoke, full mesh, and combinations of these. Any of these call controls will independently route calls offered by either endpoints, applications registered locally, or internal and external trunks.

In an environment like this, the on-net/off-net decision described in the previous section gets a little more complex. Before routing a call to an external connection, each call control needs to be sure that the dialed destination really is off-net. But by looking at only the locally registered addresses, the call control can actually get to only a reliable local/remote decision, and any destination classified as remote (not locally registered) can still be on-net but hosted on one of the other enterprise call controls deployed.

With numeric addressing and strict geographic assignment of endpoints to individual call controls, selecting the correct internal or external connection on any given call control comes down to implementing a routing scheme based on E.164 prefixes. This essentially is identical to the call routing process described for the single call control case, with the only difference being that some of the connections used for the prefix-based routing are not external connections (for example, to the PSTN) but are internal connections to other enterprise call control entities. To make sure that only calls to remote on-net destinations are routed to the remote call control, the call routing decision needs to be based on the specific address ranges local to the remote call control.

Figure 14-5 shows why the prefix-based routing between independent call controls must be very specific. In this example, to enable the left call control to decide wether 912125556001 needs to be treated as an on-net call, the left call control has to have very specific numeric prefix routes for all numeric addresses served by the right call control entity.

The maintenance of on-net prefix routes provisioned on each call control becomes more complex with an increasing number of call controls involved and sites and DID ranges to be considered. Dynamic learning of remote destinations helps to eliminate this complexity. Global Dial Plan Replication (GDPR) is one example of an architecture that allows call controls to automatically learn about destinations existing on remote call controls.

Figure 14-5   Prefix-Based Routing Between Call Controls
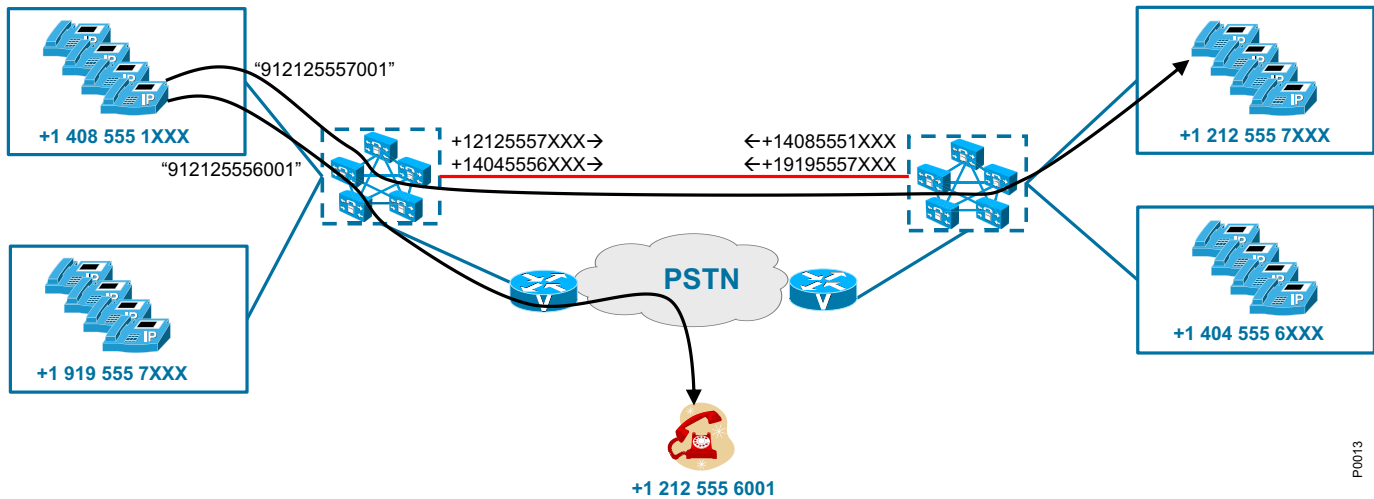
The equivalence of prefix-based routing of numeric addresses for alphanumeric URIs is to use a domain hierarchy and implement routing based on the host or domain portion of the URI. Figure 14-6 shows an example of hierarchical routing with alpha URIs. In this example all three independent call controls use a dedicated (sub) domain so that the on-net routing can easily be implemented based on this hierarchical domain structure.

Figure 14-6   Hierarchical Routing for Alpha URIs
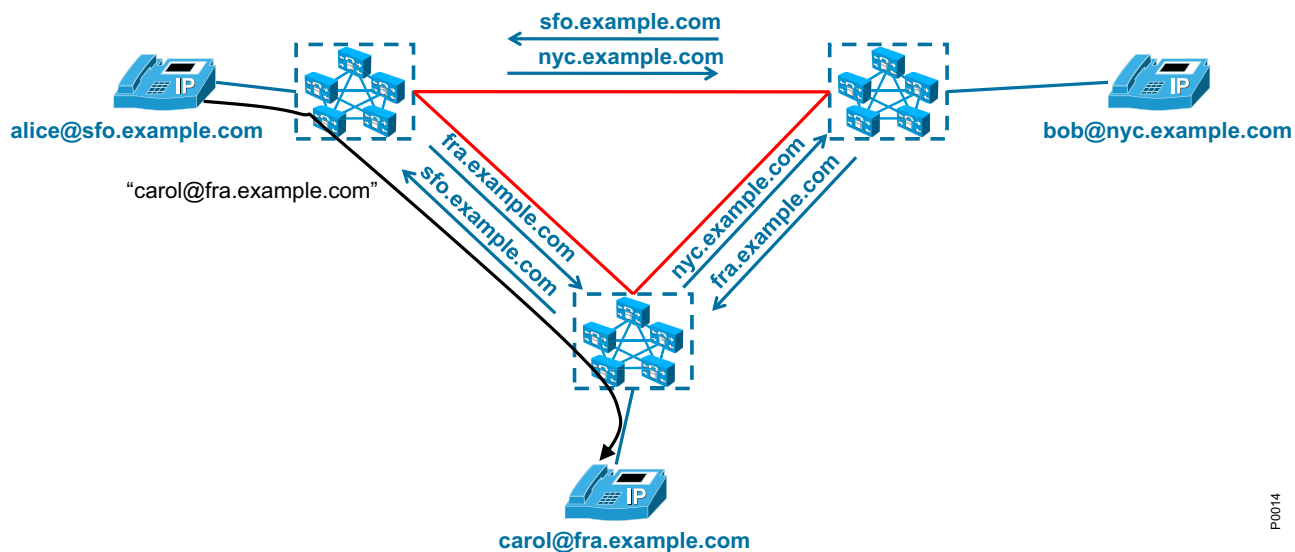
In cases where the URI addressing scheme is not hierarchical, each call control has to have knowledge of all URIs hosted on remote call controls. Global Dial Plan Replication (GDPR) offers a mechanism for call controls to exchange information about URIs hosted on each call control to enable deterministic routing even with a flat URI naming scheme.

Dial Plan Elements

This section describes the dial plan elements available in these solution components:

Cisco Unified Communications Manager

This section provides design and configuration guidelines for the following dial plan elements within Cisco Unified Communications Manager (Unified CM):

User Interface on IP Phones

Note   Different types of IP telephones accept keypad input and present visual information in different ways. For purposes of this chapter only, we define the following phone types:

- **Type-A phones** — Include the Cisco Unified IP Phone 7905, 7912, 7940, and 7960.
- **Type-B phones** — Include the Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, 6961, 7906, 7911, 7921, 7925, 7931, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975, 8961, 9951, 9971, and newer phones.

Calling Party Transformations on IP Phones

Calling Party Transformation Patterns allow the system to adapt the calling party numbers to different formats. The most typical use is to adapt from globalized to localized calling party numbers and vice versa.

The transformation pattern consists of a numerical representation of the calling party number to be matched. The syntax used is the same as that of other patterns such as route patterns, called party transformation patterns, directory numbers, and so forth.

The transformation operators available on a transformation pattern include discard digit instructions (for example, pre-dot), a calling party transformation mask, prefix digits, and an option to apply the calling party's external phone number mask. In addition, the calling party presentation indicator can be set (either Default, Allowed, or Restricted).

Partitions and calling search spaces control which calling party transformation patterns are applied to which phones. Phones can use either the device pool's calling party transformation calling search space (CSS) or the device's own calling party transformation CSS, in reverse order of precedence.

On IP phones, calling party transformations can be configured for calls originating from the phone and for calls terminated on the phone:

- For calls originating from phones where the configured directory numbers are not in a globalized (+E.164) form, the inbound call's calling party transformation CSS can be used to define the appropriate globalization. This CSS can be found on the phone configuration page in the Number Presentation Transformation section or in the Phone Settings section on the device pool configuration page under **Caller ID For Calls From This Phone**.

- For calls terminated on the phones, the outbound calls' calling party transformation CSS can be used to define the localization scheme to be applied to calling party numbers. This CSS can be found on the phone configuration page in the Number Presentation Transformation section under **Remote Number**.

For phones, outbound or remote number calling party transformations affect the number displayed while the phone is ringing.

For Type-B phones, the corresponding entry in the missed and received calls directories holds both the transformed number and also the original pre-transformation number. The transformed number is displayed in the directories´ list, but the number used for callback is the pre-transformation number.

The outbound call's calling party transformation CSS (also referred to as localization or remote number calling party transformation CSS) can also be used to localize remote connected party information. To enable this, the advanced service parameter **Apply Transformations On Remote Number** must be enabled.

Being able to provide localized connected party information to phones enables consistent remote party information display on IP phones even if mid-call features are invoked.

Support for + Dialing on the Phones

On Type-A phones, it is not possible to dial a + sign using the keypad. On Type-B phones it is possible to dial a + sign by pressing and holding either the 0 key (Cisco Unified IP Phones 7921 and 7925) or the * key (all other phone models). On Cisco Unified Personal Communicator endpoints, the + sign may be typed in by the user using the computer's keyboard or entered as part of the input string when using a click-to-dial function of the endpoint.

On Type-A phones, there is no support to dial a +. The + sign can be displayed as part of the calling party information for incoming calls and in directories, but the phone will strip the + sign when the entry is dialed from the missed calls directory. To avoid misdialed calls, Type-A phones put the transformed number in the missed calls directory, and the callback also uses the transformed number. The transformed number has to be in the form of a dialing habit supported by the dial plan to avoid misdialed calls from directories.

On Type-B phones and on Cisco Jabber, incoming calls can present a calling party number including + as part of the number. When a call is offered to a phone, the number shown on the ringing phone is processed by any configured calling party number transformation patterns. The missed and received calls directories hold both the original pre-transformation number and the transformed number. The number displayed in the list will be the transformed number, and the pre-transformation number will be visible only when looking at the details of an entry. The number dialed from the directory is the original pre-transformation number, allowing the one-touch dialing of previously received calls featuring the + sign as part of the calling number as long as the dial plan supports + dialing.

Example 14-1   Calling Party Number with + Dialing

A Type-B phone in New York receives a call from +1 408 526 4000. Calling party transformation patterns are placed in the calling party transformation CSS in the phone's device pool. One of the patterns is configured as: \+1.!, strip pre-dot.

As the call rings in, the called phone displays an incoming calling party number of 4085264000. After the call is answered and released, the received-calls directory displays the last call as 408 526 4000, but the number called when the user initiated the callback from the directory entry is +1 408 526 4000.

User Input on SCCP Phones

IP phones using SCCP report every single user input event to Unified CM immediately. For instance, as soon as the user goes off-hook, a signaling message is sent from the phone to the Unified CM server with which it is registered. The phone can be considered to be a terminal, where all decisions resulting from the user input are made by Unified CM according to the configured dial plan.

As other user events are detected by the phone, they are relayed to Unified CM individually. A user who goes off-hook and then dials 1000 would trigger five individual signaling events from the phone to Unified CM. All the resulting feedback provided to the user, such as screen messages, playing dial tone, secondary dial tone, ring back, reorder, and so forth, are commands issued by Unified CM to the phone in response to the dial plan configuration. (See Figure 14-7.)

Figure 14-7   User Input and Feedback for SCCP Phones
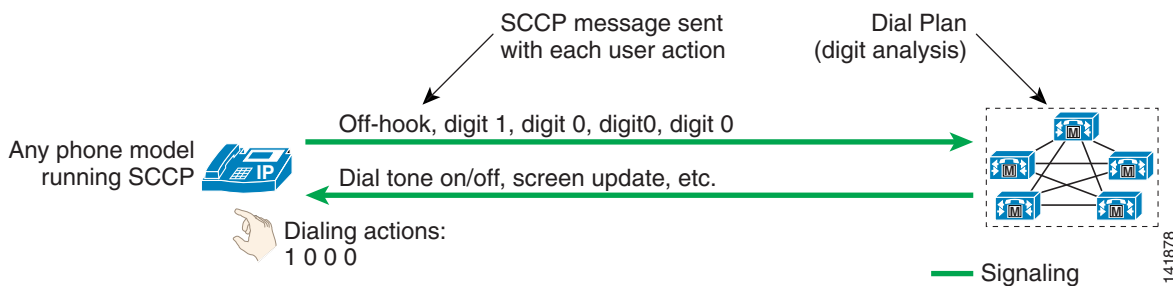
It is neither required nor possible to configure dial plan information on IP phones running SCCP. All dial plan functionality is contained in the Unified CM cluster, including the recognition of dialing patterns as user input is collected.

If the user dials a pattern that is denied by Unified CM, reorder tone is played to the user as soon as that pattern becomes the best match in Unified CM's digit analysis. For instance, if all calls to the pay-per-minute Numbering Plan Area (or area code) 976 are denied, reorder tone would be sent to the user's phone as soon as the user dials 91976.

User Input on Type-A SIP Phones

Type-A phones differ somewhat from Type-B phones in their behavior, and Type-A phones do not offer support for Key Press Markup Language (KPML) as do Type-B phones. (See User Input on Type-B SIP Phones, page 14-17.)

Type-A IP phones using SIP offer two distinct modes of operation:

- No SIP Dial Rules Configured on the Phone, page 14-16
- SIP Dial Rules Configured on the Phone, page 14-16

No SIP Dial Rules Configured on the Phone

Figure 14-8 illustrates the behavior of a SIP Type-A phone with no dial plan rules configured on the phone. In this mode of operation, the phone accumulates all user input events until the user presses either the # key or the Dial softkey. This function is similar to the "send" button used on many mobile phones. For example, a user making a call to extension 1000 would have to press 1, 0, 0, and 0 followed by the Dial softkey or the # key. The phone would then send a SIP INVITE message to Unified CM to indicate that a call to extension 1000 is requested. As the call reaches Unified CM, it is subjected to all the class-of-service and call routing logic implemented in Unified CM's dial plan.

Figure 14-8   *User Input and Feedback for Type-A SIP Phones with No Dial Rules Configured*
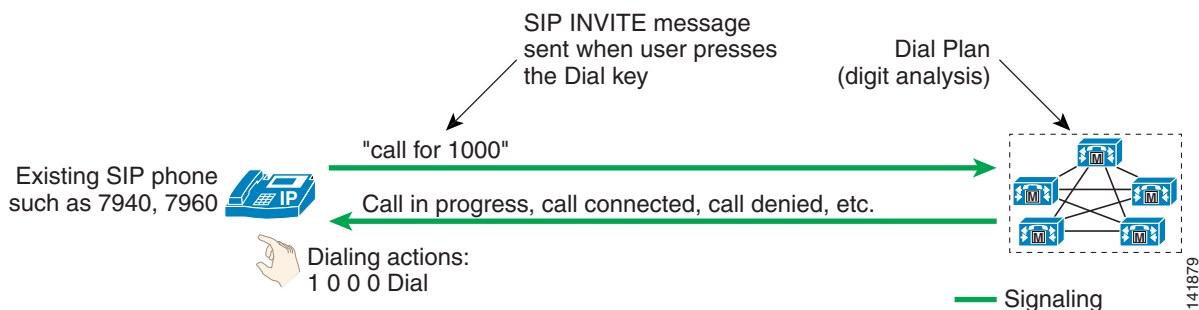
If the user dials digits but then does not press the Dial softkey or the # key, the phone will wait for inter-digit timeout (15 seconds by default) before sending a SIP INVITE message to Unified CM. For the example in Figure 14-8, dialing 1, 0, 0, 0 and waiting for inter-digit timeout would result in the phone placing a call to extension 1000 after 15 seconds.

Note   If the user presses the Redial softkey, the action is immediate; the user does not have to press the Dial key or wait for inter-digit timeout.

If the user dials a pattern that is denied by Unified CM, the user must enter the entire pattern and press the Dial key, and the INVITE message must be sent to Unified CM, before any indication that the call is rejected (reorder tone) is sent to the caller. For instance, if all calls to NPA 976 are denied, the user would have to dial 919765551234 and press Dial before the reorder tone would be played.

SIP Dial Rules Configured on the Phone

SIP dial rules enable the phone to recognize patterns dialed by users. Once the recognition has occurred, the sending of the SIP INVITE message to Unified CM is automated and does not require the user to press the Dial key or wait for the inter-digit timeout. (For more details, see SIP Dial Rules, page 14-19.)

For example, if a branch location of the enterprise requires that calls between phones within the same branch be dialed as four-digit extensions, the phone could be configured to recognize the four-digit patterns so that the user is not required to press the Dial key or wait for the inter-digit timeout. (See Figure 14-9.)

Figure 14-9   *User Input and Feedback for Type-A SIP Phones with Dial Rules Configured*
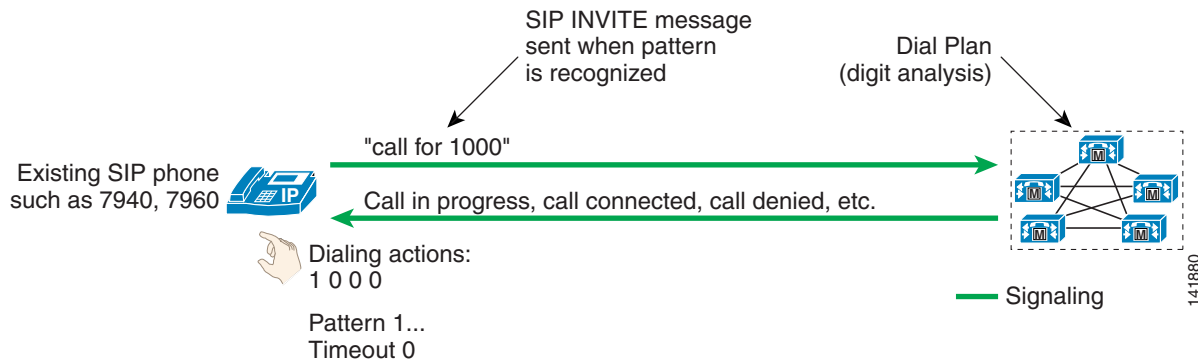
In Figure 14-9, the phone is configured to recognize all four-digit patterns beginning with 1 and has an associated timeout value of 0. All user input actions matching the pattern will trigger the sending of the SIP INVITE message to Unified CM immediately, without requiring the user to press the Dial key.

Type-A phones using SIP dial rules offer a way to dial patterns not explicitly configured on the phone. If a dialed pattern does not match a SIP dial rule, the user can press the Dial key or wait for inter-digit timeout.

If a particular pattern is recognized by the phone but blocked by Unified CM, the user must dial the entire dial string before receiving an indication that the call is rejected by the system. For instance, if a SIP dial rule is configured on the phone to recognize calls dialed in the form 919765551234 but such calls are blocked by the Unified CM dial plan, the user will receive reorder tone at the end of dialing (after pressing the final 4 key).

User Input on Type-B SIP Phones

Type-B phones differ somewhat from Type-A phones in their behavior, and Type-B phones offer support for Key Press Markup Language (KPML) but Type-A phones do not. (See User Input on Type-A SIP Phones, page 14-15.)

Type-B IP phones running SIP offer two distinct modes of operation:

- No SIP Dial Rules Configured on the Phone, page 14-17
- SIP Dial Rules Configured on the Phone, page 14-18

No SIP Dial Rules Configured on the Phone

Type-B IP telephones offer functionality based on the Key Press Markup Language (KPML) to report user key presses. Each one of the user input events will generate its own KPML-based message to Unified CM. From the standpoint of relaying each user action immediately to Unified CM, this mode of operation is very similar to that of phones running SCCP. (See Figure 14-10.)

*Figure 14-10*   *User Input and Feedback for Type-B SIP Phones with No Dial Rules Configured*
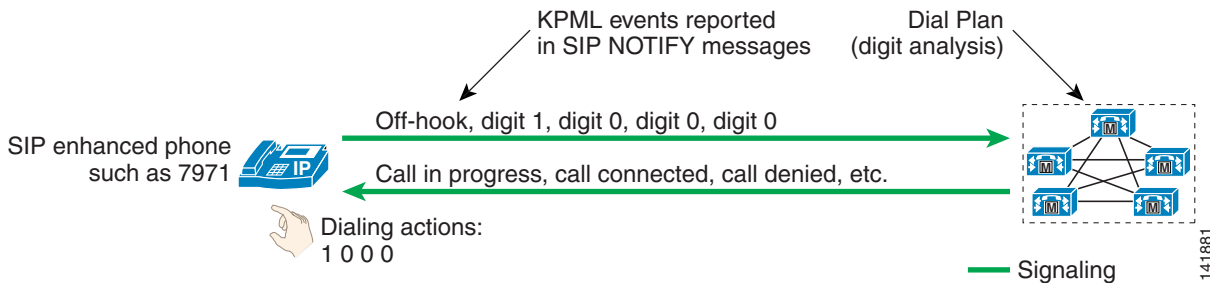
Every user key press triggers a SIP NOTIFY message to Unified CM to report a KPML event corresponding to the key pressed by the user. This messaging enables Unified CM's digit analysis to recognize partial patterns as they are composed by the user and to provide the appropriate feedback, such as immediate reorder tone if an invalid number is being dialed.

In contrast to Type-A IP phones running SIP without dial rules, Type-B SIP phones have no Dial key to indicate the end of user input. In Figure 14-10, a user dialing 1000 would be provided call progress indication (either ringback tone or reorder tone) after dialing the last 0 and without having to press the Dial key. This behavior is consistent with the user interface on phones running the SCCP protocol.

SIP Dial Rules Configured on the Phone

Type-B IP phones can be configured with SIP dial rules so that dialed pattern recognition is accomplished by the phone. (See Figure 14-11.)

Figure 14-11   *User Input and Feedback for Type-B SIP Phones with Dial Rules Configured*
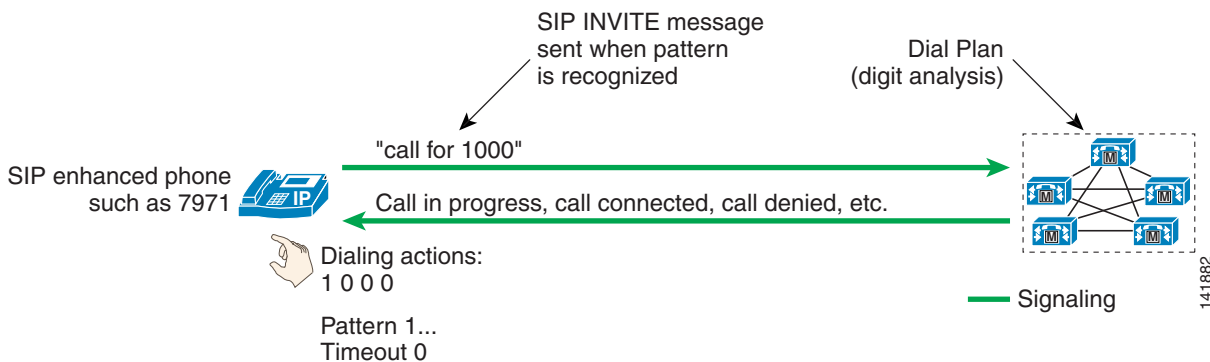
In Figure 14-11, the phone is configured to recognize all four-digit patterns beginning with 1, and it has an associated timeout value of 0. All user input actions matching these criteria will trigger the sending of a SIP INVITE message to Unified CM.

Note   As soon as SIP dial rules are implemented on Type-B IP phones, KPML-based dialing is disabled. If a user dials a string of digits that do not match a SIP dial rule, none of the individual digit events will be relayed to Unified CM. Instead, the entire dialed string will be sent en-bloc to Unified CM once the dialing is complete (that is, once inter-digit timeout has occurred).

Type-B phones using SIP dial rules offer only one way to dial patterns not explicitly configured on the phone. If a dialed pattern does not match a SIP dial rule, the user has to wait for inter-digit timeout before the SIP NOTIFY message is sent to Unified CM. Unlike Type-A IP phones, Type-B IP phones do not have a Dial key to indicate the end of dialing, except when on-hook dialing is used. In the latter case, the user can press the "dial" key at any time to trigger the sending of all dialed digits to Unified CM.

Note   When a Type-B phone registers with the SRST router, the configured SIP dial rules are disabled.

If a particular pattern is recognized by the phone but blocked by Unified CM, the user must dial the entire dial string before receiving an indication that the call is rejected by the system. For instance, if a SIP dial rule is configured on the phone to recognize calls dialed in the form 919765551234 but such calls are blocked by the Unified CM dial plan, the user will receive reorder tone at the end of dialing (after pressing the 4 key).

SIP Dial Rules

Cisco Unified CM offers SIP dial rule functionality to allow phones to perform pattern recognition as user input is collected. For example, a phone can be configured to recognize the well established pattern 911 and to send a message to Unified CM to initiate an emergency call immediately, while at the same time allowing the user to enter patterns of variable length for international numbers.

It is important to note that pattern recognition configuration on the phone through the use of SIP dial rules does not supersede the Class of Service and Route Plan configurations of Unified CM. A phone might very well be configured to recognize long-distance patterns while Unified CM is configured to block such calls because the phone is assigned a class of service allowing only local calls.

There are two types of SIP dial rules, based on the phone model on which they will be deployed:

- 7905_7912 (Used for Cisco Unified IP Phones 7905 and 7912)
- 7940_7960_OTHER (Used for all other IP phone models))

There are four basic Dial Parameters that can be used as part of a dial rule:

- Pattern

    This parameter is the actual numerical representation of the pattern. It can contain digits, wildcards, or instructions to play secondary dial tone. The following table provides a list of values and their effect for the two types of dial rules.

Pattern	Dial Rule Type	
	7905_7912	**7940_7960_OTHER**
Digits 0 through 9	Corresponding digit	Corresponding digit
.	Matches any digit (0 through 9)	Matches any character (0 though 9, *, #)
-	Indication that more digits can be entered. Must be at the end of an individual rule.	n/a

	Dial Rule Type	
Pattern	7905_7912	7940_7960_OTHER
#	Input termination key. Place the > character in the dial rule to indicate the character position after which the # key will be recognized as input termination. For instance, in 9>#..., the # character would be recognized any time after 9 has been pressed.	n/a
t*n*	Indicates a timeout value of *n* seconds. For example, 1…t3 would match 1000 and trigger the sending of an invite to Unified CM after 3 seconds.	n/a
r*n*	Repeats the last character *n* times. For example, 1.r3 is equivalent to 1….	n/a
S	When a pattern contains the modifier S, all other dial rules after this pattern are ignored. S effectively causes rule matching to cease.	n/a
*	Input termination key. Place the > character in the dial rule to indicate the character position after which the * key will be recognized as input termination.	Matches one or more characters. For instance, pattern 1* would match 10, 112, 123456, and so forth.
,	n/a	Cause the phone to play secondary dial tone. For instance, 8,…. would cause the user to hear secondary dial tone after 8 is pressed.

- IButton

  This parameter specifies the button to which the dial pattern applies. If the user is initiating a call on line button 1, only the dial patterns specified for Button 1 apply. If this optional parameter is not configured, the dial pattern applies to all lines on the phone. This parameter applies only to the Cisco SIP IP Phones 7940, 7941, 7942, 7945, 7960, 7961, 7962, 7965, 7970, 7971, and 7975. The button number corresponds to the order of the buttons on the side of the screen, from top to bottom, with 1 being on top button.

- Timeout

  This parameter specifies the time, in seconds, before the system times out and dials the number as entered by the user. To have the number dialed immediately, specify 0. This parameter is available only for 7940_7960_OTHER dial rules. If this parameter is omitted, the phone's default inter-digit timeout value is used (default of 10 seconds).

- User

  This parameter represents the tag that automatically gets added to the dialed number. Valid values include **IP** (when SIP Call Agents other than Unified CM are deployed) and **Phone**. This parameter is available only for 7940_7960_OTHER dial rules. This parameter is optional, and it should be

omitted in deployments where Unified CM is the only call agent. Keep in mind that a user=phone tag in a SIP request sent to Unified CM will force Unified CM to treat the SIP URI as a numeric URI. A SIP URI in the form of alice@cisco.com;user=phone will never be routed successfully because the user=phone tag forces numeric treatment and alice will not match any numeric pattern provisioned in Unified CM.

Note   The Cisco Unified IP Phone 7905 and 7912 choose patterns in the order in which they have been created in the SIP dial rules, whereas all the other phone models choose the pattern offering the longest match. The following table shows which pattern would be chosen if a user dialed 95551212.

| SIP Dial Rules	7905_7912	7940_7960_OTHER
.... 9.......	Chooses first matching pattern:	Chooses longest matching pattern: 9.......

Call Routing in Unified CM

All numeric dialing destinations and directory URIs configured in Unified CM are added to its internal call routing table as patterns. These destinations include IP phone lines, voicemail ports, route patterns, translation patterns, and CTI route points. Unified CM uses two distinct routing tables for numeric dialing destinations and directory URIs.

When a directory URI is dialed, Unified CM uses full-match logic to find a match among the configured directory URIs in the directory URI routing table. The **URI Lookup Policy** enterprise service parameter setting determines whether the full-match logic for the user portion (left-hand side) of the URI uses case-sensitive or case-insensitive matching. Case-sensitive matching is the default. When a number is dialed, Unified CM uses best-match logic to select which pattern to match from among all the patterns in its numeric call routing table. In practice, when multiple potentially matching numeric patterns are present, the destination pattern is chosen based on the following criteria:

- It matches the dialed string, and

- Among all the potentially matching patterns, it matches the fewest strings other than the dialed string.

For example, consider the case shown in Figure 14-12, where the call routing table includes the patterns 1XXX, 12XX, and 1234.

Figure 14-12   Unified CM Call Routing Logic Example
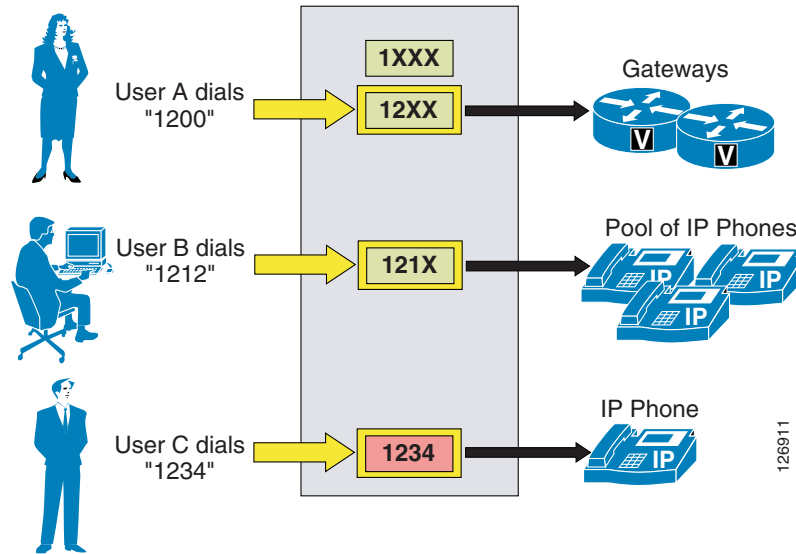
When user A dials the string 1200, Unified CM compares it with the patterns in its call routing table. In this case, there are two potentially matching patterns, 1XXX and 12XX. Both of them match the dialed string, but 1XXX matches a total of 1000 strings (from 1000 to 1999) while 12XX matches only 100 strings (from 1200 to 1299). Therefore, 12XX is selected as the destination of this call.

When user B dials the string 1212, there are three potentially matching patterns, 1XXX, 12XX and 121X. As mentioned above, 1XXX matches 1000 strings and 12XX matches 100 strings. However, 121X matches only 10 strings; therefore it is selected as the destination of the call.

When user C dials the string 1234, there are three potentially matching patterns, 1XXX, 12XX, and 1234. As mentioned above, 1XXX matches 1000 strings and 12XX matches 100 strings. However, 1234 matches only a single string (the dialed string); therefore it is selected as the destination of this call.

When determining the number of matched strings for a variable-length pattern, Unified CM takes into account only the number of matched strings that are equal in length to the number of digits dialed. Assuming a user dials 1311 and we have patterns 1XXX, 1[2-3]XX, and 13!, the following table shows the number of matched strings of these potentially matching patterns.

Pattern	Number of Matched Strings	Possible Strings Matched
1XXX	1000	1000 to 1999
1[2-3]XX	200	1200 to 1299; 1300 to 1399
13!	100	1300 to 1399; only four-digit strings counted, based on the number of digits dialed

In this example the variable-length pattern 13! is selected as the best match.

> **Note** Whenever a directory number (DN) is configured in Cisco Unified CM, it is placed in the call routing table, regardless of whether the respective device (for example, an IP phone) is registered or not. An implication of this behavior is that it is not possible to rely on secondary, identical patterns to provide failover capabilities to applications when the device (and hence the primary pattern) is unregistered. Because the primary pattern is permanently in the call routing table, the secondary pattern will never be matched.

Support for + Sign in Patterns

The + sign can be used in all patterns within Unified CM, including route patterns, translations patterns, and directory numbers. To use + in its literal sense, precede it with the escape character \ to differentiate it from the regular expression operator +, which means one or more instances of the preceding character. For example:

- \+14085264000 means +14085264000
- 2+ means 2, or 22, or 222, and so forth

This enables seamless implementation of +E.164 dial plans in Unified CM.

Directory URIs

All endpoints registered with Unified CM are provisioned with one or more numeric (possibly including a leading +) directory numbers. Up to five directory URIs can be associated with each directory number. This association can be created by explicitly associating directory URIs to directory numbers. If a directory URI is configured for an end user, this directory URI will be automatically associated with the primary extension of that end user as soon as the primary extension gets defined for that end user. All automatically associated directory URIs are created in the partition **Directory URI**, while manually configured directory URIs can be in any partition. Manually configured directory URIs can reside in the same partition as the directory number they are associated with, but do not have to. Directory URIs have to be unique per partition.

Exactly one of the directory URIs associated with a directory number has to be marked as the primary directory URI of that directory number. If a user directory URI gets associated automatically with the primary extension of that user, then this directory URI will also automatically be the primary directory URI for that directory number. If no directory URI is associated automatically, then one of the configured directory URIs has to be selected as the primary directory URI. The purpose of the primary directory URI is that this directory URI will be used as the calling identity directory URI for calls originating from the respective directory number.

The possible association of directory URIs with any directory number allows callers to reach any directory number by dialing the associated directory URI. The called directory number can be on any device registered to Unified CM using any protocol. Similarly, Unified CM can deliver a directory URI caller ID for any call from any directory number as long as a directory URI is associated with the calling directory number.

To enable intercluster routing of directory URIs, Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS). Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, the SIP route string. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI.

For details of how calls to directory URIs learned from remote clusters are routed, see the section on Routing of SIP Requests in Unified CM, page 14-47.

Translation Patterns

Translation patterns are one of the most powerful tools in Unified CM to manipulate digits for any type of call. They follow the same general rules and use the same wildcards as route patterns. As with route patterns, you assign a translation pattern to a partition. However, when the dialed digits match the translation pattern, Unified CM does not route the call to an outside entity such as a gateway; instead, it performs the translation first and then routes the call again, this time using the calling search space configured within the translation pattern.

Translation patterns can be used for a variety of applications, as shown by the example in Figure 14-13.

Figure 14-13   Application Example for Translation Patterns
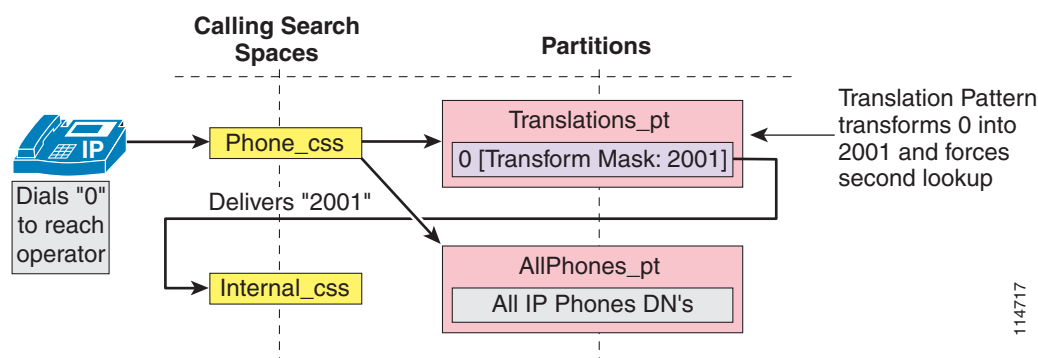
In this example, the administrator wishes to provide users with an operator service that is reached by dialing 0, while also maintaining a fixed-length internal numbering plan. The IP phones are configured with the Phone_css calling search space, which contains the Translations_pt partition (among others). A translation pattern 0 is defined in this partition, and the configured Called Party Transform Mask instructs Unified CM to replace the dialed string (0) with the new string 2001, which corresponds to the DN of the operator phone. A second lookup (of 2001 this time) is forced through the call routing engine, using the Internal_css calling search space, and the call can now be extended to the real operator DN of 2001, which resides in the AllPhones_pt partition.

Note   When a dialed number is manipulated using a translation pattern, the translated number is recorded in the call detail record (CDR). However, when the digit manipulation occurs within a route list, the CDR will show the originally dialed number, not the translated one. The Placed Calls directory on the IP phone always shows the string as it was dialed by the user.

The general use case for translation patterns is to create a mapping from a certain dial string format to a string to be matched by other dial plan elements. This mapping implements overlay dialing habits on top of the "native" dialing habits created by other patterns such as route patterns and directory numbers. Typically for the secondary lookup, translation patterns that implement a dialing normalization should simply use the calling search space that activates the translation pattern. This behavior, referred to as CSS Inheritance, is selected by the option **Use Originator's Calling Search Space** on the translation pattern. Enabling this option allows reuse of dialing normalization translation patterns for different classes of service, each defined by a different calling search space.

External Routes in Unified CM

Unified CM automatically "knows" how to route calls to internal destinations within the same cluster. For external destinations such as PSTN gateways, SIP trunks, or other Unified CM clusters, you have to use the external route construct (described in the following sections) to configure explicit routing. This construct is based upon a three-tiered architecture that allows for multiple layers of call routing as well as digit manipulation. Unified CM searches for a configured route pattern that matches the external dialed string and uses it to select a corresponding route list, which is a prioritized list of the available paths for the call. These paths are known as route groups and are very similar to trunk groups in traditional PBX terminology. Figure 14-14 depicts the three-tiered architecture of the Unified CM external route construct.

Figure 14-14   External Route Pattern Architecture
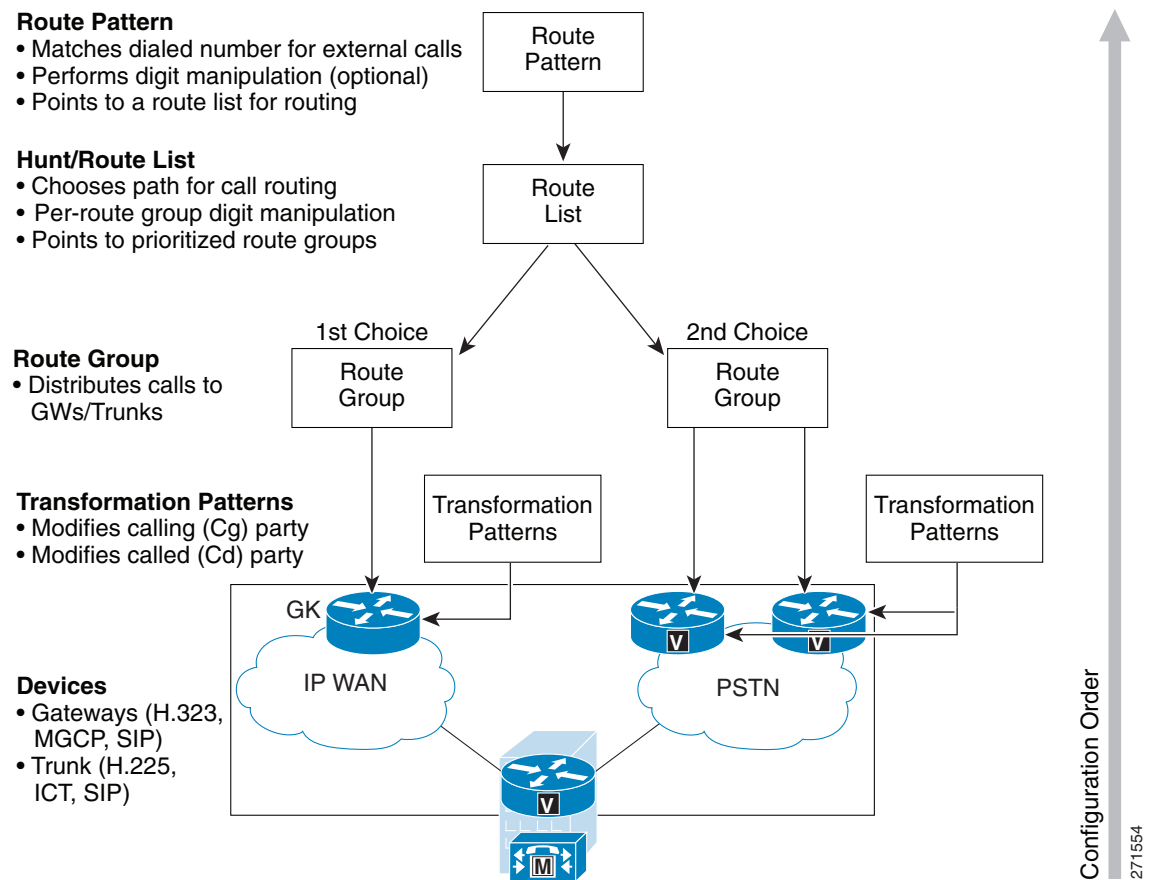
The following sections describe the individual elements of the external route construct in Unified CM:

- Route Patterns, page 14-26
- Route Lists, page 14-29
- Route Groups, page 14-29
- Route Group Devices, page 14-29

Route Patterns

Route patterns are strings of digits and wildcards, such as 9.[2-9]XXXXXX, configured in Unified CM to route calls to external entities. The route pattern can point directly to a gateway for routing calls or point to a route list, which in turn points to a route group and finally to a gateway.

Cisco strongly recommends that you use the complete route pattern, route list, and route group construct because it provides the greatest flexibility for call routing, digit manipulation, route redundancy, and future dial plan growth.

The @ Wildcard

- The @ wildcard is a special macro function that expands into a series of patterns representing the entire national numbering plan for a certain country. For example, configuring a single unfiltered route pattern such as 9.@ with the North American Numbering Plan really adds 166 individual route patterns to the Unified CM internal dial plan database.

- It is possible to configure Unified CM to accept other national numbering plans. Once this is done, the @ wildcard can be used for different numbering plans even within the same Unified CM cluster, depending on the value selected in the Numbering Plan field on the Route Pattern configuration page. For more information, please refer to the *Cisco Unified Communications Manager Dial Plan Deployment Guide*, available at

    http://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html

- The @ wildcard can be practical in several small and medium deployments, but it can become harder to manage and troubleshoot in large deployments because adopting the @ wildcard forces the administrator to use route filters to block certain patterns (see Route Filters, page 14-26).

Route Filters

- Use route filters only with the @ route pattern to reduce the number of route patterns created by the @ wildcard. A route filter applied to a pattern not containing the @ wildcard has no effect on the resulting dial plan.

- The logical expression you enter with the route filter can be up to 1024 characters, excluding the NOT-SELECTED fields.

- As you increase the number of logical clauses in a route filter, the refresh time of the configuration page also increases and can become unacceptably long.

- For large-scale deployments, use explicit route patterns rather than the @ wildcard and route filters. This practice also facilitates management and troubleshooting because all patterns configured in Unified CM are easily visible from the Route Pattern configuration page.

International and Variable-Length Route Patterns

- International destinations are usually configured using the ! wildcard, which represents any quantity of digits. For example, in North America the route pattern 9.011! is typically configured for international calls. In most European countries, the same result is accomplished with the 0.00! route pattern.

- The ! wildcard is also used for deployments in countries where the dialed numbers can be of varying lengths. In such cases, Unified CM does not know when the dialing is complete and will wait for 15 seconds (by default) before sending the call. You can reduce this delay in any of the following ways:

    – Reduce the T302 timer (Service Parameter TimerT302_msec) to indicate end of dialing, but do not set it lower than 4 seconds to prevent premature transmission of the call before the user is finished dialing.

– Configure a second route pattern followed by the # wildcard (for example, 9.011!# for North America or 0.00!# for Europe), and instruct the users to dial # to indicate end of dialing. This action is analogous to hitting the "send" button on a cell phone.

Overlap Sending and Overlap Receiving

In countries whose national numbering plan is not easily defined with static route patterns, you can configure Unified CM for overlap sending and overlap receiving.

Overlap sending means that Unified CM keeps collecting digits as they are dialed by the end users, and passes them on to the PSTN as they are dialed. To enable overlap sending, check the Allow Overlap Sending box on the Route Pattern Configuration page. The route pattern needs to include only the PSTN access code (for example, "9." in North America or "0." in many European countries).

Overlap receiving means that Unified CM receives the dialed digits one-by-one from a PRI PSTN gateway, and it then waits for completion of the dialed string before attempting to route the call to an internal destination. To enable overlap receiving, set the OverlapReceivingFlagForPRI service parameter to True.

Digit Manipulation in Route Patterns

- Digit manipulations configured on a route pattern affect the calling and called party number, no matter what route group the call eventually takes. Digit manipulations configured in the route list's view of its member route groups have a route-specific effect: only the transformations configured on the route group used to place the call will be performed.

- Digit manipulation in the route list's view of its member route group overrides any digit manipulation done in the route pattern.

- Calling and called party transformations configured in the route pattern and/or route list are ignored if transformation patterns are configured for the device selected to route the call. These device-level transformations are always applied to the original calling and called party numbers before they reach the route pattern.

- If you configure digit manipulation in the route pattern, the Call Detail Record (CDR) records the dialed number after the digit manipulation has occurred. If you configure digit manipulation only in the route group or on the device level, the CDR records the actual dialed number prior to the digit manipulation.

- Similarly, if you configure digit manipulation in the route pattern, the IP phone display of the calling party will show the manipulated number. If you configure digit manipulation only in the route group, the manipulations will be transparent to the end user.

Calling Line ID

- The calling line ID presentation can be enabled or disabled on the gateway and also can be manipulated in the route pattern, based on site requirements.

- If you select the option Use Calling Party's External Phone Number Mask, then the external call uses the calling line ID specified for the IP phone placing the call. If you do not select this option, then the mask placed in the Calling Party Transform Mask field is used to generate the calling party ID.

Call Classification

- Calls using this route pattern can be classified as on-net or off-net calls. This route pattern can be used to prevent toll fraud by prohibiting off-net to off-net call transfers or by tearing down a conference bridge when no on-net parties are present. (Both of these features are controlled by Service Parameters within Unified CM Administration.)

- When the "Allow device override" box is enabled, the calls are classified based on the call classification settings on the associated gateway or trunk.

Forced Authorization Codes (FAC)

- The Forced Authorization Codes (FAC) checkbox is used to restrict the outgoing calls when using a particular route pattern. If you enable FAC through route patterns, users must enter an authorization code to reach the intended recipient of the call.

- When a user dials a number that is routed through a FAC-enabled route pattern, the system plays a tone that prompts for the authorization code. To complete the call, the user authorization code must meet or exceed the level of authorization that is specified to route the dialed number.

- Only the authorization name appears in the call detail records (CDR); the authorization code does not appear in the CDR.

- The FAC feature is not available if the "Allow overlap sending" checkbox is enabled.

Client Matter Codes (CMC)

- The Client Matter Code (CMC) checkbox is used to track calls to certain numbers when using a particular route pattern. (For example, a company can use it to track calls to certain clients.)

- If you enable CMC for a route pattern, users must enter a code to reach the intended destination.

- When a user dials a number that is routed through a CMC-enabled route pattern, the system plays a tone that prompts for the code. The user must enter the correct code in order to complete the call.

- Client Matter Codes appear in the call detail records so that they can be used by the CDR analysis and reporting tool to generate reports for client billing and accounting.

- The CMC feature is not available if the "Allow overlap sending" checkbox is enabled.

- If both CMC and FAC are enabled, the user dials a number, enters the FAC when prompted to do so, and then enters the CMC at the next prompt.

SIP Route Pattern

SIP route patterns are configured in Unified CM to route or block calls to external entities based on the host portion (right-hand side) of SIP URIs. A SIP route pattern can point directly to a SIP trunk or point to a route list that then refers to one or more route groups and finally to SIP trunks. The use of the full SIP route pattern, route list, route group construct is highly recommended because it offers more flexibility.

SIP route patterns matching on the host piece of a SIP URI can match on a domain name or an IP address, both of which are possible as the right-hand side of a SIP URI. Wildcards can be used in domain name SIP route patterns to match on multiple domains (for example, *.cisco.com and ccm[1-4].uc.cisco.com). In IP address SIP route patterns, a subnet notation can be used (for example, 192.168.10.0/24).

Route Lists

A route list is a prioritized list of eligible paths (route groups) for an outbound call. A typical use of a route list is to specify two paths for a remote destination, where the first-choice path is across the IP WAN and the second-choice path is through a PSTN gateway.

Route lists have the following characteristics:

- Multiple route patterns may point to the same route list.

- A route list is a prioritized list of route groups that function as alternate paths to a given destination. For example, you can use a route list to provide least-cost routing, where the primary route group in the list offers a lower cost per call and the secondary route group is used only if the primary is unavailable due to an "all trunks busy" condition or insufficient IP WAN resources.

- Each route group in the route list can have its own digit manipulation. For example, if the route pattern is 9.@ and a user dials 9 1 408 555 4000, the IP WAN route group can strip off the 9 1 while the PSTN route group may strip off just the 9.

- Multiple route lists can contain the same route group. The digit manipulation for the route group is associated with the specific route list that points to the route group.

- If you are performing several digit manipulations in a route pattern or a route group, the order in which the transformations are performed can impact the resulting calling and called party numbers used for the call. Unified CM performs the following major types of digit manipulations in the order indicated:

  1. Discarding digits

  2. Called and calling party transformations as defined in the route pattern or for the route group

  3. Prefixing digits

Keep in mind that calling and called party transformations defined on the egress device (gateway or trunk) override calling and called party transformations defined in route patterns and route groups.

Route Groups

Route groups control and point to specific devices, which are typically gateways (MGCP, SIP, or H.323), H.323 or SIP trunks to a gatekeeper, remote Unified CM cluster, or Cisco Unified Border Element. Unified CM sends calls to the devices according to the distribution algorithm assigned. Unified CM supports top-down and circular algorithms.

Route Group Devices

The route group devices are the endpoints accessed by route groups, and they typically consist of gateways or trunks to a gatekeeper or to remote Unified CMs. You can configure the following types of devices in Unified CM:

- Media Gateway Control Protocol (MGCP) gateways

- SIP gateways

- H.323 gateways

- H.225 trunk, gatekeeper controlled — trunk to standard H.323 gateways, via a gatekeeper

- Intercluster trunk, not gatekeeper controlled — direct trunk to another Unified CM cluster

- Intercluster trunk, gatekeeper controlled — trunk to other Unified CM clusters and/or H.323 gateways, via a gatekeeper

- SIP trunk — trunk to another Unified CM cluster, a Cisco Unified Border Element, a Session Border Controller, or a SIP proxy

Note Both the H.225 and intercluster trunk (gatekeeper controlled) will automatically discover if the other endpoint is a standard H.323 gateway or a Unified CM and will select H.225 or Intercluster Trunk protocol accordingly.

Local Route Group

Device pools can be associated with multiple local route groups. Route patterns using a local route group offer a unique characteristic: they allow for dynamic selection of the egress gateway, based on the device originating the call. By contrast, calls routed by route patterns using static route groups will route the call to the same gateway, no matter what device originated the call.

Example 14-2   Comparison of Local and Non-Local Route Groups

In Figure 14-15, a route pattern defined as 9.1[2-9]XX[2-9]XXXXXX points to a route list referencing a non-local route group containing San Francisco gateways. If this route pattern is placed in a partition contained in the calling search spaces of phones in Dallas, San Francisco, and New York, national calls from devices in those three cities will egress to the PSTN in San Francisco.

Figure 14-15   Non-Local Route Group Behavior
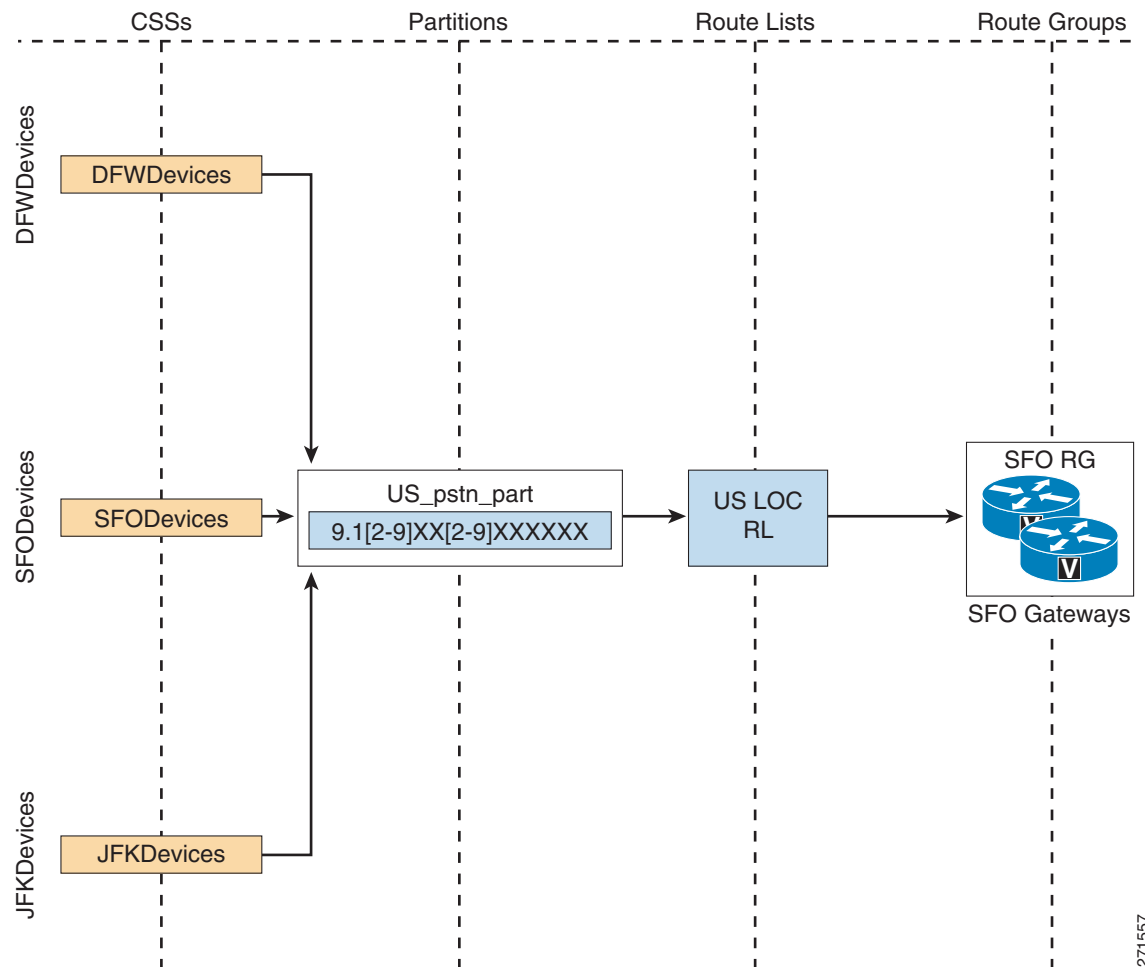
By contrast, if this same route pattern is modified to point to a route list containing the Standard Local Route Group as in Figure 14-16, then calls made from the Dallas site would egress to the PSTN through the Dallas gateway, calls made from the New York site would egress to the PSTN through the New York gateway, and calls made from the San Francisco site would egress to the PSTN through the San Francisco gateway.

The use of Local Route Group allows for egress gateway selection based on the calling device, which allows for site-independent route patterns that can be reused by calling search spaces for phones in all sites.

Figure 14-16   Local Route Group Behavior
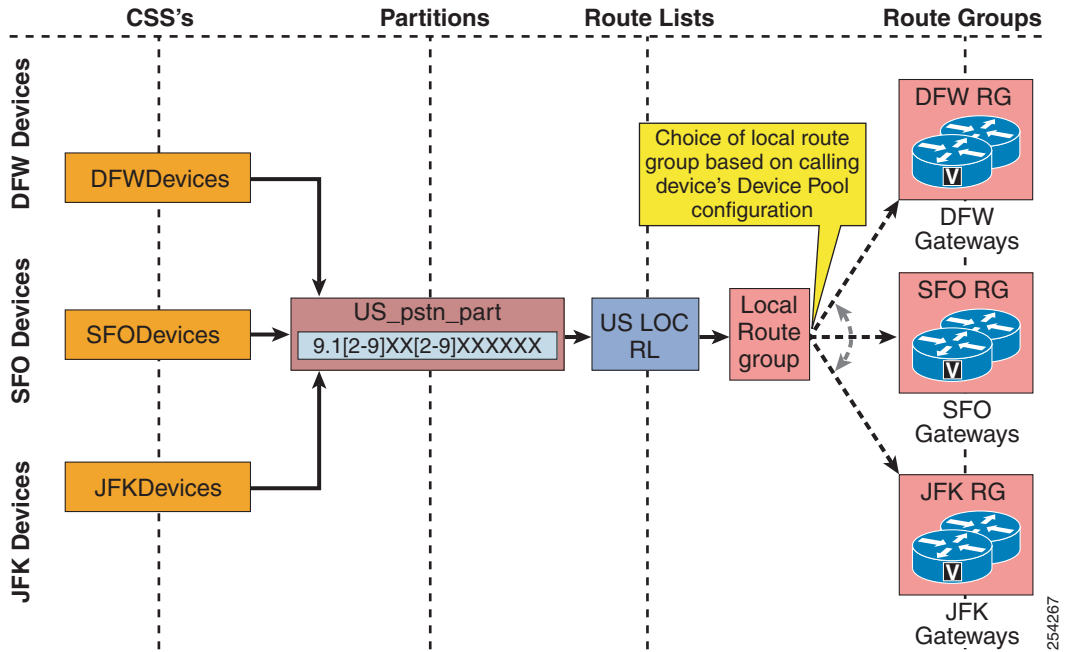
The Device Mobility feature allows the device pool to be assigned to an endpoint based on the current subnet to which it has roamed. This permits assignment of the local route group to be based on the site where the phone is currently located.

Example 14-3   Device Mobility

A phone is moved from the San Francisco site to the New York site. Based on the phone's new IP address (part of the IP subnet associated with the New York site), a New York device pool is assigned to the phone. If the next call placed by the roaming phone matches a route pattern using a route list containing the Standard Local Route Group, it will be routed through the New York gateway.

If a local route group is used in forwarded call scenarios where, for example, phone A calls phone B and B is forwarded to a destination in the PSTN, then the route pattern in the call forward calling search space of phone B determines the class of service for calls forwarded by phone B, whereas by default the local route group associated with phone A's device pool is used to determine the egress gateways when hitting Standard Local Route group in the route list selected by the route pattern found using phone B's call forward calling search space. As a result, typically a gateway local to phone A is used for the forwarded call. This makes sure that the caller ID of the initial caller (phone A) can be sent to the PSTN and that this caller ID will not be screened by the provider. There is a service parameter that allows administrators to configure the local route group selection policy for forwarded calls. The service parameter can be set to:

- **Calling Party's Local Route Group** — Backward compatible default. The local route group associated with the initial caller's device pool is selected (phone A in above example).

- **Original Called Party** — The local route group associated with the called phone's device pool is selected (phone B in above example).

- **Last Redirecting Party** — The local route group associated with the phone's device pool that is forwarding the call to the PSTN is selected (phone B in above example). These last two options differ only in cases where the call is forwarded through multiple hops before it finally gets forwarded out to the PSTN.

Centralized Gateway with Local Failover to the PSTN

Local route groups simplify the local failover to the PSTN for systems where a centralized gateway is configured. A single route list can be used to route PSTN calls for multiple sites while allowing local failover to the gateway at the site of origin.

Example 14-4   Centralized Gateways and Local Failover

A company negotiates a favorable PSTN interconnection rate for a group of trunks located in Chicago. If a route list includes a route group containing gateways in Chicago as its first entry and the Standard Local Route Group as the second choice, then any call it processes will first be sent to the preferred lower-cost gateways in Chicago. If a Chicago gateway is not available, if no ports are free, or if there is not enough bandwidth to allow the call between the calling phone and the Chicago gateway, then the next choice will be to attempt to route the call through the gateway co-located with the calling phone, as determined by the local route group in the calling phone's device pool configuration. (See Figure 14-17.)

Figure 14-17   Centralized Gateway with Local Failover to the PSTN
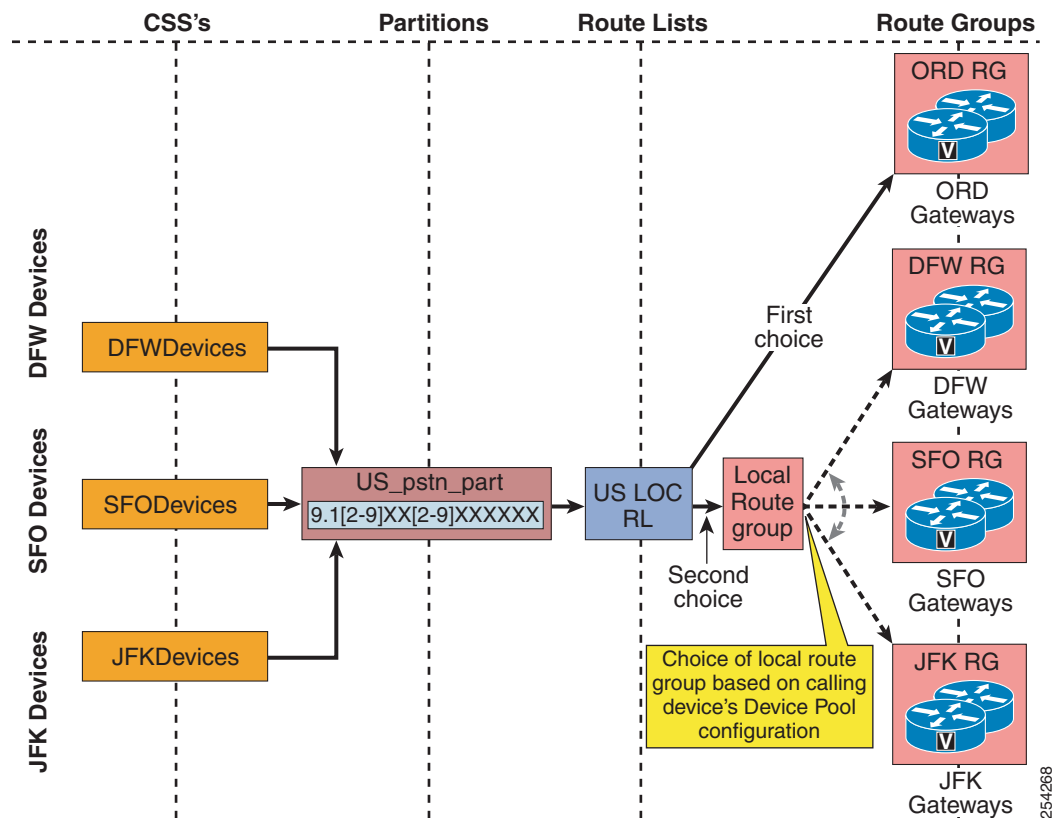
To support route lists with multiple route group elements specific to the calling device, multiple named local route groups can be configured in Unified CM. After names for all local route groups have been defined on the system level, a route group per named local route group can be configured on the device pool level. This, for example, allows to define different local route groups to be used for emergency calls, national PSTN destinations, and other destinations. Using multiple local route groups enables different gateways to be selected for different types of calls. For example, if small sites have small PSTN gateways that should be used only for emergency calls while PSTN calls of this small site should use the PSTN resources of a major hub, then we might want to use the following local route group configuration:

Sites	Local Route Groups	
	LRG_PSTN	LRG_Emergency
SJC (branch)	RG_SFO	RG_SJC
OAK (branch)	RG_SFO	RG_OAK
SFO (hub)	RG_SFO	RG_SFO
TPA (branch)	RG_MCO	RG_TPA
MIA (branch)	RG_MCO	RG_MIA
MCO (hub)	RG_MCO	RG_MCO

In this example the gateways in the major hubs (SFO and MCO) are used for PSTN calls by users in the hub sites and in the branch sites associated with the hub (SJC and OAK use SFO; TPA and MIA use MCO), while emergency calls always use local PSTN resources.

Two local route group names (LRG_PSTN and LRG_Emergency) are defined globally, and then on the device pool of each site a specific route group is assigned for each local route group name. A route group is assigned per device pool and local route group name. The dial plan will then just need to have site-independent route patterns using route lists referencing the above named local route groups. The route list (for example, RL_911) used by the emergency route pattern would have only a single route group entry for LRG_Emergency. Whenever an emergency call is placed and the route list entry LRG_Emergency is selected, Unified CM will de-reference the placeholder LRG_Emergency and will instead use the route group set for LRG_Emergency on the device pool of the calling device. Using the same concept, a site-independent PSTN route pattern can be defined to point to a route list that uses LRG_PSTN. LRG_PSTN then is de-referenced to the route group defined on the device pool level for named local route group LRG_PSTN.

Undefined local route groups are skipped during the egress routing device selection process. If a route list contains a local route group to which no route group has been assigned on the device pool of the calling device, then this entry in the route list is skipped and the next route group member of the route list is considered. When using route lists containing only local route groups, it is important to make sure that route groups are defined consistently on all device pools of all call originating devices to avoid dropping egress calls due to route list exhaustion without ever reaching a real route group.

Pattern Urgency

Translation patterns, route patterns, and DNs can be configured as urgent patterns. The default value for pattern urgency is urgent for translation patterns and non-urgent for route patterns and DNs. Only the pattern urgency of route patterns, translation patterns, and DNs can be configured. All other patterns are always non-urgent.

Marking a pattern as urgent is often used to force immediate routing of certain calls as soon as a match is detected, without waiting for the T302 timer to expire. For example, in North America, if the patterns 9.911 and 9.[2-9]XXXXXX are configured and a user dials 9911, Unified CM has to wait for the T302 timer before routing the call because further digits may cause the 9.[2-9]XXXXXX pattern to match. If Urgent Priority is enabled for the 9.911 route pattern, Unified CM makes its routing decision as soon as the user has finished dialing 9911, without waiting for the T302 timer.

Making a pattern urgent forces the T302 timer to expire as soon as the configured pattern is the best match for the dialed number. This does not mean that the urgent pattern has a higher priority than other patterns; the closest-match logic described in the section on Call Routing in Unified CM, page 14-21, still applies.

For example, assume the route pattern 1XX is configured as urgent and the pattern 12! is configured as a non-urgent route pattern. If a user dials 123, Unified CM will not make its routing decision as soon as it receives the third digit because even though 1XX is an urgent pattern, it is not the best match (10 total patterns matched by 12! versus 100 patterns matched by 1XX). Unified CM will have to wait for inter-digit timeout before routing the call because the pattern 12! allows for more digits to be input by the user.

Consider another example where pattern 12[2-5] is marked as urgent and 12! is configured as a non-urgent pattern. If the user dials 123, the pattern 12[2-5] is the best match (four total patterns matched by 12[2-5] versus 10 patterns matched by 12!). Because the T302 timer is aborted and because the urgent-priority pattern is the best match, no further user input is expected. Unified CM routes the call using pattern 12[2-5].

A variable-length urgent translation pattern like 9011.! in Figure 14-18 will not force inter-digit timeout. As the dialed digits are received and analyzed digit-by-digit, as soon as an urgent translation pattern is the only match, the digit transformations defined on the translation pattern will be executed immediately and the secondary lookup as defined by the CSS on the translation pattern occurs.

Figure 14-18   Inter-Digit Timeout with Urgent Translations
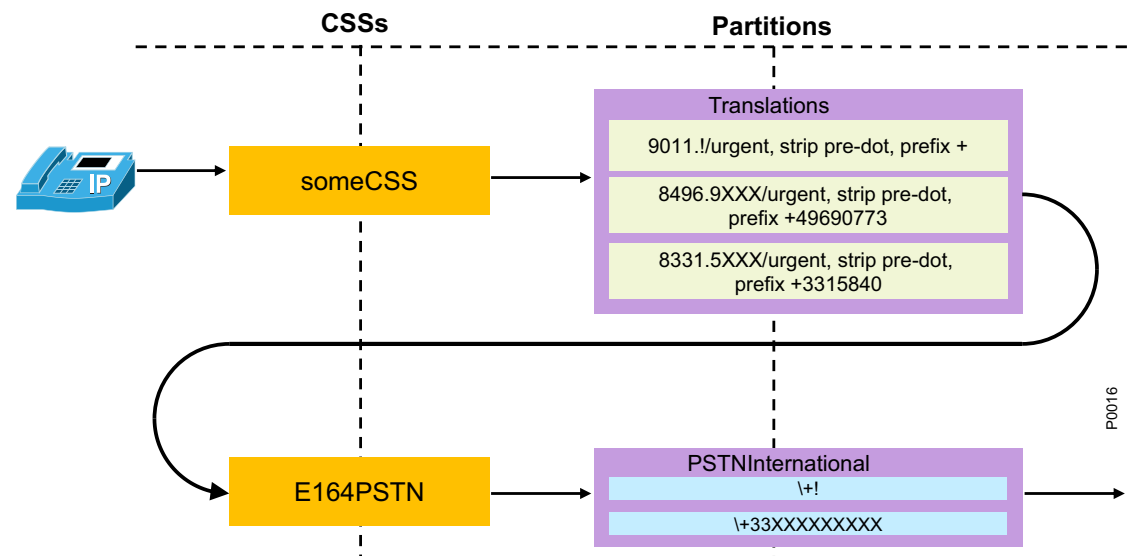
Assuming the configuration in Figure 14-18, when the user dials 901133158405858 the call will be routed immediately after the last digit is dialed. The call will match translation pattern 9011.!, the dialed digits will be transformed to +3333158405858 (9011 discarded and + prefixed), which matches the fixed-length PSTN route pattern \+33XXXXXXXXX (nine-digit NSNs used in France).

On the other hand, if the user dials 9011496907739001, the user will experience inter-digit timeout. After matching 9011.! the resulting digits +496907739001 match route pattern \+!, and Unified CM needs to wait for further digits to make sure that the caller did not intent to continue to dial further digits. Further digits dialed would still match on the same route pattern.

The example in Figure 14-18 also shows how urgent translation patterns can be used to implement some abbreviated off-net dialing habit. Both translation patterns starting with 8 will accept exactly eight digits, transform the dialed digits to +E.164, and then execute the secondary lookup.

Dialing 83315858 will be routed immediately without inter-digit timeout. The dialed digits match fixed length translation pattern 8331.5XXX, and the translated called party number +33158405858 matches the fixed-length route pattern \+33XXXXXXXXX.

However, dialing 84969001 will not be routed immediately by default. The dialed digits are matched by the fixed-length translation pattern 8496.9XXX, and the translated called party number +496907739001 matches the variable-length PSTN route pattern \+!. This example shows that neither the pattern urgency nor the fixed-length characteristic of an intermediate translation pattern match is inherited by the secondary lookup defined by the CSS configured on the intermediate translation pattern (E164PSTN). Because the route pattern matched in the secondary lookup is a variable length pattern, Unified CM is forced to wait for inter-digit timeout. If the intermediate translation pattern is a fixed length translation pattern, waiting for further digits in the secondary lookup does not make much sense because any further digits will lead to a situation where the intermediate translation pattern will not be matched any more. Hence, for fixed length translation patterns it does make sense to change the inter-digit timeout handling for the secondary lookup. To achieve this, the option **Do Not Wait For Interdigit Timeout On Subsequent Hops** on the translation pattern has to be set. If this option is set, then after matching the translation pattern, Unified CM will not wait for any further digits and will just match the translated called party number against the patterns identified by the CSS defined on the intermediate translation pattern. As a general rule, **Do Not Wait For Interdigit Timeout On Subsequent Hops** should be enabled on all fixed length translation patterns.

Calling and Called Party Transformation Patterns

A calling party transformation pattern allows the system to adapt the global form of the calling party's number into the local form required by off-cluster networks connected to the route group devices, such as gateways or trunks.

A called party transformation pattern allows the system to adapt the global form of the called party's number into the local form required by off-cluster networks connected to the route group devices.

Note   Called party transformation patterns do not have any effect on phones. The called party transformation pattern CSS of the device pool does not impart any effects on the phones to which it is assigned.

Both pattern types consist of a numerical representation of the calling or called party number to be matched. The syntax used is the same as that of other patterns such as route patterns, translation patterns, directory numbers, and so forth. (See Figure 14-19.)

The transformation operators include discard digit instructions (for example, pre-dot), a calling party transformation mask, prefix digits, and control over the calling party presentation (either Default, Allowed, or Restricted). Calling party transformation patterns can be configured to use the calling party's external phone number mask as the calling party number.

Partitions and calling search spaces control which calling party transformation patterns are applied to which gateways or trunks. Gateways or trunks can use either their associated device pool's calling party transformation CSS or the device's own calling party transformation CSS, in reverse order of precedence. The same mechanism is used to control the applicability of called party transformation patterns.

Calling and called party transformation patterns configured on a Gateway Configuration page under **Call Routing Information - Outbound Calls** affect the calling or called party number sent to the gateway, as well as the calling or called party's numbering type and numbering plan. Calling and called party transformation patterns applied under **Incoming Calling Party Settings** apply to calls coming from the gateway.

Figure 14-19   Calling and Called Party Transformation Patterns
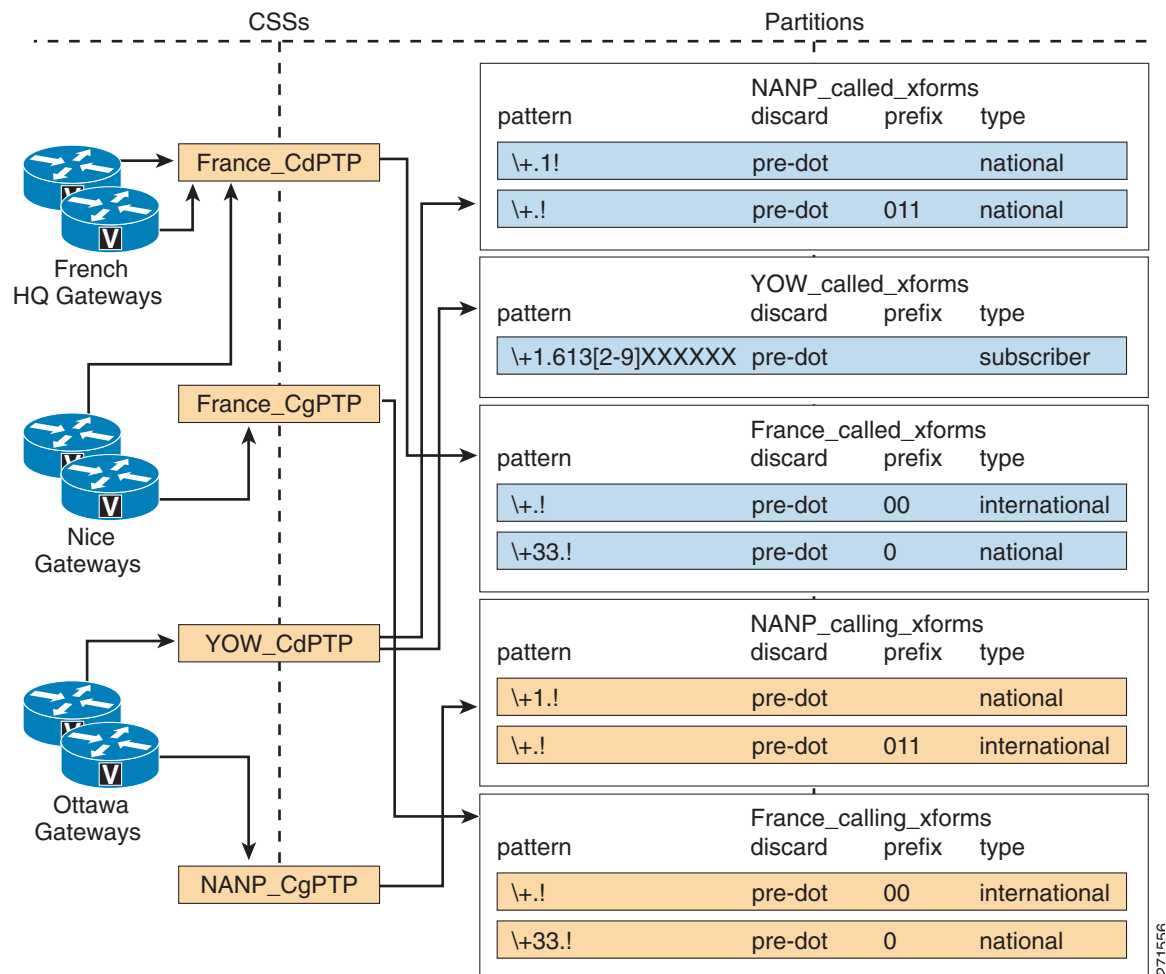
Figure 14-19 illustrates how calling and called party transformation patterns would be applied to different groups of gateways connected to the PSTN in different parts of the PSTN (France and NANP area).

Within the North American Numbering Plan (NANP), gateways located in Ottawa, Canada (airport code YOW) are assigned to the Calling Party Transformation CSS NANP_CgPTP, which contains partition NANP_calling_xforms. Any call with a calling party number beginning with +1 (that is, originating from within the NANP) would match both patterns configured within partition NANP_calling_xforms.

Following the best-match logic, the first pattern will be chosen, and the calling party number will be stripped of the + sign and NANP country code 1. The remaining part of the calling party number will be used as the calling party number sent to the PSTN, with numbering type set to National.

For example, if a call from +1 613 555 1234 were sent out the YOW gateways, the calling party number would be transformed to 613 555 1234 with a numbering type set to National.

If a call from the same caller were to be sent to a French gateway, a different set of calling party transformation patterns would apply. For example, if a call from +1 613 555 1234 were sent out a gateway located in Nice, France (airport code NCE), the calling party transformation patterns contained in partition France_calling_xforms would be applied. In this case, the calling party number would be transformed to 001 613 555 1234 with the numbering type set to International.

Note   Calling party number transformations may be overridden once the call is sent out the gateway. Many service providers will not permit calling party numbers outside a given range, as determined by local service agreements or regulations.

The same process applies to the called party number transformation patterns. For Ottawa gateways, the assigned called party transformation CSS is YOW_CdPTP, which contains partitions NANP_Called_xforms and YOW_Called_xforms. A call placed to a destination number within the Numbering Plan Area 613 would match all patterns contained in these two partitions. However, the best match process would select pattern \+1.613[2-9]XXXXXX.

For example, on a call placed to +1 613 555 9999 through the Ottawa gateways, the called party number would be transformed to 516 555 9999 with a numbering type set to Subscriber.

Incoming Calling Party Settings (per Gateway or Trunk)

Incoming calling party settings can be configured on individual gateways or trunks, at the device pool level, or at the service parameter level, in order of precedence. For each numbering type (Subscriber, National, International, or Unknown), Unified CM allows for the appropriate prefix digits to be configured. Using the service parameter settings is not recommended because the device pool and gateway or trunk settings also allow for definition of strip digit instructions and flexible transformations based on calling party transformation patterns. Digits can be stripped from and prefixed to the string provided as the incoming party number. The digit stripping operation is performed first on the incoming calling party number, and then the prefix digits are added to the resulting string. For example, if the number of digits to be stripped is set to 1 and the prefix digits are set to +33, and the incoming calling party number is 01 58 40 58 58, then the resulting string will be +33 1 58 40 58 58.

Each numbering type can be configured with a calling search space used to apply calling party transformation patterns to the calls. The calling search space should contain partitions containing calling party transformation patterns exclusively. This allows the modifications applied to the calling party number to be based on the structure of the calling party number rather than strictly on its numbering type. The calling party transformation patterns use regular expressions to match the calling party number. The best-match process is used to choose between multiple matches, and the selected pattern's calling party transformations are applied to the call.

Incoming Called Party Settings (per Gateway or Trunk)

Equivalent to the incoming calling party settings described in the previous section, incoming called party transformations can also be configured. These incoming called party transformations enable normalization of incoming called party information prior to actually routing the call.

Each numbering type can be configured with a calling search space used to apply called party transformation patterns to the calls. The calling search space should contain partitions containing called party transformation patterns exclusively. This allows the modifications applied to the called party number to be based on the structure of the called party number rather than strictly on its numbering type. The called party transformation patterns use regular expressions to match the called party number. The best-match process is used to choose between multiple matches, and the selected pattern's called party transformations are applied to the call.

Calling Privileges in Unified CM

Dialing privileges are configured in order to control which types of calls are allowed (or prevented) for a particular endpoint (such as phones, gateways, or CTI applications). All calls handled by Unified CM are subjected to the dialing privileges implemented through the configuration of the following elements:

- Partitions, page 14-40
- Calling Search Spaces, page 14-41

A *partition* is a group of directory numbers (DNs) or directory URIs with similar accessibility, and a *calling search space* defines which partitions are accessible to a particular device. A device can call only those DNs and directory URIs located in the partitions that are part of its calling search space.

As illustrated in Figure 14-20, items that can be placed in partitions all have a dialable pattern, and they include phone lines, route patterns, translation patterns, CTI route group lines, CTI port lines, voicemail ports, and Meet-Me conference numbers. Conversely, items that have a calling search space are all devices capable of dialing a call, such as phones, phone lines, gateways, and applications (via their CTI route groups or voicemail ports).

Figure 14-20   Partitions and Calling Search Spaces
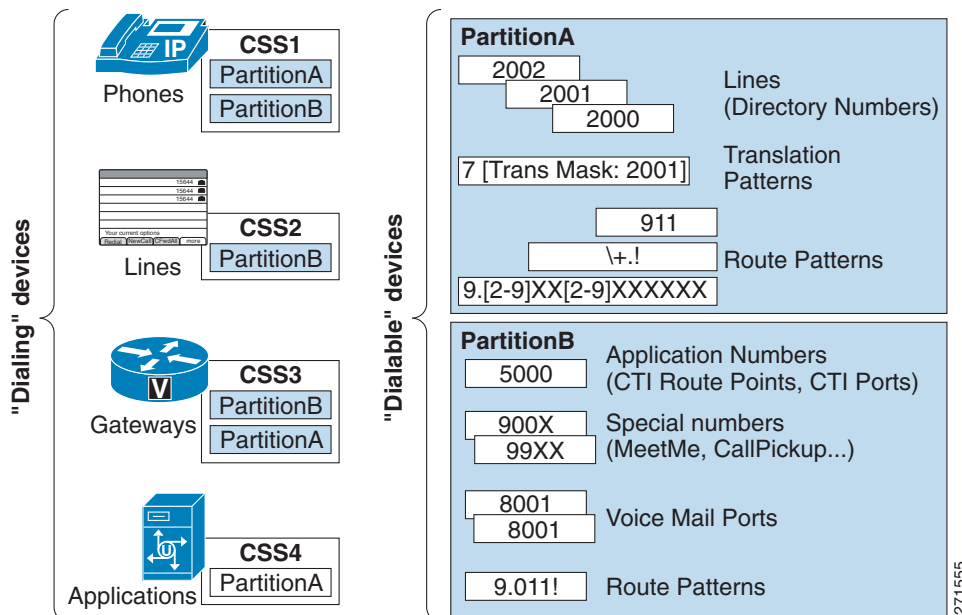
Partitions

The dial plan entries that you may place in a partition include IP phone directory numbers, directory URIs, translation patterns, route patterns, CTI route points, and voicemail ports. As described in the section on Call Routing in Unified CM, page 14-21, if two or more numeric dial plan entries (directory numbers, route patterns, or so forth) overlap, Unified CM selects the entry with the closest match (most specific match) to the dialed number. In cases where two dial plan entries match the dialed pattern equally, Unified CM selects the dial plan entry that appears first in the calling search space of the device making the call. Directory URIs always have to match completely; there is no concept of partial matches for directory URIs.

For example, consider Figure 14-21, where route patterns 1XXX and 23XX are part of Partition_A and route patterns 12XX and 23XX are part of Partition_B. The calling search space of the calling device lists the partitions in the order Partition_A:Partition_B. If the user of this device dials 2345, Unified CM selects route pattern 23XX in Partition_A as the matching entry because it appears first in the calling device's calling search space. However, if the user dials 1234, Unified CM selects route pattern 12XX in Partition_B as the matching entry because it is a closer match than 1XXX in Partition_A. Remember that the partition order in a calling search space is used exclusively as a tie-breaker in case of equal matches based on the closest-match logic.

Figure 14-21   Impact of Partition Order on the Matching Logic
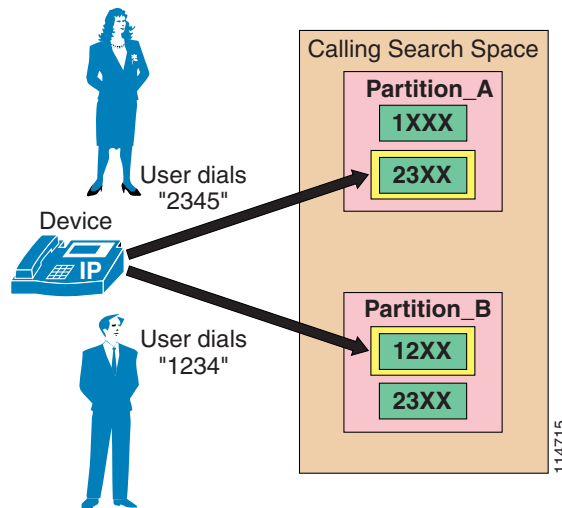

> **Note**   When multiple equal-precision matches occur in the same partition, Unified CM selects the entry that is listed first in its local dial plan database. Since you cannot configure the order in which the dial plan database lists dial plan entries, Cisco strongly recommends that you avoid any possibility of equal-precision matches coexisting within the same partition because the resulting dial plan logic is not predictable in such cases.

Partitions can be activated or deactivated based on the time and date. You can activate or deactivate partitions by first configuring time periods and schedules within Unified CM Administration and then assigning a specific time schedule to each partition. Outside of the times and days specified by the schedule, the partition is inactive, and all patterns contained within it are ignored by the Unified CM call routing engine. For more information on this feature, see Time-of-Day Routing, page 14-87.

Calling Search Spaces

A calling search space defines which partitions are accessible to a particular device. Devices that are assigned a certain calling search space can access only the partitions listed in that calling search space. Attempts to dial a DN or directory URI in a partition outside that calling search space will fail, and the caller will hear a busy signal.

If you configure a calling search space both on an IP phone line and on the device (phone) itself, Unified CM concatenates the two calling search spaces and places the line's calling search space in front of the device's calling search space, as shown in Figure 14-22.

Figure 14-22   Concatenation of Line and Device Calling Search Spaces for IP Phones
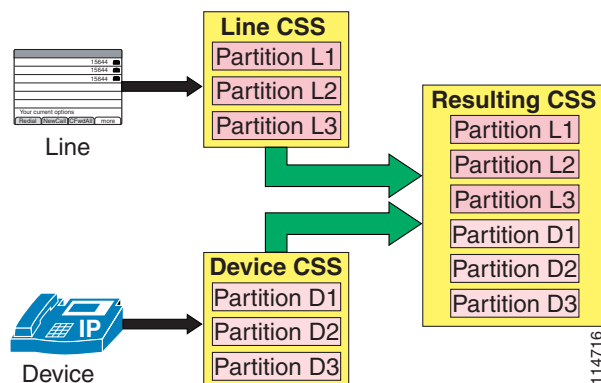
Note   When device mobility is not used, the device calling search space is static and remains the same even as the device is moved to different parts of the network. When device mobility is enabled, the device calling search space can be determined dynamically based on where in the network the phone is physically located, as determined by the phone's IP address. See Device Mobility, page 14-80, for more details.

If the same route pattern appears in two partitions, one contained in the line's calling search space and one contained in the device's calling search space, then according to the rules described in the section on Partitions, page 14-40, Unified CM selects the route pattern listed first in the concatenated list of partitions (in this case, the route pattern associated with the line's calling search space).

The maximum length of the combined calling search space (device plus line) is 1024 characters, including separator characters between each partition name. (For example, the string "partition_1:partition_2:partition_3" contains 35 characters.) Thus, the maximum number of partitions in a calling search space varies, depending on the length of the partition names. Also, because the calling search space clause combines the calling search space of the device and that of the line, the maximum character limit for an individual calling search space is 512 (half of the combined calling search space clause limit of 1024 characters).

Therefore, when you are creating partitions and calling search spaces, keep the names of partitions short relative to the number of partitions that you plan to include in a calling search space. For more details on configuring calling search spaces, refer to the *Cisco Unified Communications Manager Administration Guide*, available online at

http://www.cisco.com

Before you configure any partitions or calling search spaces, all DNs reside in a special partition named <None>, and all devices are assigned a calling search space also named <None>. When you create custom partitions and calling search spaces, any calling search space you create also contains the <None> partition, while the <None> calling search space contains *only* the <None> partition.

Note   Any dial plan entry left in the <None> partition is implicitly reachable by *any* device making a call. Therefore, to avoid unexpected results, Cisco strongly recommends that you do not leave dial plan entries in the <None> partition.

Note   Cisco strongly recommends that you do not leave any calling search space defined as <None>. Doing so can introduce dial plan behavior that is difficult to predict.

Special Considerations for Transformation Patterns

Calling and called transformation patterns are also placed in partitions, and those partitions are included in calling search spaces (CSSs) but not in order to control calling privileges. The partitioning of transformation patterns serves to choose which transformations are applied to which gateways, trunks, or phones. Partitions contained in calling party transformation pattern CSSs should contain only calling party transformation patterns. Likewise, partitions contained in called party transformation pattern CSSs should contain only called party transformation patterns.

Call-Forward Calling Search Spaces

Note   Call Forward All actions are different than any other call-forward action in that the destination number is entered by each individual user when the feature is activated from a phone.

The system allows you to decide how call-forward calling search spaces take effect. There are three possible options, as selected by the Calling Search Space Activation policy:

- Use System Default

  If you configure the Calling Search Space Activation Policy to Use System Default, then the CFA CSS Activation Policy cluster-wide service parameter determines which Forward All Calling Search Space will be used. The CFA CSS Activation Policy service parameter can be set to With Configured CSS or to With Activating Device/Line CSS (see below). By default, the CFA CSS Activation Policy service parameter is set to With Configured CSS.

- With Configured CSS

  If you select the With Configured CSS option, the Forward All Calling Search Space and Secondary Calling Search Space for Forward All explicitly configured in the Directory Number Configuration window control the forward-all activation and call forwarding. If the Forward All Calling Search Space is set to None, no CSS gets configured for Forward All. A forward-all activation attempt to any directory number with a partition will fail. No change in the Forward All Calling Search Space and Secondary Calling Search Space for Forward All occurs during the forward-all activation.

- With Activating Device/Line CSS

  If you prefer to use the combination of the Directory Number Calling Search Space and Device Calling Search Space without explicitly configuring a Forward All Calling Search Space, select With Activating Device/Line CSS for the Calling Search Space Activation Policy. With this option, when Forward All is activated from the phone, the Forward All Calling Search Space and Secondary Calling Search Space for Forward All are automatically populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device. When you set the Forward All Destination from Unified CM Administration, the Forward All Calling Search Space and Secondary Calling Search Space are not automatically populated and have to be configured explicitly. The two calling search spaces are concatenated, and the resulting calling search space is used to validate the number entered as a Call Forward All destination.

  With this configuration (Calling Search Space Activation Policy set to With Activating Device/Line), if the Forward All Calling Search Space is set to None when forward-all is activated through the phone, the combination of Directory Number Calling Search Space and activating Device Calling Search Space is used to verify the forward-all attempt.

On Type-A IP phones running SIP, if Call Forward All is invoked from the phone itself, the device's Rerouting Calling Search Space is used for forwarded calls. If Forward All actions are invoked from the Unified CM User page or the Unified CM Administrative page, then any Forward All action initiated from the phone is irrelevant.

For example, assume an Type-A IP phone running SIP is configured with Forward All to extension 3000 from the Unified CM User page. At the same time, the phone itself is configured to Forward All to extension 2000. All calls made to that phone will be forwarded to extension 3000.

Note   On Type-A IP phones running SIP, invoking Forward All from the Unified CM User or Administrative pages will not be reflected on the phone. The phone does not display any visual confirmation that calls are forwarded.

When Forward All is initiated from an IP phone running SCCP or from an Type-B IP phone running SIP, user input is simultaneously compared to the patterns allowed in the configured Forward All calling search space(s). If an invalid destination pattern is configured, the user will be presented with reorder tone. When Forward All is invoked from an Type-A IP phone running SIP, Forward All user input is stored locally on the phone and is not verified against any calling search space in Unified CM. If user input corresponds to an invalid destination, no notification is offered to the user. Calls made to that phone will be presented with reorder tone as the phone tries to initiate a SIP re-route action to an invalid destination number.

Other Call Forward Types

The calling search spaces configured for the various other types of call forward (Forward Busy, Forward No Answer, Forward No Coverage, forward on CTI failure, and Forward Unregistered) are standalone values not concatenated with any other calling search space.

Call Forward settings (except Forward All) can be configured separately for internal or external call types. For example, a user might want to have their phone Call Forward No Answer to voicemail for external callers but forward to a cell phone number if the caller is a co-worker calling from another IP phone on the network. This is possible by using different configurations for the Internal and External Call Forward settings.

When the Forward All calling search space is left as <None>, the results are difficult to predict and depend on the Unified CM release. Therefore, Cisco recommends the following best practices when configuring call-forward calling search spaces:

- Always provision the call-forward calling search spaces with a value other than <None>. This practice avoids confusion and facilitates troubleshooting because it enables the network administrator to know exactly which calling search space is being used for forwarded calls.

- Configure the Call Forward Busy and Call Forward No Answer calling search spaces with values that allow them to reach the DNs for the voicemail pilot and voicemail ports but not external PSTN numbers.

- Configure both the Call Forward All calling search space and the Secondary Calling Search Space for Forward All, according to your company's policy. Many companies choose to restrict forwarded calls to internal numbers only, to prevent users from forwarding their IP phone lines to a long-distance number and dialing their local IP phone number from the PSTN to bypass long-distance toll charges on personal calls.

The Call Forward Unregistered (CFUR) feature is a way to reroute calls placed to a temporarily unregistered destination phone. The configuration of CFUR consists of two main elements:

- Destination selection

    When the DN is unregistered, calls can be rerouted to either of the following destinations:

    - Voicemail

        Calls can be sent to voicemail by selecting the voicemail checkbox and configuring the CFUR calling search space to contain the partition of the voicemail pilot number.

    - A directory number used to reach the phone through the PSTN

        This approach is preferred when a phone is located within a site whose WAN link is down. If the site is equipped with Survivable Remote Site Telephony (SRST), the phone (and its co-located PSTN gateway) will re-register with the co-located SRST router. The phone is then able to receive calls placed to its PSTN DID number.

        In this case, the appropriate CFUR destination is the corresponding PSTN DID number of the original destination DN. Configure this PSTN DID in the destination field, preferably in E.164 format, including the + sign (for example, +1 415 555 1234). This allows the CFUR destination to be processed by the calling phone's local route group, whether or not it uses the same off-net access code and PSTN prefixes as the unregistered phone.

- Calling search space

    Unified CM attempts to route the call to the configured destination number by using the called DN's CFUR calling search space. The CFUR calling search space is configured on the target phone and is used by all devices calling the unregistered phone. This means that all calling devices will use the same combination of route pattern, route list, and route group to place the call. Cisco recommends that you configure the CFUR calling search space to route calls to the CFUR destination using patterns pointing to route lists referencing the Standard Local Route Group. This will ensure that the egress gateway to the PSTN is chosen based on the calling device.

The Call Forward Unregistered functionality can result in telephony routing loops if a phone is unregistered while the gateway associated with the phone's DID number is still under control of Unified CM, as is the case if a phone is simply disconnected from the network. In such a case, the initial call to the phone would prompt the system to attempt a first CFUR call to the phone's DID through the PSTN. The resulting incoming PSTN call would in turn trigger another CFUR attempt to reach the same phone's DN, triggering yet another CFUR call from the central PSTN gateway through the PSTN. This cycle could repeat itself until system resources are exhausted.

The service parameter **MaximumForwardUnRegisteredHopsToDn** controls the maximum number of CFUR calls that are allowed for a DN at the same time. The default value of 0 means the counter is disabled. If any DNs are configured to reroute CFUR calls through the PSTN, loop prevention is required. Configuring this service parameter to a value of 1 would stop CFUR attempts as soon as a single call is placed through the CFUR mechanism. This setting would also allow only one call to be forwarded to voicemail, if CFUR is so configured. Configuring this service parameter to a value of 2 would allow for up to two simultaneous callers to reach the voicemail of a DN whose CFUR setting is configured for voicemail, while also limiting potential loops to two for DNs whose CFUR configuration sends calls through the PSTN.

> **Note** Extension Mobility DNs should not be configured to send Call Forward Unregistered calls to the PSTN DID associated with the DN. The DNs of Extension Mobility profiles in the logged-out state are deemed to be unregistered, therefore any calls to the PSTN DID number of a logged-out DN would trigger a routing loop. To ensure that calls made to Extension Mobility DNs in the logged-out state are sent to voicemail, ensure that their corresponding Call Forward Unregistered parameters are configured to send calls to voicemail.

Global Dial Plan Replication

With Global Dial Plan Replication (GDPR), independent Unified CM clusters can share dial plan elements such as URIs, +E.164 numbers, enterprise numbers, +E.164 patterns, enterprise patterns, and PSTN failover numbers using the Intercluster Lookup Service (ILS). All local dial plan information advertised by a Unified CM cluster is advertised as part of a single GDPR catalog. Reachability for advertised dial plan elements is achieved by advertising a location attribute (SIP route string) together with each GDPR catalog.

Enterprise-specific numbers and patterns represent a global enterprise-specific dialing habit that allows abbreviated on-net inter-site dialing. Enterprise-specific numbers and patterns to be exchanged through GDPR have to be globally significant. +E.164 numbers and patterns based on the characteristics of an E.164 numbering scheme are globally significant by definition.

This location attribute in multi-cluster environments is used to direct calls for any destination learned via GDPR to the correct cluster. For directory URIs this can be used when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as <user>@example.com is used. The host portion, example.com, does not uniquely identify the remote Unified CM cluster that hosts a given URI, but an appropriately chosen SIP route string does.

For every DN in Unified CM a +E.164 alternate number and an enterprise alternate number can be defined based on masks to be applied to the configured DN. These alternate numbers can optionally be added into local partitions. Each alternate number can be configured individually to be advertised to remote clusters using GDPR.

For every DN in Unified CM, up to five URIs can be defined as aliases. Each individual URI can be configured to be advertised to remote clusters using GDPR.

For every DN in Unified CM, the enterprise or +E.164 alternate number can be selected to be advertised as the PSTN failover number. On remote clusters this PSTN failover number is used for PSTN failover for calls to the +E.164 alternate number, enterprise alternate number, or URIs. PSTN failover is triggered if a call to any GDPR learned destination fails with cause codes other than **unallocated number**, **user busy**, **normal call clearing**, **destination out of order**, or **service not available**. The PSTN failover number is also used for Automated Alternate Routing (AAR) in case of call admission control failure. For calls to the PSTN failover number, the AAR CSS of the calling device is used on the remote cluster.

In addition to DN related information (directory URIs, enterprise alternate numbers, +E.164 alternate numbers, and PSTN failover numbers), GDPR also allows advertising of enterprise patterns and +E.164 patterns. Patterns are not associated with DNs and can be defined using wildcards (fixed length and variable length). The PSTN failover number for enterprise and +E.164 patterns is defined based on strip and prefix instructions.

GDPR not only allows advertising of local routing information but also supports imported GDPR catalogs that can contain URIs, enterprise patterns, and +E.164 patterns. For each imported GDPR catalog, a unique locations attribute (SIP route string) is advertised. This allows clusters to inject routing information for non-local destinations.

On the receiving side, all directory URIs learned through GDPR are put into a single local repository to be consulted when routing a non-numeric URI does not find a local URI match. All learned URIs are treated as equivalent from the class-of-service perspective.

In contrast to this, numeric patterns and numbers learned through GDPR are put into local partitions based on the type of information. Four separate partitions can be configured for +E.164 alternate numbers, enterprise alternate numbers, +E.164 patterns, and enterprise patterns. The default partitions for these different types of learned information are **Global Learned E164 Numbers**, **Global Learned E164 Patterns**, **Global Learned Enterprise Numbers**, and **Global Learned Enterprise Patterns**. To avoid unnecessary inter-digit timeout when dialing remote destinations learned through GDPR, the pattern urgency for learned destinations can be configured per class.

Cisco strongly recommends configuring +E.164 numbers and fixed length +E.164 patterns to be inserted into local digit analysis as **urgent**.

For details of how calls to directory URIs and numeric destinations learned through GDPR are routed, see the section on Routing of SIP Requests in Unified CM, page 14-47.

Routing of SIP Requests in Unified CM

Routing of SIP requests received from SIP trunks or SIP endpoints follows certain rules to make sure that both local and intercluster routing requirements are met. Figure 14-23 shows a flowchart of routing decisions made by Unified CM. The first step is to check whether the left-hand side (user portion) of the URI is a directory number or a directory URI.

Figure 14-23   Call Routing Logic for SIP Request
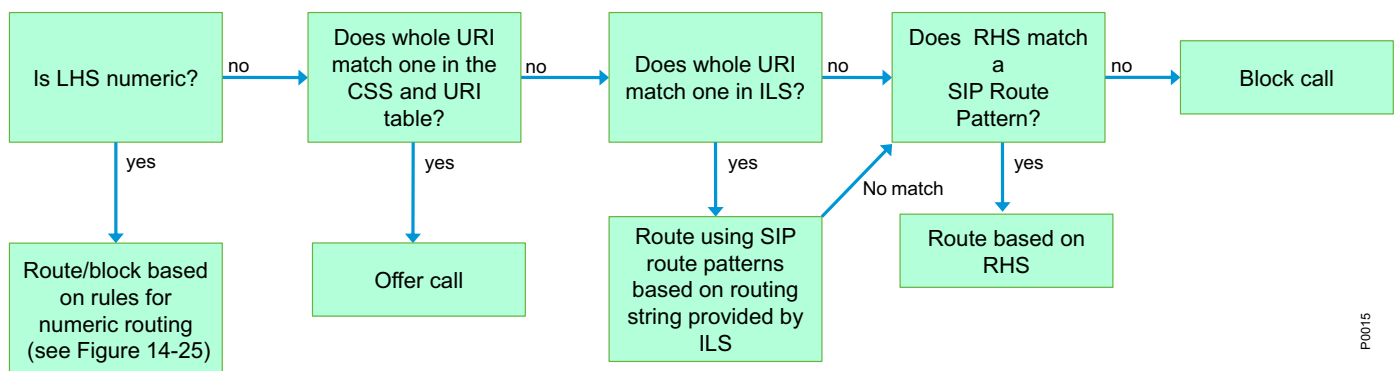
Numeric URI Versus Directory URI

If the SIP request carries a user=phone tag, the SIP URI will always be interpreted as a numeric SIP URI. If no user=phone is present, the decision is based on the dial string interpretation setting in the calling device's (endpoint or trunk) SIP profile. This setting either defines a set of characters that Unified CM will accept as part of numeric SIP URIs (0-9, *, #, +, and optionally A-D) or it enforces the interpretation as a directory URI.

In releases prior to Unified CM 9.0, all SIP URIs are always treated as numeric SIP URIs.
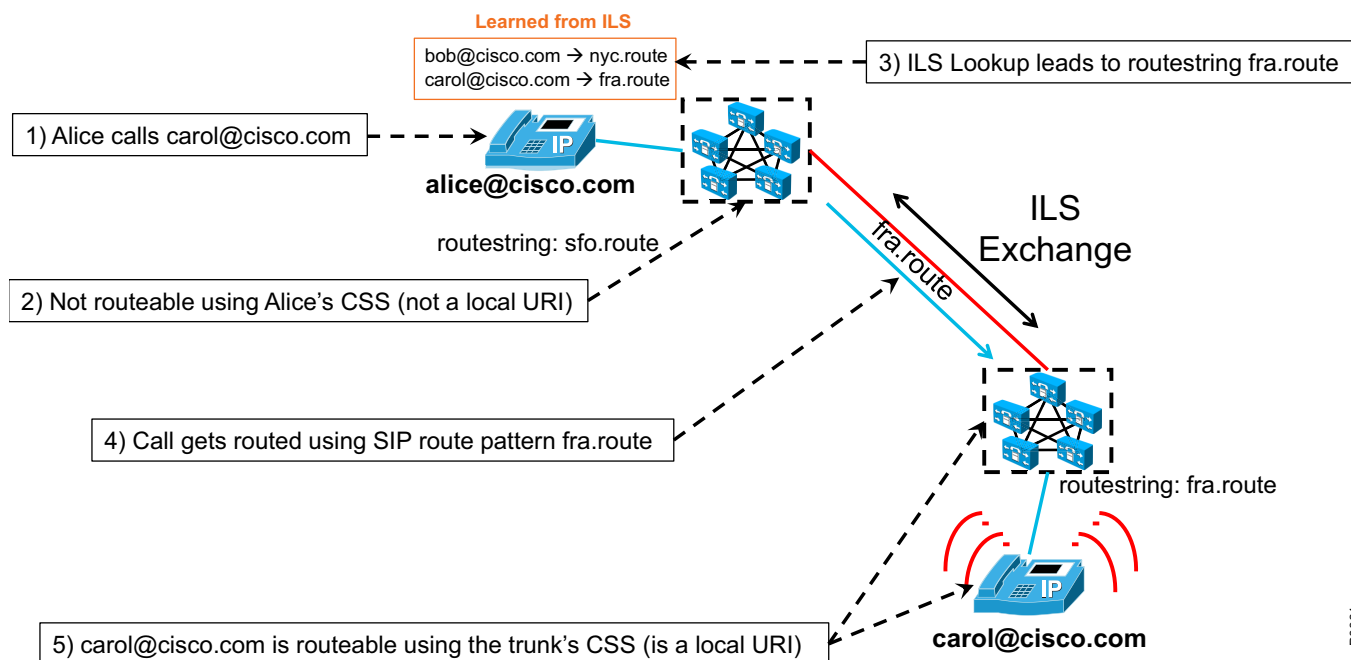
Routing Directory URIs

The next step after identifying a SIP URI as being non-numeric is to try to route the SIP request based on the calling search space of the calling device. Unified CM searches for a full match of the SIP URI against all directory URIs configured in the partitions addressed by the calling device's calling search space. If a match is found, the call is extended to the directory number associated with the matched local directory URI.

In case no matching local directory URI is found, Unified CM tries to locate the SIP URI in imported GDPR catalogs or GDPR catalogs learned from remote systems, again by searching for a full match. In case of a match, the SIP request is routed by matching the SIP route string (location identifier) associated with the GDPR catalog, as part of which the found directory URI was learned, against configured SIP route patterns addressed by the calling device's calling search space. (See Figure 14-24.)

In case the SIP URI does not match a local directory URI and also does not match any directory URI in any GDPR catalog, Unified CM then routes the SIP request based only on matching the right-hand side of the SIP URI against configured SIP route patterns. This routing of last resort can be used to create a default route for all SIP URIs not known locally or on any other call control participating in GDPR.

Figure 14-24   Example for Routing a Directory URI

Figure 14-24 shows an example of how a dialed directory URI might be routed by Unified CM. In this example the bottom Unified CM cluster advertises the local directory URI carol@cisco.com. All local directory URIs of this Unified CM cluster are advertised under the SIP routestring fra.route. As part of this information exchange through GDPR, the Unified CM cluster at the top populated its learned directory URI table with the association of carol@cisco.com to the SIP routestring fra.route. If someone then places a call from the phone registered in the top cluster to directory URI carol@cisco.com, the local lookup of directory URI carol@cisco.com will fail because carol@cisco.com is not a local directory URI. The next step in the routing process is to search for carol@cisco.com in the table of directory URIs learned through GDPR. This search will find the information learned from the bottom

cluster, and the originating cluster at the top then takes the learned SIP routestring fra.route and tries to find a route by matching this SIP routestring fra.route against the configured SIP route patterns addressed by the calling device's calling search space. A SIP route pattern fra.route is configured and points to a route list that ultimately leads to the SIP trunk pointing to the target Unified CM cluster. The originating Unified CM cluster thus routes the call down to the destination Unified CM cluster. The destination in the sent SIP request will be carol@cisco.com. On the destination cluster, the same routing logic as shown in Figure 14-23 then tries to match carol@cisco.com against all local directory URIs on the destination cluster, which leads to a full match and the target device rings.

The above example shows that the SIP route string namespace is completely independent of the directory URI namespace. There is no requirement to use SIP route strings that are related in any way to the structure of the namespace used for the host portion of directory URIs. This allows to optimize the SIP route string namespace based on the desired routing topology. To disambiguate between SIP route patterns used to directly match on the URI host portion and SIP route patterns used to route directory URIs based on SIP route strings, Cisco highly recommends using an independent namespace for SIP route string route patterns (for example, ".route" or ".ils").

In the above example, the SIP route strings chosen basically identify the individual call controls (fra.route, nyc.route), and the SIP route pattern grid used to route directory URI SIP requests based on learned SIP route strings uses explicit patterns (fra.route, nyc.route) to create the desired reachability. In a hierarchical topology, hierarchical SIP route strings (for example, sjc.us.route, nyc.us.route, fra.de.route, and muc.de.route) might be used together with wildcard SIP route patterns (*.de.route, *.us.route) routing to the respective aggregating Cisco Unified Communications Manager Session Management Edition (SME) clusters responsible for the addressed set of Unified CM clusters.

Routing Numeric URIs

If a SIP URI is considered to be a numeric URI either because the request included a user=phone tag or based on the originating device's SIP profile dial string interpretation settings, the call is handled according to the flowchart shown in Figure 14-25. For Unified CM prior to release 9.0, this is the standard routing procedure for routing of SIP requests.

Figure 14-25   Call Routing Logic for numeric SIP Request
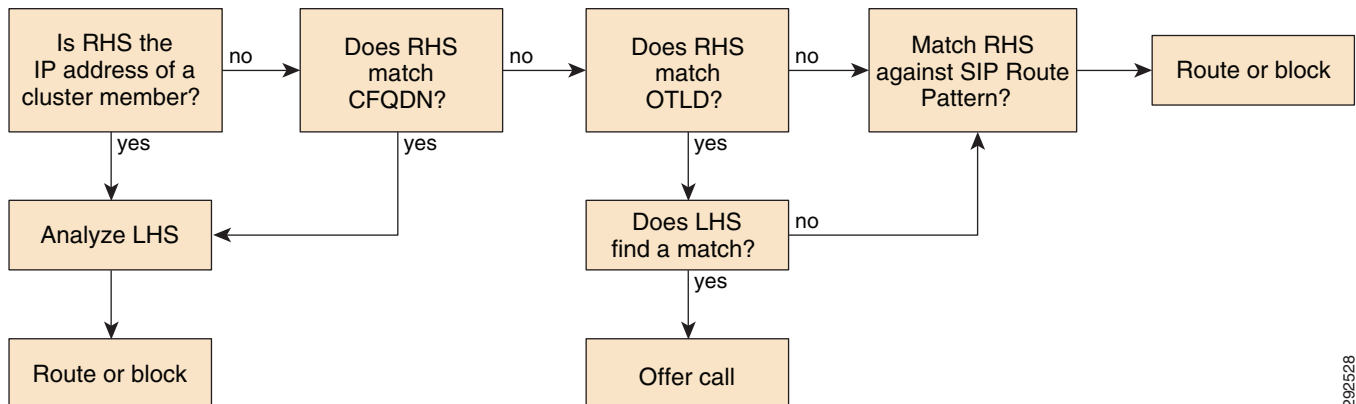
The first step is to check whether the right-hand side of the SIP URI is an IP address or hostname of any server that is a member of the Unified CM cluster or matches the Cluster Fully Qualified Domain Name (CFQDN) configured in Unified CM enterprise parameters. In this case the left-hand side of the URI is considered to be a local numeric pattern and will be matched against numeric patterns existing in local digit analysis using the calling device's calling search space.

The next step is to check whether the right-hand side of the SIP URI matches the Organization Top Level Domain (OTLD) configured in Unified CM enterprise parameters. If this is the case, again Unified CM will try to route the call numerically using the calling device's calling search space. But if no match can be found, then routing will fall back to route the call by matching the right-hand side of the SIP URI against the configured SIP route patterns.

Assuming a Unified CM cluster with cluster members having IP addresses 192.168.10.10, 192.168.10.11, 192.168.20.10, and 192.168.20.11, cluster fully qualified domain name configured as ucm1.cisco.com, and organization top-level domain configured as cisco.com, then all of the following SIP URIs would be routed to local directory number 1234:

- 1234@192.168.10.10
- 1234@192.168.10.11
- 1234@192.168.20.10
- 1234@192.168.20.11
- 1234@ucm1.cisco.com
- 1234@cisco.com

Assuming that no local match for 1234 exists, the first five calls would fail immediately while Unified CM would try to route the sixth call by matching cisco.com against the configured SIP route patterns.

Numeric matching can result in a match on any type of numeric pattern existing locally. This does not only include directory numbers and route patterns and other regular numeric patterns, but can also lead to a match on any numeric pattern learned through GDPR (+E.164 number or pattern, or enterprise number or pattern). If a GDPR learned destination is matched, this immediately leads to a secondary lookup matching the SIP route string of the matched GDPR information against configured SIP route patterns. For the secondary lookup to match the SIP route string, the same calling search space is used that also has been used for the initial numeric lookup. This behavior can be used to restrict access to information learned as part of certain GDPR catalogs by defining a CSS that does not provide access to the SIP route pattern routing the associated SIP route strings.

Note   To be able to reach destinations learned through GDPR, the calling device's calling search space has to include the partition that the GDPR learned pattern is residing in and also the partition that the SIP route pattern resides in, which matches the SIP route string associated with the GDPR learned destination.

Cisco TelePresence Video Communication Server

This section provides a high-level overview of the call routing mechanisms available in the Cisco TelePresence Video Communication Server (VCS). For more detailed descriptions, refer to the *Cisco TelePresence Video Communication Server Administrator Guide* and the Cisco VCS deployment guides available at

http://www.cisco.com/en/US/products/ps11337/tsd_products_support_series_home.html

This section covers the following topics:

Cisco VCS Addressing Schemes: SIP URI, H.323 ID, and E.164 Alias

The Cisco TelePresence Video Communication Server (VCS) enables communications using H.323 and SIP, and it allows any addressing scheme inherently supported by these protocols.

The dialable address formats are:

- IPv4/IPv6 address

  Endpoints and multipoint devices can be called using IP addressing, either IPv4 or IPv6.

- H.323 ID

  The H.323 ID is an alphanumeric identifier for H.323 endpoints. It can be any string of alphanumeric characters. Where SIP and H.323 registration is required for endpoints (dual registration), this alias usually matches the SIP URI.

- E.164 alias

  E.164 uses the same numbering scheme as the PSTN. It is an option that can be configured in H.323 (numbering plan used in the PSTN) together with the H.323 ID.

- SIP URI

  This is an alias that always takes the form *username@domain.*

- ENUM

  ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number (a telephone number) even if that endpoint has registered using a different format of alias.

In principle, any SIP URI can be made using E.164 aliases. The username portion of the alias will be the E.164 number, and the hostname portion will be the domain. When configuring this kind of E.164 mapping using SIP, the alias loses information about the user. In this case, FindMe can be configured with the proper alias *username@domain*, thus hiding the complexity of many different addressing schemes. The FindMe alias can be associated to any dialable device, regardless of its addressing scheme.

Cisco VCS Addressing Zones

The VCS receives calls from locally registered endpoints, from neighboring systems, and from endpoints on the public Internet.

Endpoints, gateways, multipoint devices, and content servers registered to the VCS are said to be part of the Local Zone. The Local Zone is further divided into subzones, some of which exist by default and some others might be configured by the administrator.

More generally, a zone is a collection of endpoints that share the same dialing behavior and bandwidth settings. Zones can be local to the VCS or remote.

If dialable entities are not registered on VCS, they might be available on remote zones managed by other call control or systems. These remote zones include: Neighbor Zone, Traversal Client and Traversal Server Zones, DNS Zone, and ENUM Zone.

The concept of Neighbor Zone is analogous to that of a trunk on Cisco Unified CM; it is a SIP or H.323 trunk-side connection to another VCS or Unified CM server or cluster, a third-party call control system, a multipoint device, or a gateway.

A DNS Zone is a non-local destination that can be found using DNS services (SRV). Traversal Client and Server are zones that give access to communications over the Internet using VCS Control and VCS Expressway. An ENUM zone is a non-local destination that is reachable using ENUM services.

Cisco VCS Pattern Matching

Important concepts on VCS routing logic are transforms, also called pre-search transforms, and search rules, also known as searches. The difference between transforms and searches is that searches have a destination target zone, while transforms are configured at system level and cannot be applied per single zone.

Searches and transforms are applied following a priority order configured by an administrator, and they use regular expressions for pattern analysis and string manipulation.

The pre-search transform concept is analogous to translation patterns on Unified CM, with the exception that the use of regular expressions enables alphanumeric transformations.

Search rules are analogous to route patterns in Unified CM. While route patterns are applied to the trunk or route list, search rules have a destination zone as a target.

Both search rules and transforms have the following main characteristics:

- A priority order, which defines the sequential order the VCS uses to analyze the rules or transforms

- A matching expression (pattern string) against which the dialed pattern is checked

- A replacement string, which is the expression used to derive the destination alias

Even though regular expressions allow for complex string manipulation, there are some very common simple applications. One of the most common string manipulations on VCS occurs by adding or stripping the domain part of an alias. An example of this is the following:

Alias: 88302

Search rule matching expression (using a regular expression): (\d+)

Search rule replacement string: \1@cisco.com

Following this simple rule, any dialed number arriving at the VCS will be translated into number@domain. In this case, 88302 will be translated into 88302@cisco.com.

Search rules have the following additional characteristics that can be useful when creating a dialing scheme:

- A target zone (mandatory). The target zone could be the Local Zone for VCS internal calls, or any other zone as a neighbor, traversal client or server, or DNS zone. It might include a policy server as well. The destination zone is selected based on the user's dialed pattern.

- A source zone (optional). Starting with Cisco VCS release 7.2, it is possible to apply a rule only to endpoints calling from a specific zone or subzone.

- A configurable behavior on a successful match of the search rule (mandatory).

On VCS, there is a difference between an alias matching a pattern and an alias that is found and that addresses a device able to answer the call.

If an alias is checked against a search rule matching expression, and the expression matches the alias, VCS will check if the alias exists in the target zone.

If the search rule matches the alias and the alias is found, the call is sent to the target zone.

If the search rule matches the alias but the alias is not found, this means that it does not exist in the target zone. In this case the behavior of VCS depends on what is configured for the **On Successful Match** field of the search rule. If this field is set to **stop**, the routing engine stops even if the alias is not found, and the call is sent to the destination zone. If the field is set to **continue**, the searching process goes on analyzing the remaining lower priority rules until the alias is found, until a rule matches the alias with the **On Successful Match** field set to **stop**, or until all the rules have been analyzed.

This behavior is useful when the administrator does not know where a specific alias is, as in the case of alphanumeric SIP URIs with the same domain registered on multiple call control platforms. As an example, there might be multiple VCSs inside the same company, sharing the same domain company.com. A call for user1@company.com cannot be routed properly if the destination VCS is not known; however, with the routing logic of VCS, it is possible to search for that alias in multiple VCSs or other call control systems and to send the call only after the alias is found.

Cisco VCS Routing Process

When Cisco VCS receives a call, it applies any configured pre-search transforms. After pre-search transforms, the call policy routing logic (CPL) applies. Such policies are configured using CPL scripts for advanced routing rules, and might include an external policy server. However, the vast majority of scenarios do not require the use of CPL.

If FindMe aliases are configured, the User Policies are then applied. The FindMe ID is resolved in one or more target aliases, and the call processing logic starts again in order to properly locate the target aliases.

VCS then tries to find a matching expression for the alias by querying the search rules in priority order. If the search rule returns a new destination (SIP URI or alias), the process starts again. This might happen if a call is sent to a DNS or ENUM services, or to a Policy Service.

If the alias is found in any of the zones (Local Zone, neighbor, or so forth) or if a routing destination is returned by the policy service, the VCS will attempt to place the call.

If a match is not found, the VCS will respond with a message to say that the call has failed.

In contrast with Unified CM where the routing logic is based on the longest match, on VCS the logic is priority-based. While changing the order of translation patterns or route patterns on Unified CM does not have any impact in the result of the routing algorithm, changing the rule priority on VCS will lead to different routing behaviors.

Recommended Design

This section provides design guidance and outlines how to implement an end-to-end enterprise dial plan.

Globalized Dial Plan Approach on Unified CM

This section describes dial plan features used to implement simplified call routing based on globalized numbers. The simplification is primarily obtained through the use of a single routing structure for off-net calls, no matter the source of the call. For example, two users in separate countries could use the same route patterns to carry calls to their respective local gateways, instead of requiring site-specific route patterns, each configured to match their respective dialing habits.

The main architectural approach used to attain this globalization can be summarized as follows:

- When a call enters the system, the destination number and the calling number are accepted in their local format but are then immediately globalized by the system.

- Once globalized, the called number is used to route the call to its destination through the use of route patterns expressed in the global form. The global form may be a combination of a global internal, enterprise-specific form such as 81001234 and/or a globalized PSTN representation of a DID number, such as the +E.164 form (for example, +12125551234).

- Once a destination has been identified, the calling and called numbers are localized to the form required by the endpoint, the network, or the system to which the call is to be delivered.

Thus, the guiding principle is:

Accept localized forms upon call ingress, and globalize them; route the call based on the globalized form; and localize the call to comply to the form required by the destination.

Cisco Unified Communications Manager (Unified CM) offers the following dial plan globalization capabilities:

- Local Route Group, page 14-54
- Support for + Dialing, page 14-54
- Calling Party Number Transformations, page 14-55
- Called Party Number Transformations, page 14-55
- Incoming Calling Party Settings (per Gateway), page 14-56
- Logical Partitioning, page 14-57

Together, these new features enable a Unified CM system to:

- Route calls based on the physical location context of the caller.
- Represent calling and called party numbers in a global form such as that described by the International Telecommunications Union's E.164 recommendation.
- Present calls to users in a format based on local dialing habits.
- Present calls to external networks (for example, the PSTN) in a manner compatible with the local requirements for calling party number, called party number, and their respective numbering types.
- Derive the global form of the calling party number on incoming calls from gateways, based on the calling number digits and the numbering type.
- Control the establishment of calls, as well as the initiation of mid-call features, between endpoints based on policies acting on each endpoint's geolocation, to comply with regulatory requirements in certain countries.

Local Route Group

Local route groups offer the ability to create patterns that route off-net calls to a gateway chosen for its proximity to the originating party. For example, a single pattern can be defined to route off-net, intra-country calls for all sites within a given country. Phones at every site can be configured to match this pattern, which then would route the call based on the local route group associated with the calling phone and based on the phone's device pool level setting for the respective local route group. This allows a phone in site 1 to route calls through the gateway at site 1, while a phone at site 2, still using the same pattern, would route calls through the gateway at site 2. This feature simplifies the configuration of site-specific routing of off-net calls.

Support for + Dialing

Telephone numbers can use the + sign to represent the international dialing access code needed to reach a destination from different countries. For example, +1 408 526 4000 is the international notation for Cisco's main corporate office in the United States. To call this number, an enterprise telephony user from France typically would have to dial 0 00 1 408 526 4000, whereas a caller from the United Kingdom

would have to dial 9 00 1 408 526 4000. In each case, + must be replaced with the appropriate off-net access code (as required by the enterprise telephony system) and international access code (as required by the PSTN carrier) relevant for each caller.

The system can route calls directly to destinations defined with +. For example, a user could program a WiFi phone's speed-dial entry for Cisco's main US office as +1 408 526 4000 and dial it directly when roaming in France, the UK, or anywhere else in the enterprise. In each location, the system would translate the destination number into the locally required digit string to allow the call to be routed properly.

Likewise, phone numbers dialed from a dual-mode phone are routable directly over the mobile carrier network when the phone is in GSM mode, or over the enterprise network when the phone is in WiFi mode, if the called number is represented in the +E.164 form. This allows a user to store a single destination number for a particular contact entry, and dial it no matter to which network the phone is currently attached.

This feature allows users to rely on the system to interpret phone numbers represented in the form described by the ITU E.164 recommendation and to route them properly without requiring the user to edit the number to adapt it manually to the local dialing habits.

Calling Party Number Transformations

The calling party number associated with a call routed through Unified CM might sometimes have to be adapted before it is presented to a phone or to the PSTN. For example, a call from +1 408 526 4000 might have to be presented as coming from 408 526 4000 if the destination phone is in the US or Canada, whereas a call from the same number might have to be presented to a destination phone in France as coming from 00 1 408 526 4000. This is mainly to offer users a presentation of the calling party in the customary form offered by their local PSTN, to maintain user familiarity with identification of the origin of calls ringing in.

Calls offered to gateways might require that the calling party number be manipulated to adapt it to the requirements of the telephony carrier to which the gateway is connected. For example, a call from +1 408 526 4000 offered to a gateway located in France might have to represent the calling number as 1 408 526 4000, with a Calling Party Number Type set to International. Similarly, a call from the same number offered to a gateway located in Canada might have to be represent the calling party number as 408 526 4000, with the Calling Party Number Type set to National.

This feature allows the calling party number to be adapted from the form used to route calls within the Unified CM system, to the form required by phone users or off-cluster networks.

> **Note** Some service providers might not be able to accept calling party numbers representing foreign telephone numbers, due to either technical limitations of their equipment, company policies, or governmental regulations. If calling party numbers cannot be accepted by the provider, the provider will either screen and overwrite the calling party number or reject the call. In some networks two calling party identities can exist for a call: user provided and network provided.

Called Party Number Transformations

The called number associated with a call routed through Unified CM might sometimes have to be adapted before it is presented to the PSTN. For example, a call placed to +1 408 526 4000 requires the called party number be transformed to 1 408 562 4000 with the numbering type set to National if it egresses to the PSTN through a gateway located in Canada. If the same call were re-routed toward a French gateway, the called party number would have to be transformed to 00 1 408 526 4000 with the numbering type set to International.

By manipulating the called party number as well as setting the numbering type for the called number, this feature allows the called party number to be adapted to the form required by off-cluster networks.

At the same time, incoming called party transformations allow the normalization of incoming called party information to a common globalized format before routing the call. Unified CM offers per-gateway settings for this feature, which allow different prefixes for each numbering type to be applied to calls entering different gateways. The settings can be configured on the gateway itself or on the gateway's device pool in order of precedence. A blank entry signifies that no digits will be prefixed; to inherit the settings from the lower-precedence setting, the entry must be set to **Default**. For more complex called party transformations, called party transformation calling search spaces per numbering type can be used. Because SIP does not support the concept of a typed number, for SIP the device pool settings for type Unknown are considered.

Incoming Calling Party Settings (per Gateway)

The calling party number associated with a call as it enters a gateway through a digital interface (for example, ISDN PRI) is also associated with an attribute identifying the calling number's numbering type as either Unknown, Subscriber, National, or International. When combined, the incoming call's calling number and its associated numbering type allow the system to determine the identity of the caller by stripping and prefixing appropriate digits to the incoming call's calling party number. Incoming Calling Party Settings allow the system to apply separate combinations of stripped and/or prefixed digits to the calling party number for each of the four calling number types.

For example, assume two calls come into a gateway located in Hamburg, Germany. Both feature a calling party number of 691234567. The first call is associated with a numbering type of Subscriber. This means the caller is located in Hamburg, thus the city code of Hamburg (40) is implied, as is the country code of Germany (49). Therefore, a full representation of the incoming call is +49 40 69 1234567, which can be obtained by prefixing +49 40 to the incoming call's calling party number for numbering type Subscriber.

The second call is associated with a numbering type of National. This means the caller is located in Germany, and the number already contains the applicable city code (69 is the city code of Frankfurt), but the country code of Germany (49) is implied. A full representation of the second incoming call is thus +49 69 1234567, which can be obtained by prefixing +49 to the second incoming call's calling party number for numbering type National.

Unified CM offers per-gateway settings for this feature, which allow different prefixes for each numbering type to be applied to calls entering different gateways. The settings can be configured on the gateway itself, on the gateway's device pool, or through the cluster-wide service parameters, in order of precedence. A blank entry signifies that no digits will be prefixed; to inherit the settings from the lower-precedence setting, the entry must be set to **Default**.

Due to the global significance of the settings at the service parameter level, Cisco highly recommends using the settings at the device pool level and allowing these settings to be shared for all gateways sharing the same device pool, or at the gateway level if only a single gateway exists that has to use the specific set of transformations. To avoid confusion, Cisco recommends always using only device-pool-level settings or device-level settings in any given installation and not mixing them (using device-level settings for some and device-pool-level settings for others).

For all calls within a given numbering type, the prefix and strip-digits operations are applied, with no consideration for the calling party number originally received.

Note   Calls coming from SIP trunks or from SIP gateways are all associated with calling party numbering type Unknown.

In particular, the SIP protocol as implemented on SIP gateways and SIP trunks effectively places the incoming calling party number of all calls in the numbering type Unknown. This prevents Unified CM from applying different calling party number modifications for different calling party number categories.

Unified CM allows the use of Incoming Calling Party Settings Calling Search Spaces (CSSs) for each number type. These CSSs are used to apply modifications to the calling party based on Calling Party Transformation Patterns. These patterns use regular expressions to match a subset of cases, followed by separate digit manipulation operations for each subset. This new capability enables Unified CM to apply different calling party number modifications for different calling party number categories. For example, a SIP trunk used to connect to the PSTN could present calls from local, national, and international parties with the numbering type set to Unknown; then each call's calling party number would be used to match a Calling Party Transformation Pattern in the trunk's CSS associated with number type Unknown, thus allowing Unified CM to apply different calling party number modifications for different calling party number categories.

Logical Partitioning

Some countries such as India have Telecom regulations requiring an enterprise's voice infrastructure to use the local PSTN exclusively when connecting calls outside the enterprise. This requires that the voice system be partitioned logically into two systems: one for Closed User Group (CUG) communications within the enterprise, and a second one to access the local PSTN. A call from an enterprise user in location A to another enterprise user in location B could be made within the CUG system; however, a call from an enterprise user in location A to a PSTN destination, no matter the location, must be made through local access to the PSTN in location A.

While existing dial plan tools can be used to prevent a call from completing if it were placed between endpoints outside the CUG, they are not able to prevent new call legs from being established while the call is in progress. For example, assume that an enterprise user in London, England, calls a co-worker in Delhi, India, over the enterprise network. Once the call is established, the user in Delhi conferences in a customer in India, from the same line on which the call from London was received. This mid-call addition (on the same line) of a destination outside the closed user group is not preventable solely by using the existing dial plan tools in Unified CM (such as Calling Search Spaces and Partitions). Unified CM 7.1 and later releases offer logical partitioning functionality, which allows the establishment and enforcement of policies that apply not only to the initial onset of calls, but also to mid-call features such as conference and transfer.

The combination of globalization features available in Unified CM allows the system to accept calls in the local format preferred by the originating users and carriers, to route the calls on-net using global representations of the called and calling numbers, and to deliver the calls to phones or gateways in the local format required by the destination user or network. These three aspects of the dial plan design approach can be summarized as:

- Localized Call Ingress, page 14-57
- Globalized Call Routing, page 14-59
- Localized Call Egress, page 14-60

Localized Call Ingress

Unified Communications systems with multiple sites located in different regions or countries must satisfy different dialing habits from users and different signaling requirements from the service providers to which gateways are connected. Each local case can be different; this requires that the system be able

to "translate" the local dialing habits and signaling requirements into a form that allows for the calls to be routed properly. Therefore, the systems must not only provide for many localized ingress requirements but also yield a single globalized form of any destination pattern.

Localized Call Ingress on Phones

Calls originating on endpoints such as phones or video terminals are typically dialed by users accustomed to a certain set of local dialing habits. Enterprise users in the US are used to dialing 9 1 408 526 4000 to reach Cisco's world headquarters in San Jose, California, whereas users in the UK would dial 9 00 1 408 526 4000 and users in France would dial 0 00 1 408 526 4000. Each of those three dialing forms features an enterprise off-net access code (9 for the US and UK, 0 for France), an international access code (00 for the UK and France, none needed for the US because the destination is intra-country), and a representation of the destination number, including the country code (1). Each of those three groups of users are dialing the same globalized destination number (+1 408 526 4000), but each with their own local dialing habits. In each of the three cases, + can be used as a global abstraction of the local dialing habits.

Unified CM's translation patterns are used to convert localized user input as dialed from phones, to the global form used to route the calls within the Unified Communications system. These patterns must allow all localized dialing habits to be recognized. For details on how these dialing normalizations based on translation patterns can be implemented, see the section on Call Routing in a Globalized Dial Plan, page 14-62.

Phones can also provide dialed strings in the global form of the dialed number. In the case of software endpoints such as Cisco Unified Personal Communicator, + dialing can be accommodated directly from the Telephony User Interface (TUI) of the phone or can be derived from click-to-dial actions taken by the user. On Type-B IP phones, dialing + from the keypad can be achieved by pressing and holding either the * or 0 key, depending on the phone model. Also, the missed and received calls directories can contain entries where the number includes a +. As the user dials from those directories, the resulting call into Unified CM will have a called number beginning with +.

Note   For definitions of Type-A and Type-B phones, see Dial Plan Elements, page 14-13.

The calling party number for calls originating from phones is set to the number configured as the directory number of the line from which the call originates. Following the concepts of a globalized dial plan design approach, the calling party information of all calls should be globalized. If the directory number format is not identical to the format chosen for the globalized internal calling party information (typically +E.164), then the correct handling of calling party information has to be achieved by properly globalizing the directory number by using the **Caller ID for Calls from this Phone** Calling Party Transformation CSS. This is the recommended way to globalize the calling party information of calls from phones to +E.164, because this method also is compatible with URI-dialed call flows for which calling party transformations in translation patterns are not applicable.

Localized Call Ingress on Gateways

The called and calling numbers delivered into the Unified Communications system by external networks (for example, the PSTN) are typically localized. The form of the numbers may vary, depending on the service provider's configuration of the trunk. As a gateway is connected to a PSTN trunk, the system administrator must work with the PSTN service provider to determine the applicable signaling rules to be used for this specific trunk. As calls are delivered into the system from the trunk, some of the information about the calling and called numbers will be provided explicitly and some of it will be implied. Using this information, the system must derive the calls' globalized calling and called party numbers.

The globalization of the called party number can be implemented through one of the following methods:

- In the gateway configuration, configure **Call Routing Information** > **Inbound Calls**, where the quantity of significant digits to be retained from the original called number and the prefix digits to be added to the resulting string are used to globalize the called number. The prefix digits should be used to add the applicable + sign and country, region, and city codes.

- Place translation patterns in partitions referenced by the gateway's calling search space. The translation patterns should be configured to match the called party number form used by the trunks connected to the gateway, and should translate it into the global form. The prefix digits should be used to add the applicable + sign and country, region, and city codes.

- Use the incoming call's called party transformation settings available on the gateway and on the gateway's device pool. There you can define strip and prefix digit instructions or alternatively configure a called party transformation calling search space per numbering type.

The globalization of the calling party number should be implemented by using the Incoming Calling Party Settings configured either on the gateway directly or in the device pool controlling the gateway.

Note   If the administrator sets the prefix to **Default**, this indicates call processing will use the prefix at the next level setting (device pool or service parameter). Otherwise, the value configured is used as the prefix unless the field is empty, in which case there is no prefix assigned.

For example, assume a call is placed to Cisco's US headquarters (+1 408 526 4000) from a US number, and the call is delivered to a gateway located in San Jose, California. The called number provided to the gateway is 526 4000. This information is sufficient for the Cisco Unified Communications system to derive the full destination number for the call. A call delivered by the service provider on this specific trunk group should inherit an implied country code and area code based on the characteristics of the trunk group connected to the gateway, which presumes that all destination DID numbers handled by the trunk group are from the North American Numbering Plan country code (1) and for area code 408. Therefore, the derived global form of the number is +1 408 526 4000. The calling number provided to the gateway is 555 1234, with the numbering type set to Subscriber. The numbering type allows the system to infer the country code and area code from the configured characteristics of the trunk group. Thus, the system knows that the calling number is +1 408 555 1234.

On a different call, if the calling number is 33158405858 with numbering type International, this is an indication that the global form of the calling number should represented as +33158405858.

Globalized Call Routing

For the destination to be represented in a global form common to all cases, we must adopt a global form of the destination number from which all local forms can be derived. The + sign is the mechanism used by the ITU's E.123 recommendation to represent any global E.164 PSTN number in a global, unique way. This form is sometimes referred to as a fully qualified PSTN number. In this document we refer to this notation as +E.164 (E.164 with leading + sign).

The system can be configured with route patterns that match globalized called numbers including the + sign. These same route patterns can point to route lists and route groups featuring the Standard Local Route Group. This allows for the creation of truly global route patterns because the egress gateway can be determined from the calling endpoint's device pool at the time of the call. All the necessary tasks of adapting the calls (both the calling and the called party numbers) to the local preferences and requirements are performed once a destination has been selected.

Localized Call Egress

When calls are routed to a destination using a global form of the called and the calling numbers, you might have to consider the following localization actions when the call is delivered to its destination.

Phone Calling Party Number Localization

As a call is delivered to a phone, the calling number will be in its global form, which might not be recognizable to the called party. Typically, users prefer to see calls from callers within their country presented with an abbreviated form of the caller's number.

For example, users in the US want to see incoming calls from US callers with a ten-digit national number, without the + sign or the country code (1). If a user whose global phone number is +1 408 555 1234 calls +1 408 526 4000, the called phone would like to receive 408 555 1234 as the calling party number while the phone is ringing. To achieve this, the system administrator should configure a Calling Party Transformation Pattern of: \+1.!, strip pre-dot. The Calling Party Transformation Pattern is placed in a partition included in the destination phone's Calling Party Transformation Pattern CSS, configured at the device-pool level. As a call from +1 408 555 1234 is offered to the phone, it matches the configured Calling Party Transformation Pattern, which removes the +1 and presents a calling party number of 408 555 1234 as the call rings in.

> **Note** The calling party number stored in the missed and received calls directories of Type-B phones to be used for call-backs is left in its globalized form to allow one-touch dialing from the directories without requiring manual editing of the directory's stored number string. The calling party number stored in the missed and received calls directories of Type-A phones is the transformed calling party number. For Type-A phones, the transformed calling party number needs to be in the form of a supported dialing habit to make sure the user can call back from the missed and received calls directory. This behavior permits implementation of globalized dial plans even with older Type-A phones present in the network.

> **Note** Many phone users are becoming accustomed to the globalized form of PSTN numbers, mainly due to the common use of mobile phones across international boundaries. The system administrator can forego the configuration of Calling Party Transformation Patterns for phones if displaying the global form of incoming numbers is preferred.

Gateway Calling Party Number Localization

As a call is delivered to a gateway, the calling party number must be adapted to the requirements of the PSTN service provider providing the trunk group to which the gateway is connected. Calling Party Number Transformation patterns can be used to change the calling party number digit string and numbering type. Typically, a calling party number featuring the gateway's country code should be changed to remove the + sign and the explicit country code, and they should be replaced with the national prefix. Also, the numbering type of the calling party number should be changed to National. If the gateway is connected to a trunk group featuring a specific area, region, or city code, the specific combination of + sign, country code, and local area code usually must be replaced by the applicable local prefix. Also, the numbering type must be adjusted to Subscriber.

For example, assume that a call from a San Francisco user (+1 415 555 1234) is routed through a route list featuring a San Francisco gateway as a first choice and a Chicago gateway as a second choice. The San Francisco gateway is configured with two Calling Party Transformation Patterns:

- \+1415.XXXXXXX, strip pre-dot, numbering type: subscriber
- \+1.!, strip pre-dot, numbering type: national

As the call is delivered to the San Francisco gateway, the calling party number matches both Calling Party Transformation Patterns. However, the first one is a more precise match and is selected to process the calling party number. Thus, the resulting transformed number is 5551234, with a calling party type set to Subscriber.

If the gateway had not been able to process the call (for example, if all ports were busy), the call would have been sent to the Chicago gateway to egress to the PSTN. The Chicago gateway is configured with the following two Calling Party Transformation Patterns:

- \+1708.XXXXXXX, strip pre-dot, numbering type: subscriber
- \+1.!, strip pre-dot, numbering type: national

As the call is delivered into the Chicago gateway, the calling party number matches only the second Calling Party Transformation Pattern. Therefore, the resulting calling party number offered to the gateway is 4155551234, with a calling party number type set to National.

Gateway Called Party Number Localization

As a call is delivered to a gateway, the called party number must be adapted to the requirements of the PSTN service provider providing the trunk group to which the gateway is connected. Called Party Number Transformation patterns can be used to change the called party number digit string and numbering type. Typically, a called party number featuring the gateway's country code should be changed to remove the + sign and the explicit country code, and they should be replaced with the national prefix. Also, the numbering type of the called party number should be changed to National. If the gateway is connected to a trunk group featuring a specific area, region, or city code, the specific combination of + sign, country code, and local area code usually must be replaced by the applicable local prefix. Also, the numbering type must be adjusted to Subscriber.

For example, assume that a call to a San Francisco user (+1 415 555 2222) is routed through a route list featuring a San Francisco gateway as a first choice and a Chicago gateway as a second choice. The San Francisco gateway is configured with two Called Party Transformation Patterns:

- \+1415.XXXXXXX, strip pre-dot, numbering type: subscriber
- \+1.!, strip pre-dot, numbering type: national

As the call is delivered to the San Francisco gateway, the called party number matches both of the Called Party Transformation Patterns. However, the first one is a more precise match and is selected to process the called party number. Thus, the resulting transformed number is 5552222, with a called party type set to Subscriber.

If the gateway had not been able to process the call (for example, if all ports were busy), the call would have been sent to the Chicago gateway to egress to the PSTN. The Chicago gateway is configured with the following two Called Party Transformation Patterns:

- \+1708.XXXXXXX, strip pre-dot, numbering type: subscriber
- \+1.!, strip pre-dot, numbering type: national

As the call is delivered into the Chicago gateway, the called party number matches only the second Called Party Transformation Pattern. Therefore, the resulting called party number offered to the gateway is 4155552222, with a called party number type set to National.

> **Note**   When a call egresses to a gateway, the calling and called party transformation patterns are applied to the calling and called numbers respectively.

> **Note**   SIP does not offer an indication of the numbering type. Therefore, SIP gateways are not able to receive an indication of the called or calling party number type set by Unified CM.

Call Routing in a Globalized Dial Plan

The system must be configured to recognize user input and then route and deliver the call to the proper destination. Because the call can originate in many different forms, the system must provide pattern recognition to match each of those forms.

Core routing in the globalized dial plan approach is based on routing +E.164 patterns so that the native dialing habit for this dial plan approach is global +E.164 dialing.

Unified CM's translation patterns are used to convert localized user input as dialed from phones, to the global +E.164 form used to route the calls within the Unified Communications system.

The calling search spaces configured for each site should generally at least allow for:

* Localized intra-site dialing habits of the site
* Localized off-net dialing habits of the users at the site
* Applicable local telephony services such as emergency calls, directory, and operator services
* The globalized form of on-net and off-net numbers

Figure 14-26 shows how to support dialing in the globalized form using local habitual dialing for an example site in the US.

Figure 14-26   Localized and Globalized Dialing
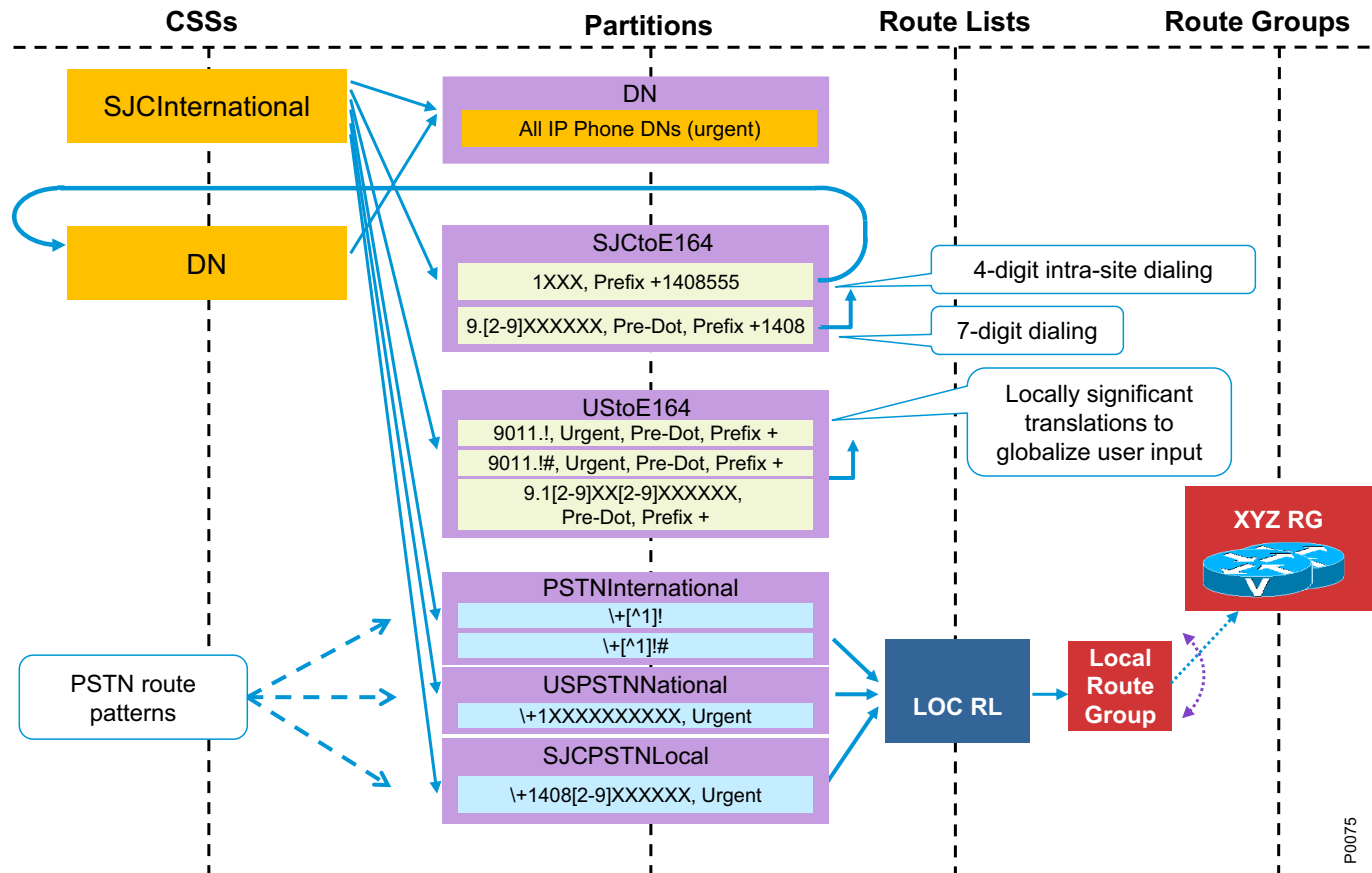
In Figure 14-26, a US IP phone user dials 9011496100773, connects to the destination in Germany, and then releases the call. The called party in Germany calls the US user back, connects, and then releases the call. The US user then goes into the Received calls directory, selects the entry for the last received call (+49 6100 773), and presses Dial.

In this example, the US user initiates two separate calls to the same destination (+496100773). For the first call, the form of the destination number localized for US dialing habits is used, and the corresponding translation pattern 9011.! is matched by the user's input. Once translated, the same calling search space is used for the secondary lookup (**Use Originator's Calling Search Space** set on the translation pattern) and the route pattern \+[^1]! is used to route the call. For the second call, the globalized form of the destination number is used and the route pattern \+[^1]! is used directly.

Comparing these call flows clearly shows the two-step routing process implemented in this dial plan approach: first normalize all dialing habits to +E.164 and then route based on +E.164 patterns. The effective PSTN access level is defined by the PSTN route patterns addressed by the calling search space. More granular access levels can be implemented by adding more specific route patterns.

All directory numbers in partition DN are configured as urgent DNs to avoid potential inter-digit timeout if an on-net destination is called, and the dialed on-net destination overlaps with the variable length off-net route pattern in partition PSTNInternational.

The first translation in partition SJCtoE164 implements 4-digit intra-site dialing, assuming that all local DIDs of the site are in the range +1 408 555 1XXX. Local dialing (9+7) for the site in San Jose is implemented by the second translation pattern in the same partition by again transforming the local habitual dialing to +E.164. The same is true for partition UStoE164, which implements the globalization of US habitual PSTN dialing to international and national destinations.

All dialing normalization translation patterns have **Use Originator's Calling Search Space** set (CSS Inheritance) so that the calling search space used for the secondary lookup, after applying the called party transformations defined in the translation pattern, is identical to the activating calling search space.

The single calling search space creating the requested class of service can be used as a line or device calling search space. In deployments that support mobility features such as extension mobility or device mobility, the line calling search space has to be used to enable the user to keep his class of service when roaming.

A user with extension +1 408 555 1234 can now be reached from other users using the calling search space in the example by dialing:

- 1234 — Translation pattern in partition SJCtoE164 transforms dialed digits to +14085551234, and then there is a match on the directory number in partition DN.

- 95551234 — Translation pattern in partition SJCtoE164 globalizes the dialed digits, and then the directory number in partition DN is matched.

- 914085551234 — Translation pattern in partition UStoE164 globalizes the dialed digits, and then the directory number in partition DN is matched.

- +14085551234 — Direct match on the directory number in partition DN.

Other Classes of Service

All translation patterns creating the normalization of dialing habits to +E.164 for class of service "international" in Figure 14-26 use CSS inheritance so that the activating CSS is also used for the secondary lookup after the called party transformations (globalizing to +E.164) are applied. This permits the reuse of the same dialing normalization translation patterns for other classes of service.

Figure 14-27 shows how class of service "national" can be defined based on the same schema used for class of service "international." Comparing this schema to class of service "international" in Figure 14-26, we see that all partitions containing the dialing normalization and PSTN route patterns can be reused. Effectively the only difference is that calling search space SJCNational does not have access to the international PSTN route patterns in partition PSTNInternational.

Figure 14-27   Sharing Dialing Normalization Between Classes of Service
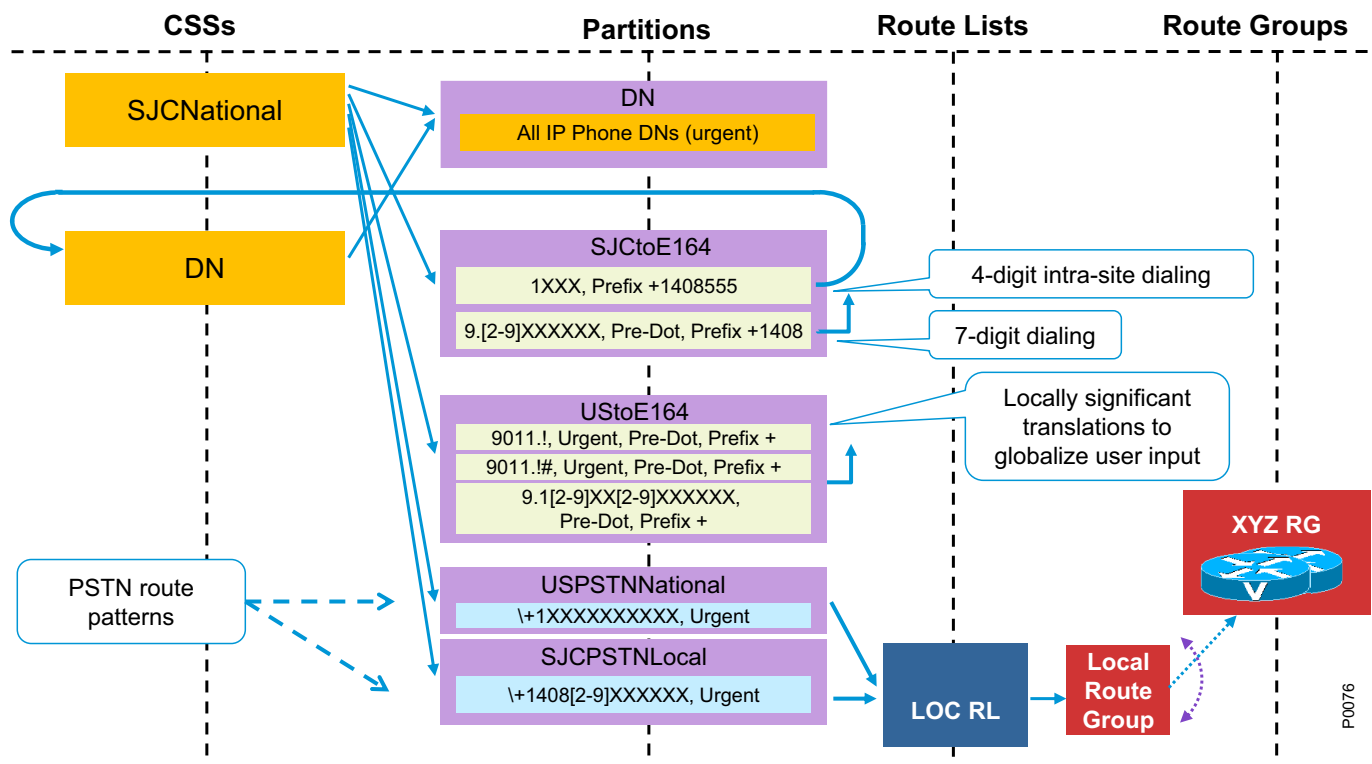
Having access to dialing normalization patterns for the local habitual international dialing 9011 is required even for class of service "national" because we need to support international dialing to international on-net destinations (directory numbers in partition DN outside the US).

More restrictive classes of service such as "local" and "internal" are built following the same schema of simply removing access to the partitions holding the inappropriate PSTN route patterns.

The naming convention used for partitions and calling search spaces in the preceding illustrations helps to identify which pieces of the dial plan need to be replicated to support multiple classes of service, sites, and dialing domains. If the name includes the specification of a site (for example, SJC in partition name SJCtoE164), then that element needs to be replicated for every site. If the name includes the specification of a class of service (for example, International in SJCInternational), then that element needs to be

replicated for every class of service. If the name does not include the specification of a site (for example, partition USPSTNNational), then it can be reused for all sites sharing the same dialing habit (in this case all sites in the US).

Calling Unassigned DNs

Four-digit dialing normalization translation pattern 1XXX in partition SJCtoE164 does not use CSS inheritance. Instead, this translation pattern uses calling search space DN for the secondary lookup. This is to make sure that if a user dials 1234 and directory number \+14085551234 does not exist, then the call is rejected with cause "unassigned number." If pattern 1XXX used CSS inheritance, the call would instead be routed to the PSTN after matching the route pattern in partition USPSTNNational. Ultimately this would lead to the same result because the PSTN would either reject the call immediately or route it to the enterprise's PSTN gateway, where it would be seen as an inbound call and then rejected because the called directory number does not exist. Keep in mind that the inbound calling search space on any gateway typically should have access to internal destinations only and not PSTN destinations, to break routing loops and to avoid toll fraud.

The same PSTN hairpinning problem with calls to unassigned DNs also exists for the other dialing habits implemented by the dialing normalization translation patterns using CSS inheritance and also for +E.164 dialing. For these dialing habits, using the DN calling search space to loop back to the DN partition is not an option because on-net destinations are only a subset of destinations reachable through these dialing habits.

If this hairpinning needs to be avoided, the schema in Figure 14-28 can be used. Here partition E164OnNet holds urgent translation patterns matching the +E.164 prefixes of all on-net destinations. For a site with DID range +1 408 555 1XXX, an urgent translation pattern \+14085551XXX would exist in E164OnNet. These on-net intercept patterns then point back to a DN calling search space that ultimately provides access to the provisioned DNs. All dialing normalization patterns (including the dialing normalization pattern for abbreviated intra-site dialing) use CSS inheritance. A call to an unassigned DN now is not routed to the PSTN because the call is intercepted by the on-net pattern. If the dialed DN then does not exist in the DN partition, the call is rejected with cause "unallocated number."

Figure 14-28   Avoid PSTN Hairpinning for Unassigned DNs and Support for Non-+E.164 DNs
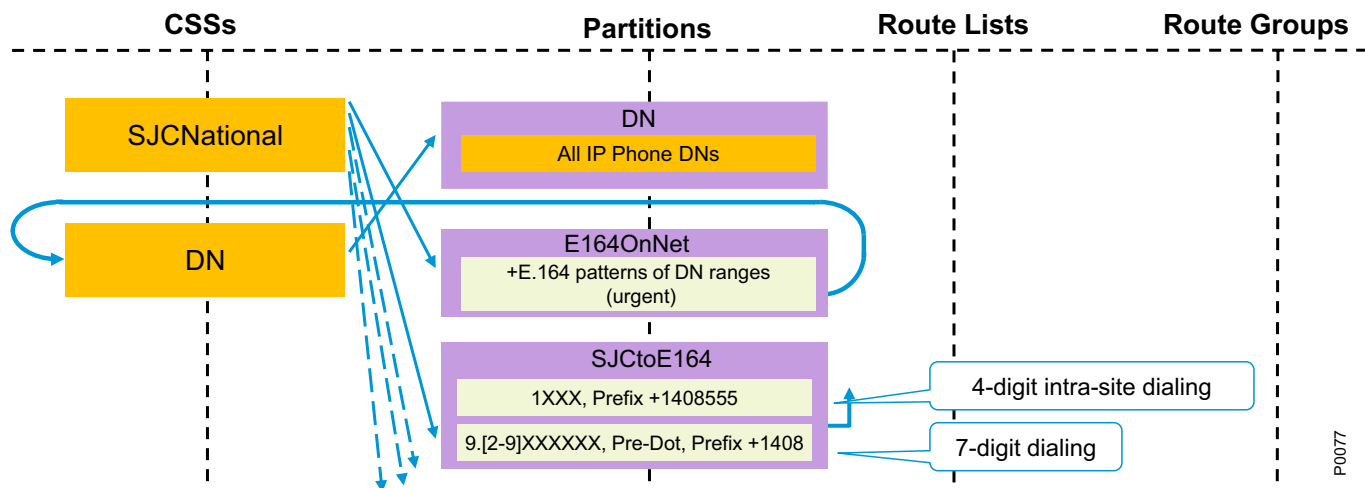
Another potential purpose of the intercept patterns in E164OnNet is to map from +E.164 to the format of the directory numbers. For example, if the directory numbers are configured as E.164 (without the plus) for a site with DID range +1 408 555 1XXX, a translation pattern \+.14085551XXX with called party transformation "strip pre-dot" (removing the +) would need to be configured in E164OnNet.

Although it is highly recommended to configure directory numbers as +E.164, in some cases the directory numbers might be configured in a different globalized format such as E.164 (without the +), an abbreviated enterprise numbering scheme, or 10 digits in the US. Not configuring directory numbers as +E.164 requires additional number normalization to be configured for globalized caller IDs. Also, some CTI applications (for example, attendant console applications) might require additional number normalization if configured directory numbers do not match the format of numbers stored in global directories.

If +E.164 DNs are used and the rare hairpinning of on-net calls to unassigned DNs is not considered critical, the effort to maintain the list of on-net DN ranges in partition E.164OnNet should be avoided and the simplified dial plan approach shown in Figure 14-26 and Figure 14-27 should be deployed.

Emergency Calls

Access to emergency services has to be granted to all users. This can be achieved either by adding the partition with the emergency number route patterns to each calling search space or by enabling access to the emergency number route patterns through the device-level calling search space. If access to emergency numbers is granted through the device calling search space, then in roaming scenarios (for example, extension mobility) the user has to dial emergency services using the habitual dialing of the visited site, while access to emergency numbers through the line calling search space would allow the user to dial emergency services using the habitual dialing of the home site. This differentiation obviously is important only if the habitual dialing of emergency services differs between home and visiting sites as, for example, in the case of a European user (emergency number 112) logging into an US phone (emergency number 911).

Typically the recommend method is to provide emergency calling services via the emergency number local to the physical location of the calling device. Although this might create overlap between the emergency number and other dialing habits (for example, between 911 and four-digit intra-site dialing starting with 9 for a non-US user from a site with 9XXX abbreviated dialing who logs into a phone in the US), this at least guarantees that any phone in a given location at any time is allowed to place emergency calls using the local habitual emergency dialing independent of whether a remote user from a region with a different emergency number is logged in or not.

To implement this behavior, the emergency patterns needs to be addressed by the device calling search space.

Benefits of the Design Approach

The benefits of the dial plan design approach enabled by the new globalization features include:

- Simplified configuration of call routing, especially when considering local egress to the PSTN
- Simplified configuration and enhanced functionality of system functions such as:
  - Automated Alternate Routing (AAR)
  - Emergency Responder site-specific failover
  - Call Forward Unregistered (CFUR)
  - Tail End Hop Off (TEHO)
  - Click-to-dial of E.164 numbers from soft clients such as Cisco Jabber

- Adaptive call routing for speed dials originating from roaming extension mobility users or roaming devices

- One-touch dialing from phone directory entries, including dual-mode phones

- One-touch dialing from missed and received call lists in IP phone directories

Automated Alternate Routing

If the automated alternate routing (AAR) destination mask is entered in the globalized form, and if every AAR CSS is able to route calls to destinations in the globalized form, then the system administrator can forego the configuration of AAR groups because their sole function is to determine what digits to prefix based on the local requirements of the calling phone's PSTN access to reach the specific destination. A single AAR group with no prefix digits configured can be used for all provisioned devices.

Note   The AAR mask or the external phone number mask must be configured in the globalized form on the called destinations to enable AAR, even if the called directory number might already be configured in the globalized form. AAR will be activated only if either the AAR mask or the external phone mask is configured.

Furthermore, in most cases the sole function of the AAR CSS is to route the call to the calling phone's co-located gateway; therefore, it can be configured with only a single route pattern (\+!) pointing to a route list that contains the Standard Local Route Group. Because calls routed by this single route pattern will always be routed through the Local Route Group associated with the calling endpoint, that unique AAR CSS can be used by all phones at all sites, no matter in which region or country they are located.

Cisco Emergency Responder

Call routing to Cisco Emergency Responder is typically implemented by configuring a 911 CTI route point to connect to the primary Emergency Responder server and a 912 CTI route point to connect to the backup Emergency Responder server.

If both Emergency Responder servers are unavailable, 911 calls can be directed to the PSTN egress gateway co-located with the calling phone by configuring:

- The 911 CTI route point to Call Forward No Answer (CFNA) and Call Forward Busy (CFB) to 912, through a calling search space that contains the partition of the 912 CTI route point

- The 912 CTI route point to CFNA and CFB to 911, through a calling search space that contains a global partition, itself containing a route pattern 911 pointing to a route list that contains the Standard Local Route Group

If both CTI route points become unregistered, calls to 911 will be forwarded through the local route group as determined by the calling phone's device pool. If Device Mobility is configured, roaming phones will be associated with the visited site's device pool, and thus associated with the visited site's Local Route Group.

Call Forward Unregistered (CFUR)

To allow calls handled by the Call Forward Unregistered function to use a gateway co-located with the calling phone, configure the CFUR destination of phones using the globalized + form of their PSTN number. The CFUR CSS can be configured with only a single route pattern (\+!) pointing to a route list that contains the Standard Local Route Group. Because calls routed by this single route pattern will always be routed through the Local Route Group associated with the calling endpoint, the same CSS can be used as the CFUR CSS by all phones at all sites, no matter in which region or country they are located.

Tail End Hop Off (TEHO)

To reduce PSTN connectivity charges, system administrators might want to route calls to off-net destinations by using the IP network to bring the egress point to the PSTN as close as possible to the called number. At the same time, if the call's preferred TEHO route is not available, it might be necessary to use the calling phone's local gateway to send the call to the PSTN. This can be achieved by allowing all phones partaking in TEHO routing for a given type of number to match the same route pattern that matches the specific destination number and that points to a route list containing the TEHO egress gateway-of-choice as the first entry and the Standard Local Route Group as the second entry.

Dial Plan with Global Dial Plan Replication (GDPR)

+E.164 alternate numbers and enterprise alternate numbers are defined on a directory number using a mask, and they can be inserted into local digit analysis and advertised to remote call controls. Insertion into local digit analysis and advertising to remote call controls are options that can be enabled independently. A +E.164 or enterprise alternate number needs to be defined only if the number needs to be inserted into local digit analysis, advertised to a remote call control, or used as a PSTN failover number on remote call controls.

Inserting enterprise or +E.164 alternate numbers into local digit analysis effectively creates alternatives to dialing the directory number. For a directory number \+14085551234 in site SJC we could define an enterprise alternate number in partition SJCToE164 using mask 1XXX. This would create a local pattern 1234 in this partition. Using the same enterprise alternate number scheme for all DNs in site SJC would effectively allow removal of the four digit intra-site dialing translation pattern 1XXX shown in Figure 14-26 and Figure 14-27. This schema can be extended to multiple sites because the enterprise alternate numbers that have only local site significance are put into site-specific partitions so that ambiguities are avoided (for example, see Table 14-4).

Table 14-4   Local Site Enterprise Alternate Numbers

Site	DID Range	Enterprise Alternate Number Mask	Enterprise Alternate Number Partition
SJC	+14085551XXX	1XXX	SJCToE164
RTP	+19195552XXX	2XXX	RTPToE164
NYC	+12125551XXX	1XXX	NYCToE164

Using the settings shown in Table 14-4 for directory numbers +14085551234 and +12215551234, the exact same enterprise alternate number 1234 would be created, but both are in different partitions so that the site specificity is preserved.

Although the schema shown in Table 14-4 demonstrates how GDPR enterprise alternate numbers added to local digit analysis can be used to implement abbreviated intra-site dialing without adding dialing normalization translation patterns for this dialing habit, enterprise alternate numbers with only local site significance should never be advertised across GDPR. On the receiving cluster, overlapping (and possibly even identical) enterprise alternate numbers would need to be learned, which causes routing ambiguities.

Note   Cisco highly recommends advertising only enterprise alternate numbers with global significance over GDPR. Typically these enterprise alternate numbers follow an enterprise abbreviated on-net numbering plan.

Table 14-5 shows a potential enterprise alternate number schema based on an enterprise abbreviated on-net numbering plan using 8 as the access code and two-digit site numbers.

Table 14-5   Global Enterprise Alternate Numbers

Site	DID Range	Enterprise Alternate Number Mask	Enterprise Alternate Number Partition
SJC	+14085551XXX	8011XXX	DN
RTP	+19195552XXX	8022XXX	DN
NYC	+12125551XXX	8031XXX	DN

These enterprise alternate numbers now have global significance and thus can simply be added into the DN partition implementing the abbreviated inter-site dialing habit for all local directory numbers. The traditional approach to implement the equivalent abbreviated inter-site on-net dialing habit based on dialing normalization translation patterns is shown in Figure 14-29.

Figure 14-29   Abbreviated Intra-Site On-Net Dialing Normalization Translation Patterns
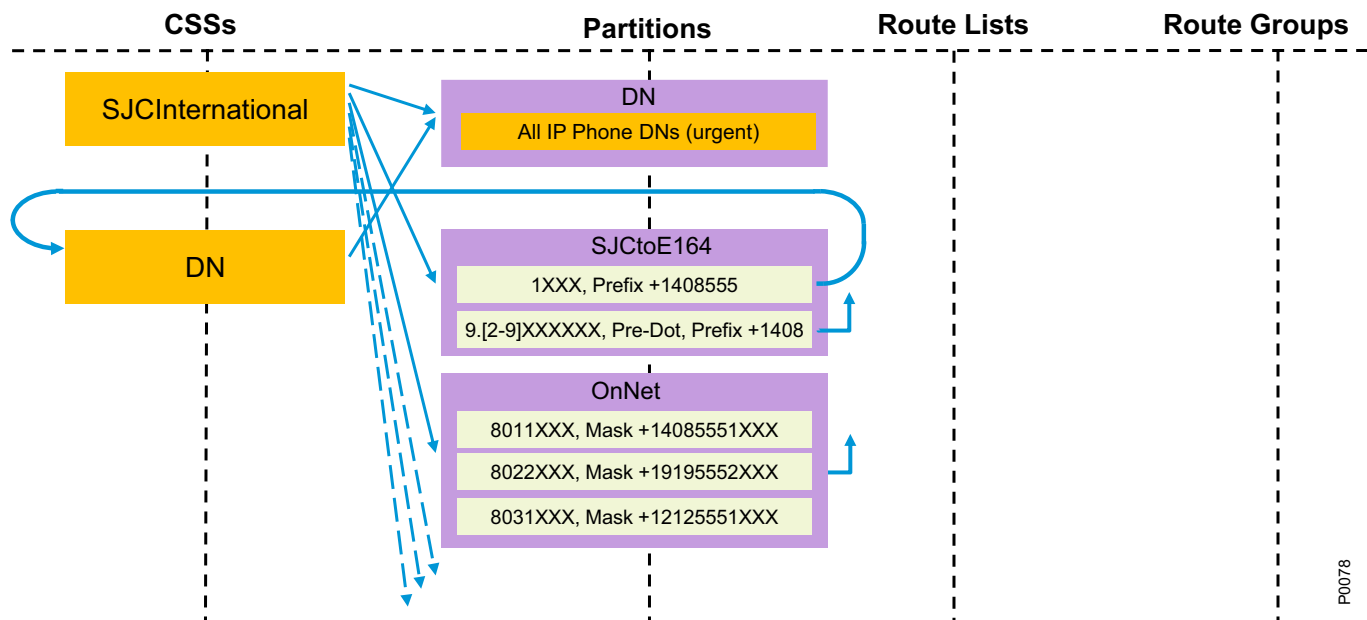
Both schemes (adding enterprise alternate numbers to local digit analysis or using dialing normalization) implement equivalent user experiences. The only difference again is that with dialing normalization patterns, calls to unassigned numbers dialed using this overlay dialing habit are routed to the PSTN and then are hairpinned back. On the other hand, adding explicit enterprise alternate numbers for each directory number to local digit analysis enlarges the local dial plan significantly, which might add complexity to troubleshooting the local dial plan.

Similar to enterprise alternate numbers, +E.164 alternate numbers are also defined by masking the directory number. To define a +E.164 alternate number for a +E.164 DN, the mask simply can be left empty. A +E.164 alternate number of a +E.164 DN should obviously not be added to the local dial plan, but it is still required to be able to advertise the +E.164 alternate number or a +E.164 PSTN failover number to remote call controls.

Using dialing normalization translation patterns to implement abbreviated on-net dialing habits, instead of defining enterprise alternate numbers for each directory number, reduces the complexity of digit analysis because fewer patterns are actually added into the digit analysis. To the same extent, advertising +E.164 and enterprise alternate patterns instead of individual alternate numbers per directory, minimizes the number of advertised dial plan elements and thereby reduces the complexity of dial plans of remote call controls that import the advertised information from GDPR. Advertising only summaries in the form of +E.164 and enterprise patterns is highly recommended.

Call controls that learn dial plan information from GDPR can put the learned information into different partitions based on the type: +E.164 alternate number, enterprise alternate number, +E.164 pattern, and enterprise pattern. If this type-based differentiation is not required to implement the required classes of service, then all numeric dial plan information learned from GDPR can be put into a single partition (such as the OnNet partition in Figure 14-29) that then is added to all calling search spaces implementing classes of service with access to remote on-net destinations.

Differentiated class of service can also be achieved based on limiting access to the SIP route patterns creating the routing schema for the location information in the form of SIP route strings advertised over GDPR. This allows for limiting the reachability of destinations advertised by certain call controls or as part of certain imported GDPR catalogs based on the reachability of the advertised SIP route strings.

Integrating Unified Communications Manager and TelePresence Video Communication Server

Cisco Unified Communications Manager (Unified CM) supports codec registration and alphanumeric URI dialing for the Cisco TelePresence System C Series, EX Series, Profile Series, and SX Series. In this scenario, the Cisco TelePresence Video Communication Server (VCS) can perform two main functions:

- H.323-to-SIP interoperability for video and content
- Business-to-business (B2B) access using VCS Control and VCS Expressway

H.323 legacy endpoints can be registered to the VCS, which will perform protocol conversion and content interoperability between H.323/H.239 and SIP Binary Flow Control Protocol (BFCP). Note that VCS behaves as a signaling and media gateway in this scenario, and as such it has to handle the media too, therefore the Interworking feature has to be turned on.

H.323 endpoints connected to the VCS share the same numbering plan used by Unified CM.

Alias manipulation and normalization is done on VCS using the standards-based Portable Operating System Interface for Unix (POSIX) format for regular expression syntax. POSIX is a collection of standards that define some of the matching and replacement functionality that an operating system (UNIX) should support.

Figure 14-30 shows an example topology for interconnecting Cisco VSC and Unified CM to enable end-to-end communications between voice and video endpoints registered with Unified CM and VCS and also communications peers outside the enterprise via VCS Expressway.

Figure 14-30   Sample Topology for Interconnecting Cisco VCS and Unified CM
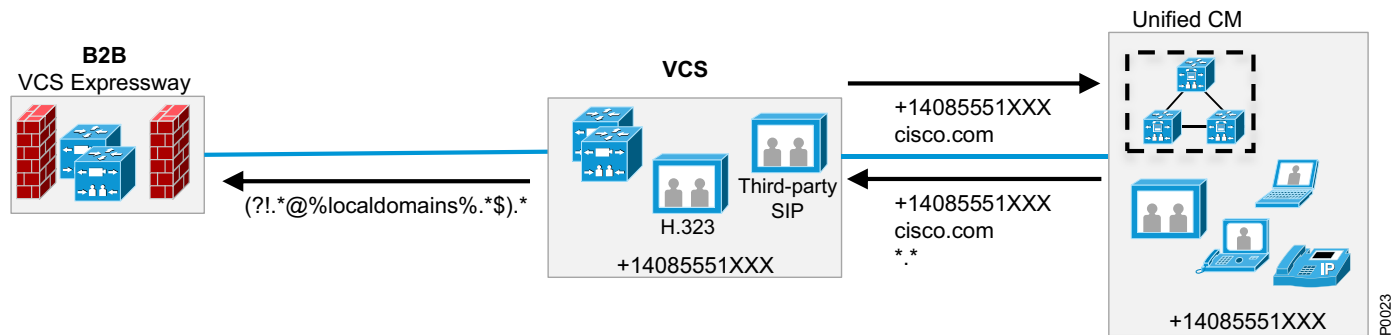
+E.164 Numbering Plan

To allow for globalized call routing between Unified CM and VCS, a globalized dial plan as described in the section on Globalized Dial Plan Approach on Unified CM, page 14-53, should be implemented on Unified CM and +E.164 addresses need to be provisioned on VCS. Also, the H.323 ID of each endpoint registered with VCS has to be configured with the +E164 number and registered to the Local Zone.

Alias Normalization and Manipulation

Alias normalization has the purpose of presenting the correct alias when dialing an endpoint. Alias normalization might occur at system level or at zone level.

An example of normalization at system level occurs when implementing dial plan transparency with a mixed environment of H.323 and SIP endpoints registered to VCS. H.323 endpoints register the H.323 ID and E.164 alias on the Local Zone of the VCS. However, if a SIP endpoint dials an E.164 alias, it will automatically append the domain, even if the user has just dialed the E.164 number. Regardless of whether the E.164 number is local or remote on another VCS, a normalization rule would strip the domain before forwarding the call. This can be done using a transform.

An example of normalization at zone level occurs when connecting VCS to a Unified CM cluster. In this case Unified CM might use an alias format that does not match the registered endpoint alias. Since this happens only with calls received from Unified CM, a search rule can be applied to normalize the alias before forwarding to the destination.

After normalization, manipulation might also occur. Manipulation after normalization might occur when the call is sent to a non-VCS system that does not support the alias format of VCS.

The following example considers a Unified CM cluster connected to a VCS cluster, where the VCS cluster is used for H.323 endpoint connectivity and B2B connection (see Figure 14-30).

In this case there is no need for alias normalization. All endpoints are reachable through their H.323 ID, which is equal to the +E164 alias. However, calls sent to and received from Unified CM need manipulation before routing them to the final destination.

When a H.323 endpoint calls another H.323 endpoint registered to VCS, it uses the +E.164 number that has been set equal to the H.323 ID (+14085551001 in Figure 14-30), and the call is properly placed.

However when the call is sent to Unified CM, SIP-to-H.323 interworking takes place, and as a consequence a search rule which adds the domain is needed. Assuming that +E.164 numbers from the range +14085551XXX are used on the local VCS, the search rule in Example 14-5 would be required.

Example 14-5   Search Rule for Local +E.164 Destinations on VCS

```
Search Rule "To VCS"
Description: To Local +E164
Priority: 50
mode: alias pattern match
pattern type: regex
pattern string: (\+14085551\d{3})(@.*)
pattern behavior: replace string: \1
On successful Match: Stop
Target: Local Zone
```

Each H.323 client registered to the VCS dialing the internal range would match this rule.

If a +E.164 call comes into VCS from Unified CM, the address dialed would be in any of the following forms:

- +14085551XXX@10.10.10.10:5060 (@ followed by the IP address of the VCS and port number 5060 or 5061 if the trunk configuration on Unified CM uses the IP address of VCS as a peer)

- +14085551XXX@vcs1.cisco.com:5060 (@ followed by the DNS name of VCS and port number 5060 or 5061 if the trunk configuration on Unified CM uses the DNS name of VCS)

- +14085551XXX@cisco.com:5060 (@ followed by the domain and port number 5060 or 5061 if the trunk configuration on Unified CM uses a domain name and a DNS SRV record)

The recommended way to configure the trunk from Unified CM to VCS is to use IP addresses on Unified CM to define VCS as a peer.

The pattern string (\+14085551\d{3})(@.*) in Example 14-5 matches all three of the above formats, and the defined replacement string strips the right-hand side of the received SIP URI to make sure that the received +E.164 address can successfully be matched against the H.323 IDs configured on VCS.

It is possible to use a more stringent pattern matching if a better pattern selection is needed. For example, ([^@]*)@(%ip%|[^@]*cisco.com(.*)). This pattern would match all URIs starting with a sequence of characters that do not include the @, followed by the @ and the IP address of any of the VCS peers in the VCS cluster, or anything that includes "cisco.com" and the port number.

If some SIP endpoints are also registered to VCS, they will automatically add the domain. The search rules above strip the domain even in this case.

For numeric +E.164 calls routed from VCS to Unified CM, a domain has to be added to the SIP URI in the outgoing request because H.323 endpoints do not automatically add a domain. A search rule has to be created in order to add a domain for calls sent to Unified CM, as illustrated in Example 14-6.

Example 14-6   Search Rule "To UCM"

```
Search Rule "To UCM"
Description: To UCM +E164
Priority: 100
mode: alias pattern match
pattern type: regex
pattern string: (\+14085551\d{3})(.*)
pattern behavior: replace string: \1@cisco.com
On successful Match: Stop
Target: UCM Zone
```

The search rule in Example 14-6 makes sure that all numeric dialing from VCS matching \+14085551XXX but not matched by any local client is sent to Unified CM and that the host portion of the SIP URI sent to Unified CM is set to "cisco.com". According to the SIP routing mechanisms of Unified CM as documented in the section on Routing of SIP Requests in Unified CM, page 14-47, and

Cisco Collaboration Systems 10.x SRND

especially Figure 14-25, the organization top level domain (OTLD) on Unified CM has to be set to "cisco.com" so that Unified CM routes these numeric SIP URIs according to the numeric +E.164 dial plan configured on Unified CM. This rule is also matched by SIP endpoints registered to VCS, if there are any.

To enable B2B connectivity, VCS has to route all B2B calls identified by having a non-local SIP URI host portion to VCS Expressway in the B2B building block. The search rule in Example 14-7 accomplishes this by matching everything that has a domain other than cisco.com and sending it to the VCS Expressway and to the Internet.

Example 14-7   B2B Search Rule

```
Search Rule "External"
Description: for B2B
Priority: 110
mode: alias pattern match
pattern type: regex
pattern string: [^@]*@[^@]*(?<!cisco.com)
pattern behavior: leave
On successful Match: Stop
Target: VCS-E
```

On Unified CM the +E.164 prefix hosted on VCS has to be added by adding a specific +E.164 route pattern to the Unified CM dial plan and making sure that this route pattern addresses the trunk to VCS by means of an appropriate route list and route group configuration.

If endpoints registered to VCS share the same DN range than the endpoints registered to Unified CM, then the dial plan configuration on Unified CM has to ensure that all +E.164 numbers from the local prefix that are unknown on Unified CM are routed to VCS. Figure 14-31 shows how this can be achieved with a globalized dial plan approach.

Figure 14-31   Intercepting Unassigned Directory Numbers.
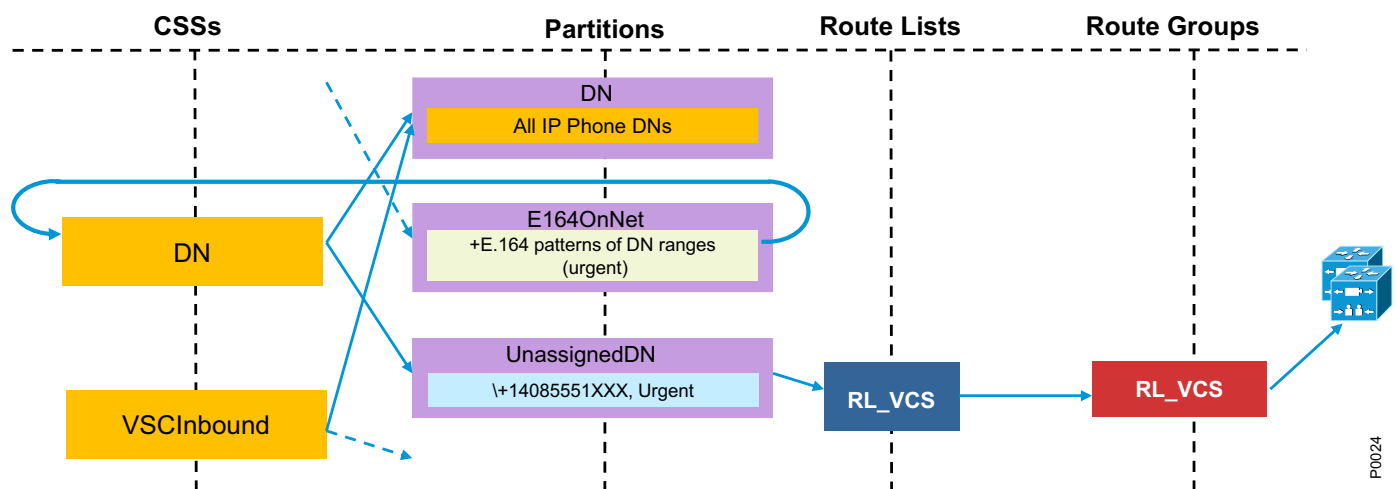
The globalized dial plan in Figure 14-31 uses the approach as discussed in the section on Globalized Dial Plan Approach on Unified CM, page 14-53. Simply put, the DN calling search space referenced by all dialing normalization translation patterns and the urgent translation patterns matching on the known on-net +E.164 prefixes, has to be extended to include a route pattern matching on the +E.164 prefix that

is shared with VCS. All +E.164 patterns from this range not matched by directory numbers on Unified CM will be matched by this route pattern and sent to VCS. To make sure that no routing loop is created, the inbound calling search space of the trunk coming from VCS should not have access to this route pattern pointing back.

Also, the dial plan on Unified CM has to make sure that all calls dialed as a URI (non-numeric) that do not address a directory URI local to Unified CM, are routed to VCS. The easiest way to achieve this is to add a "catch-all" SIP route pattern (for example, *.*) on Unified CM that also addresses the trunk to VCS through an appropriate route list and route group configuration. Again, to make sure that routing loops are avoided, the inbound calling search space of the trunk coming from VCS should not have access to this "catch-all" SIP route pattern.

Implementing Endpoint SIP URIs

If endpoints on Unified CM can be reached using SIP URIs and +E164 numbers, another search rule can be added to route them properly from VCS to Unified CM, as shown in Example 14-8.

Example 14-8   Search Rule for URI Dialing from VCS to Unified CM

```
Search Rule "URI To UCM"
Description: SIP URI to UCM
Priority: 100
mode: alias pattern match
pattern type: suffix
pattern string: cisco.com
pattern behavior: leave
On successful Match: Stop
Target: UCM Zone
```

If the H.323 endpoints are also addressed using alphanumeric aliases of the same form of a SIP URI instead of using +E.164 aliases, the "To VCS" search rule in Example 14-5 can be replaced by the one in Example 14-9.

Example 14-9   Modified Search Rule "To VCS" Supporting URI Dialing of H.323 Registered Endpoints

```
Search Rule "To VCS"
Description: To Local H.323 aliases
Priority: 50
mode: alias pattern match
pattern type: suffix
pattern string: cisco.com
pattern behavior: leave
On successful Match: Continue
Target: Local Zone
```

"Continue" has to be enabled because, if the alias is not found in the Local Zone, this means that the alias is not local and it will be sent to Unified CM following the next rule of priority 100 ("To CUCM"). However, if the call comes from Unified CM, it will not be sent back to the CUCM zone where the call came from, thus prohibiting routing loops.

On Unified CM a SIP route pattern has to be created to match on "cisco.com" pointing to the same route list used for +E.164 routing to VCS.

If a user on Unified CM dials alice@cisco.com, Unified CM will first match this URI against the locally configured SIP URIs and then as a fallback will match the host portion (cisco.com) against the configured SIP route patterns so that the above SIP route pattern is matched and the call is routed to VCS. If the URI is known on VCS, the call is routed to the endpoint, but the call will not be sent back to Unified CM if the URI is unknown because the call comes from that zone and has not been manipulated.

Special Considerations

This section describes dial plan considerations related to a number of Cisco Unified CM features, including:

Automated Alternate Routing

The automated alternate routing (AAR) feature enables Unified CM to establish an alternate path for the voice media when the preferred path between two endpoints within the same cluster runs out of available bandwidth, as determined by the locations mechanism for call admission control.

The AAR feature applies primarily to deployments with sites connected via a WAN. For instance, if a phone in branch A calls a phone in branch B and the available bandwidth for the WAN link between the branches is insufficient (as computed by the Locations mechanism), AAR can reroute the call through the PSTN. The audio path of the call would be IP-based from the calling phone to its local (branch A) PSTN gateway, TDM-based from that gateway through the PSTN to the branch B gateway, and IP-based from the branch B gateway to the destination IP phone.

AAR can be transparent to the users. You can configure AAR so that users dial only the on-net (for example, four-digit) directory number of the called phone and no additional user input is required to reach the destination through the alternate network (such as the PSTN).

Note   AAR does not support CTI route points as the origin or the destination of calls. Also, AAR is incompatible with the Extension Mobility feature when users roam across different sites. Refer to Extension Mobility, page 14-81, for more details.

You must provide the following main elements for AAR to function properly:

- Establish the PSTN Number of the Destination, page 14-77
- Prefix the Required Access Codes, page 14-77
- Select the Proper Dial Plan and Route, page 14-79

Establish the PSTN Number of the Destination

The rerouting of calls requires using a destination number that can be routed through the alternate network (for example, the PSTN). AAR uses the dialed digits to establish the on-cluster destination of the call and then combines them with the called party's AAR Destination Mask; if it is not configured, the External Phone Number Mask is used instead. The combination of the dialed digits and the applicable mask must yield a fully qualified number that can be routed by the alternate network.

Alternatively, by selecting the voicemail checkbox in the AAR configuration, you can allow calls to be directed to the voicemail pilot number. This choice does not rely on the numbers originally dialed by the caller, but routes the call according to the voicemail profile configuration.

Note   By default, the directory number configuration retains the AAR leg of the call in the call history, which ensures that the AAR forward to the voice messaging system will select the proper voice mailbox. If you choose "Remove this destination from the call forwarding history," the AAR leg of the call is not present in the call history, which would prevent the automated voice mailbox selection and would offer the caller the generic voicemail greeting.

The AAR Destination Mask is used to allow the destination phone number to be determined independently of the External Phone Number mask. For example, if Caller ID policy for a company required a phone's external phone number mask to be the main directory number of an office (such as 415 555 1000), the AAR destination mask could be set to+1 415 555 1234, to provide AAR with the phone's specific PSTN number.

For example, assume phone A in San Francisco (DN = 2345) dials an on-net DN (1234) configured on phone B located in New York. If locations-based call admission control denies the call, AAR retrieves the AAR Destination Mask of the New York phone (+1212555XXXX) and uses it to derive a number (+12125551234) that can be used to route the call on the PSTN.

It is best to configure the AAR destination mask to yield a fully qualified E.164 number, including the + sign, because this will greatly simplify the overall configuration of AAR. For example, a phone in Paris is configured with an AAR destination mask of +33 1 58 04 58 58. Because this number is a fully qualified E.164 number, it contains all the information required for the Cisco Unified Communications system to derive a routable PSTN number as required by the calling phone's gateway to the PSTN, regardless of whether it is located in France, in Canada, or anywhere else in the world. The following sections elaborate on this approach.

Prefix the Required Access Codes

If the AAR Destination Yields a Fully Qualified E.164 Number Including the + Sign

This is the simplest case; the AAR destination contains + as a wildcard to be replaced by the appropriate access codes require at each gateway. The destination number is ready to be routed to an appropriate route pattern and then transformed at the point of egress to the PSTN by the appropriate called party transformation patterns.

Example 1: A phone in Ottawa, Canada calls a phone in Paris, which triggers AAR due to a lack of bandwidth on the WAN. The AAR destination is +33 1 58 04 58 58. The AAR calling search space of the calling phone contains a route pattern \+!, which routes the call to the Standard Local Route Group. The call is routed to the local gateway in Ottawa, where called party transformation patterns will replace the + with the applicable international access code 011. The resulting call is placed to 011 33 1 58 04 58 58.

Example 2: A phone in Nice, France calls a phone in Paris, which triggers AAR due to a lack of bandwidth on the WAN. The AAR destination is +33 1 58 04 58 58. The AAR calling search space of the calling phone contains a route pattern \+!, which routes the call to the Standard Local Route Group. The call is routed to the local gateway in Nice, where called party transformation patterns will replace the + 33 with the applicable national access code 0. The resulting call is placed to 01 58 04 58 58.

If the AAR Destination Mask Yields a Number Including the Country Code

The destination number (assumed to include the country code) might require a prefix to be routed properly by the origination branch's dial plan. Furthermore, if the point of origin is located in a different area code or even a different country, then other prefixes such as international dialing access codes (for example, 00 or 011) might be required as part of the dialed string.

When configuring AAR, you place the DNs in AAR groups. For each pair of AAR groups, you can then configure prefix digits to add to the DNs for calls between the two groups, including prefix digits for calls originating and terminating within the same AAR group.

As a general rule, place DNs in the same AAR group if they share the same inter-country dialing structure. For example, all phones in the UK dial numbers outside the UK with 9 as a PSTN access code, followed by 00 for international access; all phones in France and Belgium use 0 as a PSTN access code, followed by 00 for international access; all phones in the NANP use 9 as a PSTN access code, followed by 011 for international access.

This yields the following AAR group configuration:

AAR Group	NANP	Cent_EU	UK
NANP	9	9011	9011
Cent_EU	000	000	000
UK	900	900	9

Example 3: A phone in Ottawa, Canada calls a phone in Paris, which triggers AAR due to a lack of bandwidth on the WAN. The AAR destination is 33 1 58 04 58 58. The AAR group of the calling phone is NANP and that of the destination phone is Cent-EU, thus yielding a prefix of 9011. The AAR calling search space of the calling phone contains a site-specific route pattern 9011!, which routes the call to a route list in Ottawa, stripping the 9. The call is routed to the local gateway in Ottawa. The resulting call is placed to 011 33 1 58 04 58 58.

Example 4: A phone in Brussels, Belgium calls a phone in Paris, which triggers AAR due to a lack of bandwidth on the WAN. The AAR destination is 33 1 58 04 58 58. The AAR group of the calling phone and that of the destination phone is Cent-EU, thus yielding a prefix of 000. The AAR calling search space of the calling phone contains a site-specific route pattern 000!, which routes the call to a route list in Brussels, stripping the leading 0. The call is routed to the local gateway in Brussels. The resulting call is placed to 00 33 1 58 04 58 58.

These examples clearly show the benefit of a +E.164 dial plan where no specific AAR groups need to be configured.

Voicemail Considerations

AAR can direct calls to voicemail. The voicemail pilot number is usually dialed without the need for an off-net access code (if the voicemail pilot number is a fully qualified on-net number, such as 8 555 1000). When AAR is configured to send calls to voicemail, the AAR group mechanism will still prefix the configured access code(s). This configuration requires the creation of an AAR group to be used by all

DNs whose desired AAR destination is voicemail (for example, vmail_aar_grp). Ensure that the configuration for this voicemail AAR group uses no prefix numbers when receiving calls from other AAR group DNs.

For example: Assume that DNs located in sites San Francisco and New York are configured with AAR group NANP, which prefixes 9 to calls made between any two DNs in the group. If a DN in San Francisco is configured to send AAR calls to voicemail (for example, 8 555 1000), a call would be placed to 985551000, which would result in a failed call. Instead, the San Francisco DN should be configured with AAR group vmail. The prefix digits for calls from AAR group NANP to AAR group vmail are <none>, as shown in the following table. The call will be placed successfully to 85551000.

AAR Group	NANP	Cent_EU	UK	vmail
NANP	9	9011	9011	<none>
Cent_EU	000	000	000	<none>
UK	900	900	9	<none>

Note When Device Mobility is not used, the AAR group configuration of a DN remains the same even as the device is moved to different parts of the network. With Device Mobility, the AAR group can be determined dynamically based on where in the network the phone is physically located, as determined by the phone's IP address. See Device Mobility, page 14-80, for more details.

Select the Proper Dial Plan and Route

AAR calls should egress through a gateway within the same location as the calling phone, thus causing the completed dial string to be sent through the origination site's dial plan. To ensure that this is the case, select the appropriate AAR calling search space on the device configuration page in Unified CM Administration. Configure the off-net dial plan entries (for example, route patterns) in the AAR calling search space to point to co-located gateways and to remove the access code before presenting the call to the PSTN.

For example, phones at the San Francisco site can be configured with an AAR calling search space that permits long distance calls dialed as 91-NPA-NXX-XXXX but that delivers them to the San Francisco gateway with the access code (9) stripped.

The AAR calling search space configuration can be greatly simplified if the local route group is used in conjunction with using a fully qualified E.164 address (including the + sign) as the AAR destination mask. A single calling search space configured with a single partition, containing a single route pattern \+!, pointing to a single route list featuring the Standard Local Route Group, can be used to route the calls of all phones at all sites in an entire cluster. This relies on the pre-configuration of the appropriate gateway-specific called party transformation patterns to adapt the universal form of the destination number to the localized form required by the service provider networks to which the call is delivered at each site.

Note If you have configured additional route patterns to force on-net internal calls dialed as PSTN calls, ensure that these patterns are not matched by the AAR feature.

Note   To avoid denial of re-routed calls due to call admission control, AAR functionality requires the use of a LAN as the IP path between each endpoint and its associated gateway to the PSTN. Therefore, AAR dial plans cannot rely on centralized gateways for PSTN access.

Note   When Device Mobility is configured, the AAR calling search space can be determined dynamically based on where in the network the phone is physically located, as determined by the phone's IP address. See Device Mobility, page 14-80, for more details.

Device Mobility

Device Mobility offers functionality designed to enhance the mobility of devices within an IP network. (For example, a phone initially configured for use in San Francisco is physically moved to New York.) Although the device still registers with the same Unified CM cluster, it now will adapt some of its behavior based on the new site where it is located. Those changes are triggered by the IP subnet in which the phone is located.

When roaming, a phone will inherit the parameters associated with the device pool associated with the device's current subnet. From a dial-plan perspective, the functionality of the following five main configuration parameters can be modified due to the physical location of the phone. For these parameters to be modified, the device must be deemed as roaming outside its home physical location but within its home device mobility group.

- Local route group

  the roaming device pool's Local Route Group is used. For example, if a device is roaming from San Francisco to New York, the local route group of the New York device pool is used to route calls to the PSTN whenever a pattern points to a route list invoking the Standard Local Route Group.

- Calling party transformation CSS

  The roaming device pool's calling party transformation CSS is used. This allows a phone to inherit the calling party presentation mode that is customary for the phones of the visited location.

- Device calling search space

  The roaming device pool's Device Mobility calling search space is used instead of the device calling search space configured on the device's configuration page. For example, if a device is roaming from San Francisco to New York, the Device Mobility calling search space of the New York device pool is used as the roaming phone's device calling search space. If you use the line/device approach to classes of service, this approach will establish the path taken for PSTN calls, routing them to the local New York gateway.

- AAR calling search space

  The roaming device pool's AAR calling search space is used instead of the AAR calling search space configured on the device's configuration page. For example, if a device is roaming from San Francisco to New York, the AAR calling search space of the New York device pool is used as the roaming phone's AAR calling search space. This calling search space will establish the path taken for outgoing AAR PSTN calls, routing them to the local New York gateway.

- DN's AAR group

  For incoming AAR calls, the AAR group assigned to a DN is retained, whether or not the DN's host phone is roaming. This ensures that the reachability characteristics established for the AAR destination number are retained.

For outgoing AAR calls, the calling DN's AAR group uses the roaming device pool's AAR group instead of the AAR group selected on the DN's configuration page. Note that this AAR group will be applied to all DNs on the roaming device. For example, all DNs on a device roaming from New York to Paris (assuming both locations are in the same Device Mobility group) would inherit the AAR group configured for outgoing calls in the Paris device pool. This AAR group would be applied to all DNs on the roaming device and would allow for the appropriate prepending of prefix digits to AAR calls made from DNs on the roaming phone.

Call Forward All When Roaming

When a device is roaming in the same device mobility group, Unified CM uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, if the CFA CSS is set to None, and if the CFA CSS Activation Policy is set to With Activating Device/Line CSS, then:

- The Device CSS and Line CSS get used as the CFA CSS when the device is in its home location.

- If the device is roaming within the same device mobility group, the Device Mobility CSS from the Roaming Device Pool and the Line CSS get used as the CFA CSS.

- If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.

The section on Device Mobility, page 23-13, explains the details of this feature.

Extension Mobility

The Extension Mobility feature enables a user to log in to an IP phone and automatically apply his or her profile to that phone, including extension number, speed dials, message waiting indicator (MWI) status, and calling privileges. This mechanism relies on the creation of a device profile associated with each Extension Mobility user. The device profile is effectively a virtual IP phone on which you can configure one or more lines and define calling privileges, speed dials, and so on.

When an IP phone is in the logged-out state, (that is, no Extension Mobility user has logged into it), the phone characteristics are determined by the device configuration page and the line configuration page(s). When a user logs in to an IP phone, the device configuration does not change, but the existing line configuration is saved in the Unified CM database and is replaced by the line configuration of the user's device profile.

One of the key benefits of Extension Mobility is that users can be reached at their own extensions regardless of where they are located, provided that they can log in to an IP phone controlled by the same Unified CM cluster. When Extension Mobility is applied to multisite deployments with centralized call processing, this capability is extended to multiple sites geographically separated from each other.

However, if you combine the Extension Mobility feature with the AAR feature described in the section on Automated Alternate Routing, page 14-76, some limitations exist. Consider the example shown in Figure 14-32, where Extension Mobility and AAR are deployed in a centralized call processing Unified CM cluster with one site in San Jose and one in New York.

Figure 14-32   Extension Mobility and AAR
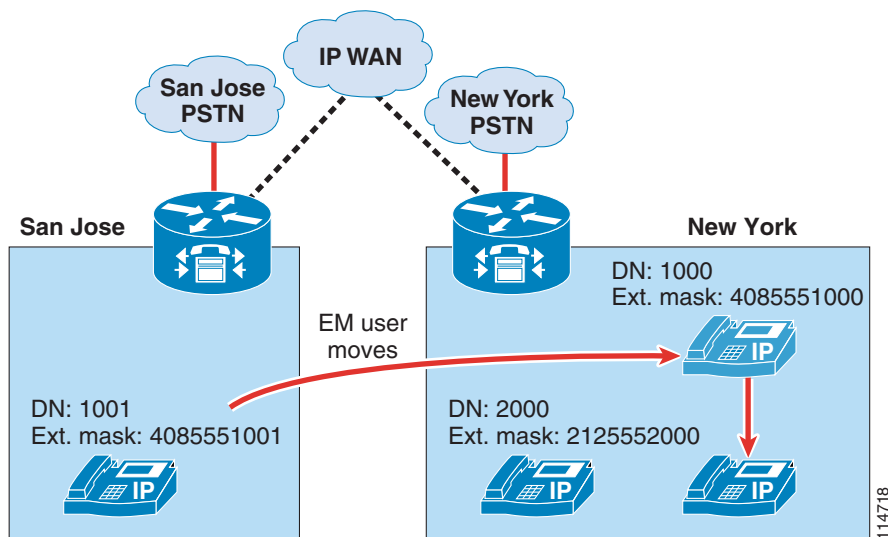
In this example, assume that an Extension Mobility user who is normally based in San Jose has a DN of 1000 and a DID number of (408) 555-1000. That user's external phone number mask (or AAR mask, if used) is therefore configured as 4085551000. The user now moves to the New York site and logs in. Also, assume that the IP WAN bandwidth between San Jose and New York has been entirely utilized.

When the user in San Jose with extension 1001 tries to call 1000, AAR is triggered and, based on the AAR calling search space of the calling party and the AAR groups of both parties, a new call to 914085551000 is attempted by the San Jose phone. This call uses the San Jose gateway to access the PSTN, but because the DID (408) 555-1000 is owned by that same gateway, the PSTN sends the call back to it. The San Jose gateway tries to complete the call to the phone with extension 1000, which is now in New York. Because no bandwidth is available to New York, the AAR feature is invoked again, and one of the following two scenarios will occur:

- If the gateway's AAR calling search space contains external PSTN route patterns, this is the beginning of a loop that eventually uses all the PSTN trunks at the San Jose site.

- If, on the other hand, the gateway's AAR calling search space contains only internal numbers, the call fails and the caller hears a fast-busy tone. In this case, one PSTN call is placed and one is received, so two PSTN trunks are utilized on the San Jose gateway for the duration of the call setup.

Tip   To prevent routing loops such as the one described here, always configure all calling search spaces on the gateway configuration pages to include only internal destinations and no route patterns pointing to route lists or route groups containing that same gateway.

This example highlights the fact that Extension Mobility leverages the dynamic aspect of Cisco IP Communications and, therefore, requires that the call routing between sites use the IP network. Because the E.164 numbers defined in the PSTN are static and the PSTN network is unaware of the movements of the Extension Mobility users, the AAR feature, which relies on the PSTN for call routing, cannot be used to reach Extension Mobility users who move to a site other than their home site.

Note   However, if the Extension Mobility user moves to a remote site that belongs to the same AAR group as his or her home site, he or she can use the AAR feature to place calls to other sites when the available IP WAN bandwidth is not sufficient. This is because the path of such a call is determined by the AAR

calling search space of the phone from which the call originates. This AAR calling search space does not change when users log in or out of Extension Mobility, and it should be configured to use the visited remote site's gateway.

Tip Configure unregistered Extension Mobility profile DNs to send calls to voicemail. See Call-Forward Calling Search Spaces, page 14-43, for details.

Special Considerations for Cisco Unified Mobility

Cisco Unified Mobility (see the section on Cisco Unified Mobility, page 23-35) relies on functionality that has a direct impact on call routing. To understand the effects of the Cisco Unified Mobility parameters related to dial plans, consider the following example:

Note Only those parameters required in the discussion are mentioned here.

User Paul has an IP phone configured as follows:

DN: 8 555 1234

DID number: +1 408 555 1234

External Phone Number Mask: 408 555 1234

Line Calling Search Space: P_L_CSS

Device Calling Search Space: P_D_CSS

Paul's DN is associated with a Remote Destination Profile configured as follows:

Calling Search Space: P_RDP_CSS

Rerouting Calling Search Space: P_RDP_Rerouting_CSS

Calling Party Transformation CSS: P_CPT_CSS

Paul's RDP is associated with a Remote Destination configured as follows:

Destination Number: +1 514 000 9876 (This is Paul's mobile phone number, on either a single-mode or dual-mode phone.)

Calls from the PSTN placed to Paul or Ringo's DID number are handled by a gateway configured as follows:

Calling Search Space: GW_CSS

Significant digits: 7

Prefix DN: 8

User Ringo has an IP phone configured as follows:

DN: 8 555 0001

DID number: 408 555 0001

External Phone Number Mask: 408 555 0000 (This is the enterprise's main business number.)

Line Calling Search Space: R_L_CSS

Device Calling Search Space: R_D_CSS

■ **Special Considerations**

The following sections explain the effects of the above mobility parameters on call routing.

Remote Destination Profile

Remote destination profiles (RDPs) are associated with directory numbers (for example, the DN of a user's IP phone) and with remote destinations (for example, the mobile phone number of a user). The RDP controls the interaction between the IP phone and the external numbers (for example, a mobile phone) configured as remote destinations.

Note   Remote destinations cannot be configured with on-cluster DNs as destination numbers.

Remote Destination Profile's Rerouting Calling Search Space

When a call is placed to a DN associated with a remote destination profile, the call has the effect of ringing both the DN and the number(s) configured as remote destination(s).

The ability of the caller to reach the destination IP phone is controlled by the caller's Calling Search Space settings. However, the ability for the call to be forked toward the remote destination (for example, a mobile phone) is controlled by the called mobility user's Rerouting Calling Search Space.

For example:
Ringo calls Paul from his IP phone by dialing 8 555 1234. Paul's IP phone rings, as well as his mobile phone.

Here, the ability for Ringo to reach Paul's DN is controlled by the Line and Device calling search spaces on Ringo's IP phone. The dialed destination (8 555 1234) must be in a partition found in the concatenated calling search spaces R_L_CSS and R_D_CSS.

For this same call to be forked to ring Paul's mobile phone, the configured remote destination (+1 514 000 9876) must match a pattern found in the calling search space P_RDP_Rerouting_CSS.

Note   Even if the dialing privileges assigned to Ringo's phone do not allow for external calls, the call to the remote destination is handled by the rerouting calling search space associated with Paul's remote destination profile.

Remote Destination Profile's Calling Search Space

A service parameter (Inbound Calling Search Space for Remote Destination) controls which calling search space is used to route calls originating from one of the cluster's remote destinations. Its default setting is Trunk or Gateway Inbound Calling Search Space, which routes all incoming calls using the trunk's or gateway's configured CSS. If the service parameter is set to Remote Destination Profile + Line Calling Search Space, then the concatenation of the line CSS of the DN associated with the match's remote destination and the CSS of the Remote Destination Profile associated with the remote destination will be used to route the call.

All the numbers defined as remote destinations within the same cluster will be searched to find a match for any external call coming into the cluster.

The following examples assume that the service parameter Inbound Calling Search Space for Remote Destination is set to Trunk or Gateway Inbound Calling Search Space.

For example:

Paul uses his mobile phone to call Ringo at his desk. The call comes into the gateway from the PSTN, with a calling party number of 514 000 9876 and a called party number of 408 555 0001. The call is routed to Ringo's phone. The number displayed as the calling party number on Ringo's phone is Paul's desk phone number, 8 555 1234. This allows Paul's mobile phone number to remain confidential and allows Ringo's calls placed from the missed and received calls lists to ring into Paul's IP phone, thus making the full set of enterprise mobility features available.

When the call comes into the gateway, the PSTN offers a calling party number of 514 000 9876 and a called party of 408 555 0001. The gateway's configuration will retain the last seven significant digits of the called number and prefix 8, yielding 8 555 0001 as the destination number.

The system detects that the calling party number matches Paul's remote destination number. Upon detecting this match, the system will:

1. Change the calling party number to Paul's DN, 8 555 1234.

2. Route the call to the called number using the incoming gateway's calling search space. Specifically, the routing is done through the GW_CSS calling search space.

The destination (called) number presented by the gateway should be the DN of the phone, and the calling party substitution illustrated in step 1 above renders possible the use of one-touch dialing from the missed/received calls lists.

Note   There is no way to partition remote destination numbers. This is worth noting in case multiple user groups (such as different companies, sub-contractors, and so forth) are using the same cluster. When the service parameter Inbound Calling Search Space for Remote Destination is set to Trunk or Gateway Inbound Calling Search Space, the call routing is based on the incoming trunk's or gateway's CSS, regardless of whether or not the calling number matches a remote destination. However, the calling party number substitution still occurs if the calling party matches any remote destination. This means that calls from one tenant's remote destination numbers to another tenant's DID numbers will be presented with a transformed calling party number that matches the caller's on-net extension DN.

Note   Any incoming external call where Calling Party Number is not available will be routed according to the incoming gateway's CSS. This also applies to incoming calls from IP trunks, such as SIP or H.323 trunks.

Remote Destination Profile's Calling Party Transformation CSS and Transformation Patterns

Calls originating from an enterprise IP phone to a mobility-enabled DN are forked to both the enterprise destination IP phone's DN and one (or multiple) external destinations. One challenge this creates is to deliver calling party numbers adapted to each destination phone's dial plan. This is to allow for redialing of calls from missed calls and received calls lists. For an enterprise phone, the calling party numbers should be redialable enterprise phone numbers. For a remote destination on the PSTN (such as a home phone or a mobile phone), the calling party number should be transformed from the enterprise number associated with the calling IP phone to a number redialable from the PSTN (generally, the DID number of the calling phone).

When a call is placed to a mobility-enabled enterprise DN, the associated remote destination profile's calling party transformation calling search space is used to find a match to the caller's calling party number. It contains partitions which themselves contain transformation patterns.

Transformation patterns control the adaptation of calling party numbers from enterprise format to PSTN format. They differ from all other patterns in Unified CM in that they match on the calling number, not the called number. The matching process is done through a regular expression (for example, 8 555 XXXX), and the transformation process allows for the optional use of the calling DN's external phone number mask as well as transformation patterns and digit prefixing.

Once matched, they perform all configured transformations, and the resulting calling party number is used to reach all remote destinations associated with the Remote Destination Profile for which the match occurred.

For example:

When Ringo calls Paul, we want Paul's IP phone to display the calling party number as 8 555 0001 and Paul's mobile phone to display 408 555 0001.

For this case, we create a transformation pattern with the following parameters:

> Pattern: 8 555 XXXX
>
> Partition: SJ_Calling_Transform
>
> Use calling party's external phone number mask: un-checked
>
> Calling Party Transformation mask: 555 XXXX
>
> Prefix Digits (outgoing calls): 408

We also have to ensure that partition SJ_Calling_Transform is placed in calling search space P_CPT_CSS.

When the call from Ringo is anchored on Paul's phone, two separate call legs are attempted. The first rings Paul's IP phone and offers the caller's DN as Calling Party Number (that is, 8 555 0001). The second call leg is attempted through Paul's Remote Destination Profile. The RDP's calling party transformation CSS, P_CPT_CSS, is used to find a match for 8 555 0001 in all the referenced partition's transformation patterns. Pattern 8 555 XXXX is matched in partition SJ_Calling_Transform. The transformation mask is applied to the calling party number and yields 555 0001. The prefix digits are added, and the resulting calling party number 408 555 0001 is used when placing the call to the remote destinations.

Note that, in this example, we chose not to use the external phone number mask because it is set to a number different than that of Ringo's DID. This offers flexibility in situations where the calling party number offered to off-net destinations is required to be different based on the relationship of the caller to the called party. The call from Ringo to Paul is between co-workers, thus the disclosure of Ringo's DID number is deemed acceptable. Ringo's next call could be to a customer, in which case the main enterprise number 408 555 0000 is the desired Calling Party Number to be offered to the destination.

Note Calling Party Transformation calling search spaces do not implicitly include the <none> partition; therefore, transformation patterns left in the <none> partition do not apply to any Calling Party Transformation calling search space. This is different from all other patterns in Unified CM, where all patterns left in the <none> partition are implicitly part of every calling search space.

Application Dial Rules

Numbers defined as remote destinations are also used to identify and anchor incoming calls as enterprise mobility calls. Often, the form in which the PSTN identifies calls differs from the form in which an enterprise dial plan requires that calls to external numbers be dialed. Application dial rules can be used to adapt the form in which remote destinations are configured to the form required when forking a call to the remote destination. They allow for the removal from, and prefixing of digits to, the numbers configured as remote destinations.

For example:

Assume the number 514 000 9876 is configured as Paul's remote destination number. This corresponds to the form used by the PSTN to identify calls coming into the enterprise. But it differs from the form used by the enterprise dial plan for outgoing calls, which requires that 91 be prefixed. In this case, we need to create an application dial rule to adapt the remote destination form to the enterprise dial plan's form:

Application Dial Rule:

Name: 514000_ten

Description: Used to prefix 91 to ten-digit numbers beginning with 514000

Number begins with: 514000

Number of Digits: 10

Total digits to be removed: 0

Prefix with Pattern: 91

In this example, calls made from Paul's mobile phone into the enterprise are identified as coming from 514 000 9876. This matches the form in which his number is configured as a remote destination, thus allowing the match to be made and triggering the anchoring of the call on Paul's desk phone as well as adapting the Calling Party Number offered to the on-net destination. (For example, when a call is placed to Ringo's DID number, he sees the call as coming from 8 555 1234.)

When a call is placed to Paul's enterprise DN number, the call leg forked to his remote destination number will be processed by the application dial rule above. The string 514 000 matches the beginning of Paul's remote destination number, and it is ten digits long, so no digits are removed and 91 is prefixed. This yields 91 514 000 9876 as a number to be routed through Paul's Remote Destination Profile calling search space (P_RDP_CSS in this case).

Note This approach offers the ability to reuse calling search spaces already defined to route calls made from IP phones. Creating new calling search spaces not requiring prefixes for outbound calls (that is, ones able to route calls to 514 000 9876 directly) is less preferable because it can create situations where external patterns overlap with on-net patterns.

Time-of-Day Routing

To use this feature, configure the following elements:

- Time period
- Time schedule

The time period allows you to configure start and end times for business hours. The start and end times indicate the times during which the calls can be routed. In addition to these times, you can set the event to repeat itself on a weekly or yearly basis. Moreover, you can also configure non-business hours by selecting "No business hours" from the Start Time and End Time options. All incoming calls will be blocked when this option is selected.

A time schedule is a group of specific time periods assigned to the partition. It determines whether the partition is active or inactive during the specified time periods. A matching/dialing pattern can be reached only if the partition in which the dialing pattern resides is active.

As illustrated in Figure 14-33, two hunt pilots with the same calling pattern (8000) are configured in two partitions (namely, RTP_Partition and SJC_Partition). Each of these partitions is assigned a time schedule, which contains a list of defined time periods. For example, RTP phones can be reached using

Hunt Pilot 1 from 8:00 AM to 12:00 PM EST (GMT - 5.00) Monday through Friday as well as 8:00 AM to 5:00 PM on Sundays. In the same way, SJC phones can be reached using Hunt Pilot 2 from 8:00 AM to 5:00 PM PST (GMT - 8.00) Monday through Friday and 8:00 AM to 5:00 PM on Saturdays. Both of the hunt pilots in this example are inactive on July 4th.

Figure 14-33   Time-of-Day Routing
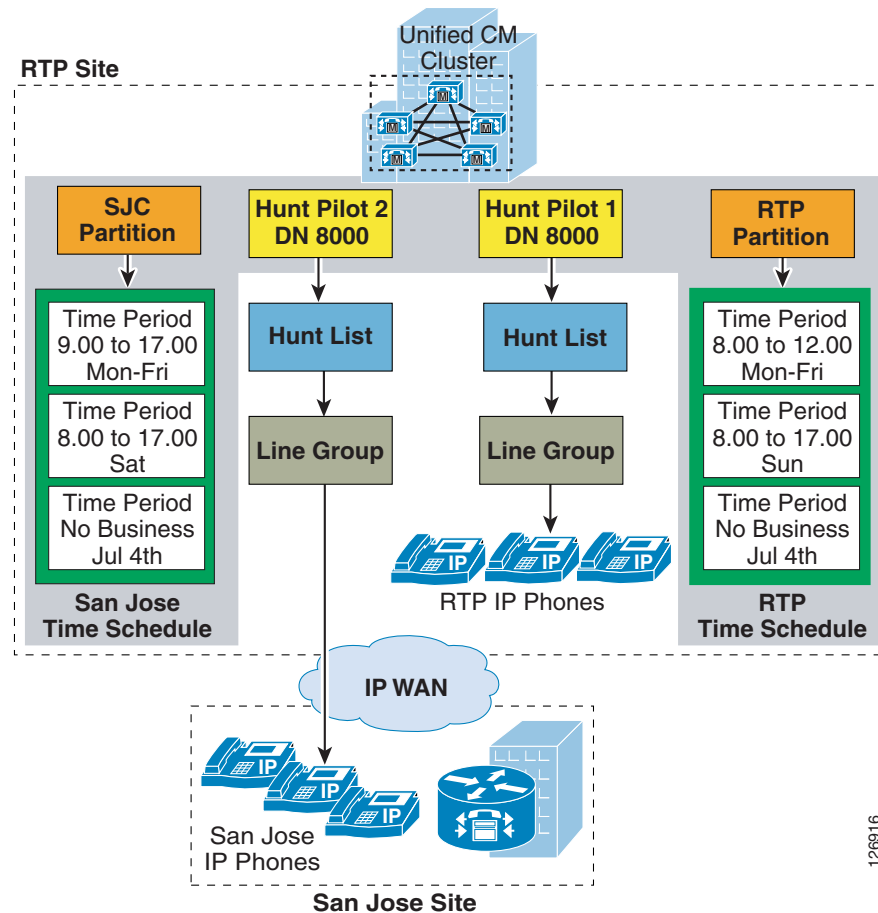
For the example in Figure 14-33, an incoming call to the hunt pilot (8000) on Wednesday at 3:00 PM will be forwarded to the SJC phones, while a person calling the hunt pilot on July 4th will get a fast busy tone unless there is another pattern that matches 8000.

Logical Partitioning

The elements of logical partitioning include:

- Device types, where phones are classified as *interior*, and gateways and trunks are defined as *border*. Table 14-6 lists the endpoint types for different devices.

- Geolocations, where endpoints are assigned a civic address to be used in policy decisions.

- Geolocation filters, where policy decisions can be made on a subset of the geolocation objects.

- Policies, where communications between endpoints are either allowed or denied based on their comparative (filtered) geolocations and device types.

> **Note**   Policies are not applied if all participants in a call (or call attempt) are classified as *interior*. This means that calls between phones on the same cluster are never subjected to logical partitioning policies.

> **Note**   Geolocations are not to be confused with locations configured in Unified CM, which are used for call admission control, or with physical locations used for Device Mobility.

Table 14-6   Device Types

Logical Partitioning Device Types	Cisco Unified Communications Manager Device
Border	• Gateway (for example, H.323 gateway) • Inter-luster trunk (ICT), both gatekeeper-controlled and non-gatekeeper-controlled • H.225 trunk • SIP trunk • MGCP port (E1, T1, PRI, BRI, FXO)
Interior	• Phones (SCCP, SIP, or third-party) • CTI route points • VG224 analog phones • MGCP port (FXS) • Cisco Unity voicemail (SCCP)

Logical Partitioning Device Types

Unified CM classifies endpoints as either *interior* or *border*. This classification is fixed and cannot be modified by the system administrator.

Geolocation Creation

The (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format specified by the following objects:

- Name
- Description
- Country using the two-letter abbreviation
- State, Region, or Province (A1)
- County or Parish (A2)
- City or Township (A3)
- Borough or City District (A4)
- Neighborhood (A5)

- Street (A6)

- Leading Street Direction, such as N or W (PRD)

- Trailing Street Suffix, such as SW (POD)

- Address Suffix, such as Avenue, Platz (STS)

- Numeric house number (HNO)

- House Number Suffix, such as A, 1/2 (HNS)

- Landmark (LMK)

- Additional Location Information, such as Room Number (LOC)

- Floor (FLR)

- Name of Business or Resident (NAM)

- Zip or Postal Code (PC)

Note In Unified CM, you must define geolocations manually.

Geolocation Assignment

Devices are assigned a geolocation from either the device page, the device pool, or the default Geolocation as configured under Enterprise Parameters, in that order of precedence.

Geolocation Filter Creation

Geolocation filters define which of the geolocation objects should be used when comparing the geolocations of different endpoints. For example, a group of phones may be assigned identical geolocations, except for the room and floor in which they are located. Policies may want to consider endpoints located within the same building as being within the same Closed User Group, and thus allowed to communicate. Even though the actual geolocations of each phone differ, the filtered geolocation is the same. This is useful when policies need to be applied to only the top-level fields of geolocation. For instance, a policy that denies communications between phones and gateways in different cities but allows communications between phones and gateways in the same city, could be based on the comparative filtered geolocations where objects more granular than the City are ignored.

Geolocation Filter Assignment

Phones inherit the filter assignment of their device pool. Gateways and trunks can be configured with a geolocation filter at the device or device pool level, in that order of precedence.

Logical Partitioning Policy Configuration

Logical partitioning policies are configured between geolocation identifiers. A geolocation identifier is the combination of a filtered geolocation and a device type. The filtered geolocation is obtained by taking a device's geolocation and applying the device's associated geolocation filter.

A policy is created as the combination of a set of geolocation objects and a device type (a source geolocation identifier) in relationship with another such combination (the target geolocation identifier). When the relationship is matched, the configured action of "allow" or "deny" is applied to the call leg.

Note   Each set of geolocation objects configured in a policy is considered in association with a single device type. For example, a set of geolocation objects such as Country=India, State=Karnataka, City=Bangalore needs to be associated with device type Interior for actions pertaining to Bangalore phones, and separately associated with device type Border for actions pertaining to Bangalore gateways.

Logical Partitioning Policy Application

When user action results in the creation of a new call leg (for example, when a user conferences a third caller into a preexisting call), Unified CM will match the geolocation identifiers of each participant pairs to those of preconfigured policies.

Note   When the geolocation identifiers of two devices are being evaluated by logical partitioning, no policy is applied if both devices are of device type Interior. This means that no call, conference, transfer, or so forth, between IP phones within the same cluster will ever be denied due to logical partitioning policies.

For example, consider phones A and B located in Bangalore, India, and gateway C located in Ottawa, Canada. Phone A calls phone B. Because both devices are of type Interior, no policy is invoked. The call is established, and then the user at phone A invokes a conference, which would bring in gateway C. Before the action is allowed, Unified CM will check the geolocation identifiers of A and C, as well as those of B and C, for a match with the preconfigured policies. If any of the matching policies results in a deny action, the new call leg cannot be established.

Note   The default policy in Unified CM is deny; in other words, if no policy is configured explicitly to permit a call leg, the call leg will be denied.

In the example above, unless an explicit policy is configured to allow Bangalore Interior devices to connect to Ottawa Border devices, the call leg will be denied.