

Designing a Static Dial Plan

Version History

Version Number	Date	Notes
1	09/10/2001	This document was created.
2	10/25/2001	Editorial comments were incorporated.

This solutions document describes how to design and implement static H.323 dial plans and how to configure and manage static H.323 dial plans on gateway and gatekeeper platforms for large Voice over IP (VoIP) networks.

This document includes the following sections:

- [Introduction, page 1](#)
- [Design Methodology for Large-Scale Dial Plans, page 5](#)
- [H.323 Network Components in Large-Scale Dial Plans, page 26](#)
- [Use of Translation Rules, Technology Prefixes, and Dial Peer Failover Example, page 34](#)
- [Implementing an International Dial Plan Example, page 39](#)
- [Related Documents, page 55](#)

Introduction

A dial plan is a numbering plan for the voice-enabled network. It is the way that you assign individual or blocks of telephone numbers (E.164 addresses) to physical lines or circuits. The North American telephone network is based on a 10-digit dial plan consisting of 3-digit area codes and 7-digit telephone numbers. For telephone numbers located within an area code, a 7-digit dial plan is used for the Public Switched Telephone Network (PSTN). Features within a telephone switch (such as Centrex) support a custom 5-digit dial plan for specific customers that subscribe to that service. PBXs also support variable-length dial plans, containing from 3 to 11 digits.

Dial plans in the H.323 network contain specific dialing patterns so that users can reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the numbers of digits dialed are all a part of any particular dial plan. Dial plans used with voice-capable routers essentially describe the process of determining which and how many digits to store in each of the configurations. If the dialed digits match the number and patterns, the call is processed for forwarding.

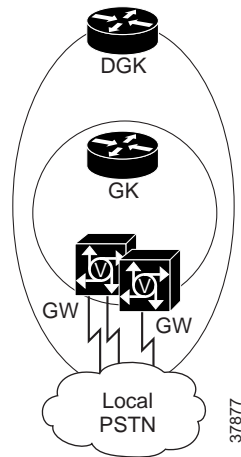
Design of dial plans requires knowledge of the network topology, current telephone number dialing patterns, proposed router locations, and traffic routing requirements. No standard protocol is defined for the dynamic routing of E.164 telephony addresses. Until a standards-based dynamic routing protocol for E.164 telephony addresses is developed, H.323 VoIP dial plans are statically configured and managed on gateway and gatekeeper platforms.

Core Components of Large H.323 Networks

The infrastructure of a typical H.323 VoIP network includes gateways (GWs) and gatekeepers (GKs). In a typical service provider network, a number of GWs are deployed at points of presence (POPs) throughout the service provider coverage area. A GK is used to group these GWs into a logical zone of control and perform all call routing among them.

Larger H.323 VoIP networks might consist of multiple GKs that segment the network into various local zones. In this case, GKs must communicate with each other to route calls between GWs located in different zones. To simplify dial plan administration for these multigatekeeper networks, Cisco introduced the concept of a directory gatekeeper (DGK) to handle call routing between local GKs. [Figure 1](#) illustrates how these core components of an H.323 network relate to one another.

Figure 1 H.323 Network Core Components



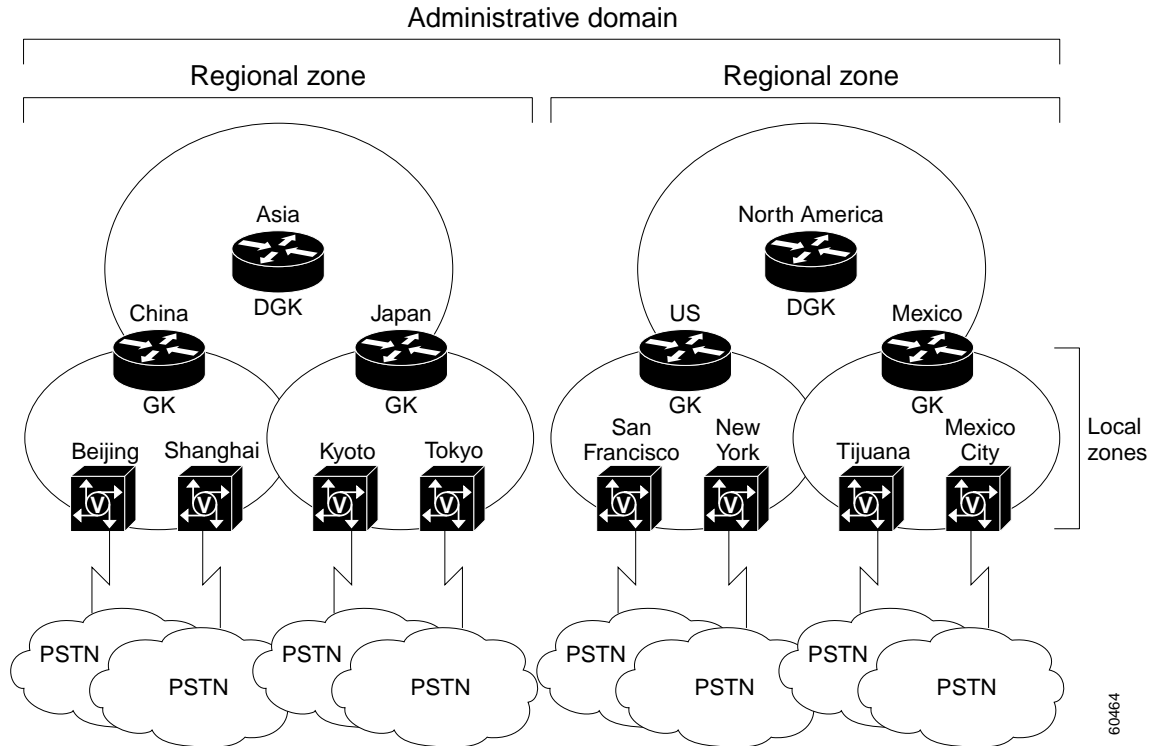
[Table 1](#) summarizes the functions of the network core components.

Table 1 Core Components and Their Functions

Component	Functions
Gateway	<ul style="list-style-type: none"> • Acts as the interface between the PSTN and the IP network • Normalizes numbers from the PSTN before they enter the IP network • Normalizes numbers from the IP network before they enter the PSTN • Contains the dial peer configuration • Registers to a GK
Gatekeeper	<ul style="list-style-type: none"> • Performs call routing searches at an intermediate level (for example, NPA-NXX) • Distributes the NPA among other GKs • Provides GW resource management (for example, RAI and gw-priority) • Provides zone maintenance
Directory Gatekeeper	<ul style="list-style-type: none"> • Performs call routing searches at the highest level (for example, country code) • Distributes country codes among other DGKs • Forwards location requests (LRQs) to a partner DGK if the call does not terminate in the local service provider DGK

With respect to the VoIP dial plan, each component within the H.323 network has a specific responsibility. GWs make edge routing decisions between the PSTN and the H.323 network; gatekeepers and directory gatekeepers handle the core call routing logic among devices within the H.323 network. This document explains the configuration requirements for each of these network components. [Figure 2](#) illustrates the relationship of GWs, GKs, and DGKs in a large-scale H.323 VoIP network.

Figure 2 Relationship of Gateways, Gatekeepers, and Directory Gatekeepers

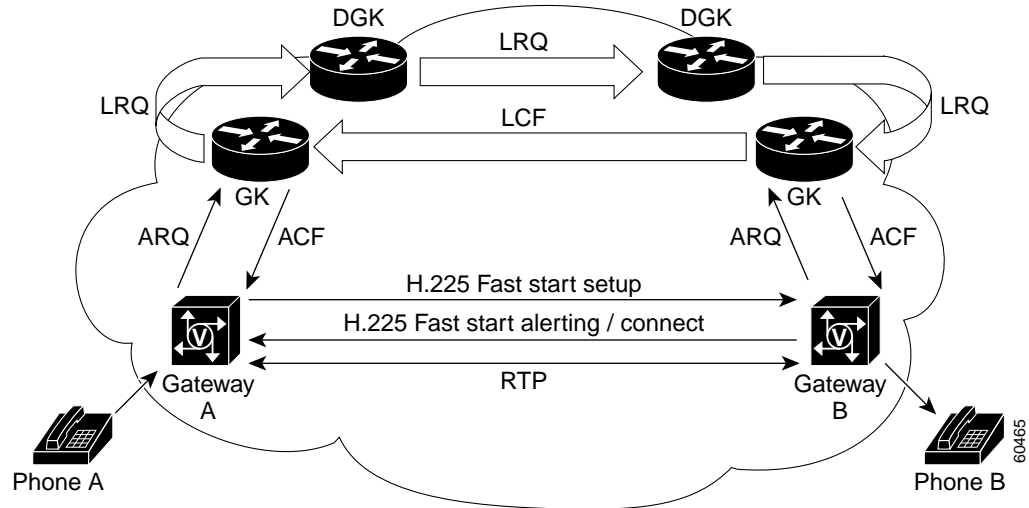


60464

When presented with a call, GWs determine whether to send it to the PSTN or into the H.323 VoIP network. If the call is sent into the H.323 VoIP network, the GW then asks the gatekeeper to select the best endpoint to receive the call. Based on its routing table, the gatekeeper might find that this endpoint is a device within its own local zone of control and supply the IP address of the terminating endpoint. Alternatively, it might determine that the endpoint resides under the control of another remote gatekeeper. In this latter case, the gatekeeper would forward the location request (LRQ) to the remote gatekeeper either directly or through a directory gatekeeper. The remote gatekeeper would ultimately respond with the address of the terminating endpoint.

The communication between GWs and GKs is based on standard H.323v2 Registration, Admission, and Status (RAS) messages. GWs query gatekeepers for routes using RAS admission request (ARQ) and admission confirmation (ACF) messages. Cisco gatekeepers and directory gatekeepers also communicate with each other using RAS LRQ and location confirmation (LCF) messages. Real-Time Transport Protocol (RTP) provides the end-to-end transport functions. Figure 3 shows an example RAS message sequence when phone A calls phone B.

Figure 3 Example of RAS Messaging When Phone A Calls Phone B



Overview of the Dial Plan

The dial plan is the method by which individual blocks of telephone numbers (technically, E.164 addresses) are assigned to physical facilities, or circuits. For large-scale service provider networks, dial plans consist of the following elements:

- A grouping of E.164 prefixes with respect to zones and zone GKs
- An assignment of E.164 address blocks to POPs and POP GWs
- The normalization (number translation, prefixing, and digit stripping) of telephone numbers at the POP GWs
- The establishment of POTS and VoIP dial peers at the GWs

POTS dial peers define the phone numbers or prefixes of attached telephony devices, and the VoIP dial peers define the IP address of the remote device (H.323 GW, GK, or endpoint) that is connected to remote phone numbers. POTS dial peers will always point to a voice port on the router, and the destination of a VoIP dial peer will always be the IP address of a device that can terminate the VoIP call.

Design Methodology for Large-Scale Dial Plans

It is important to apply some basic design principles when designing a large-scale dial plan. Design options in this document will consider the principles described in the following sections:

- [Dial Plan Distribution, page 6](#)
- [Hierarchical Design, page 6](#)
- [Simplicity in Provisioning, page 7](#)
- [Reduction in Postdial Delay, page 17](#)
- [Availability and Fault Tolerance, page 19](#)

Dial Plan Distribution

Good dial plan architecture relies on effectively distributing the dial plan logic among the GW and GK components. Isolating H.323 devices to a specific portion of the dial plan reduces the complexity of the configuration. Each component can focus on accomplishing specific tasks. Generally, local POP-specific details are handled at the local GW; higher-level routing decisions are passed along to the GKs and DGKs. A well-designed network places the majority of the dial plan logic at the GK and DGK devices.

Hierarchical Design

Strive to keep the majority of the dial plan logic (routing decision-making and failover) at the highest component level. The DGK is generally considered the highest-level device. By maintaining a hierarchical design, you make the addition and deletion of zones more manageable. For example, scaling of the overall network is much easier when configuration changes need be to made to only a single DGK and a single zone GK instead of all the zone GKs.

Use a tiered architecture approach, using GWs, GKs, and DGKs. Security, redundancy, and network management are implemented after you take the following steps:

1. Determine your dial plan coverage areas. A GK (instead of a DGK) could cover one country code, for example.
2. Analyze and logically group the components to determine what area(s) each component will be responsible for: a country code, an area code, or several prefixes, for example.
3. At the GW level, logically group the GWs into POPs. (Generally, POPs are situated in the highest density coverage areas: major cities, for example.)
4. Determine how many gateways you need by doing the following:
 - a. Measure the busy hour traffic (BHT). (Design the network for the peak-hour volume.)
 - b. Determine the number of DS-0s that you need to handle the BHT.
 - c. Determine how many GWs you need to service the DS-0s.
 - d. Understand the calls-per-second performance and DS-0 capacity of the selected GW platform.



Note

GWs have different DS-0 capacities; a Cisco 5400 router has the capacity for many more DS-0s than does a Cisco 5300, for example. The number of GWs needed also depends on the processing capability of the selected GW platform. A Cisco 5400 has more DS-0 capacity and more processing capability (than a Cisco 5300), so it would use more GK resources than a Cisco 5300. You would need to provision fewer Cisco 5400 routers at a POP than you would Cisco 5300 routers.

5. Logically separate the POPs into zones. A zone can have one or many POPs.
6. At the GK level, determine which GKs should administer which zones. A GK is used to group GWs into logical zones of control, and perform all call routing between the zones.

The number of GKs you need depends on GW capacity and traffic load. The number of GKs per POP or POPs per GK depends on how many GWs are used. For example, 35 GWs in 1 POP could be 1 zone, requiring one GK; 4 POPs with 4 GWs each might function adequately with one GK administering the 16 GWs.

7. At the DGK level, determine which DGKs should administer which GKs. See step 3.

8. Consider that your DGKs (your highest level component) will exchange LRQs with other DGKs, acting as a demarcation point between separate carriers.

Simplicity in Provisioning

You should keep the dial plan on the GWs and GKs as simple and symmetrical as possible when designing a network. Try to keep consistent dial plans on the GWs by using translation rules to manipulate the local digit dialing patterns. These number patterns can be normalized into a standard format or pattern before the digits enter the VoIP core. Putting digits into a standard format simplifies GK zone prefix provisioning and GW dial peer management.

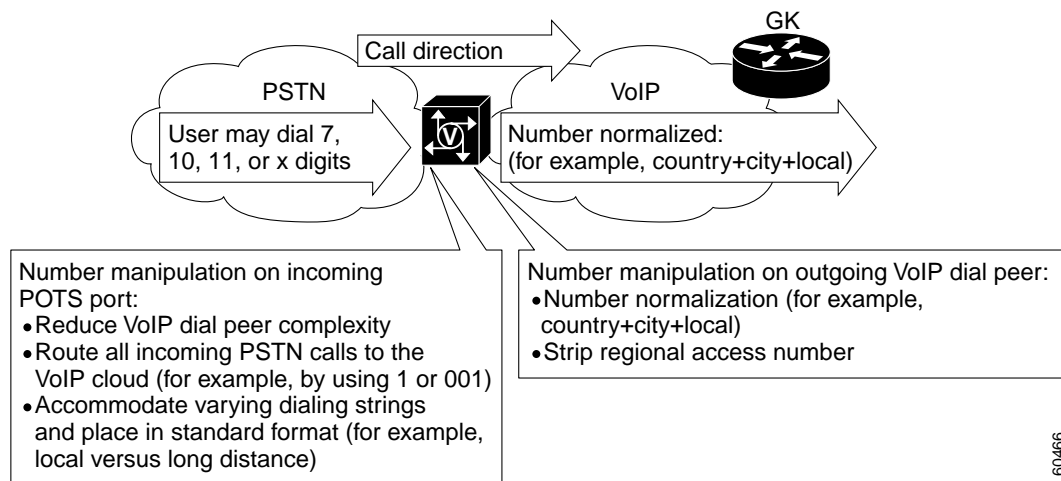
This methodology helps reduce the number of dial peer configurations on the outgoing POTS interface. If the GK can be provisioned to direct only calls of a certain area code to a particular GW, then you would not need to provision all of the individual GWs with their respective area codes. Instead, you might be able to generalize the GW configurations. By normalizing the number, you also reduce the zone prefix search length, reducing the time required to search for a zone prefix match. For example, if you have the 0118943xxxx digit pattern, you can send the number as 8943xxxx and have the GK search on 89 as opposed to 01189.

Number Normalization and Translation Rules

Gateway dial plan configurations focus on local PSTN access information for the edge of the H.323 network. These dial plan configurations include defining which E.164 prefixes are supported by the PSTN connections of the GW. In large-scale service provider designs, you might rely on the GW to perform digit manipulation, whereby the GW takes a calling (or called) number and strips or adds (prefixes) digits before sending the number to its destination. The process of formatting the number to a predefined pattern is called *number normalization*.

Figure 4 illustrates an example of number normalization from the PSTN to the VoIP core. Digit manipulation can be configured on the incoming POTS port or the outgoing VoIP dial peer to format a 7-, 10-, 11-, or x-digit pattern into a fixed 10-digit pattern (United States-centric). The result is a number that has been normalized when it enters the VoIP cloud.

Figure 4 Number Normalization from PSTN to VoIP



60466

Translation Rules

The GW uses the Cisco IOS translation rules to accomplish digit manipulation. Translation rules can be configured on the GW physical port or on a VoIP dial peer, as shown in the following example:

```
translation-rule 1
Rule 0 ^0111.% 1
Rule 1 ^0112.% 2
Rule 2 ^0113.% 3
Rule 3 ^0114.% 4
Rule 4 ^0115.% 5
Rule 5 ^0116.% 6
Rule 6 ^0117.% 7
Rule 7 ^0118.% 8
Rule 8 ^0119.% 9
!
dial-peer voice 1 voip
destination-pattern 011T
translate-outgoing called 1
session target ras
!
```

The preceding translation rule matches digit patterns that begin with 0111 through 0119 and translates this 4-digit pattern into a single digit from 1 to 9, while preserving the remaining digits included in the digit pattern. This process effectively strips the 011 (a common international access code) and sends the remaining digits to the VoIP gatekeeper for call routing.

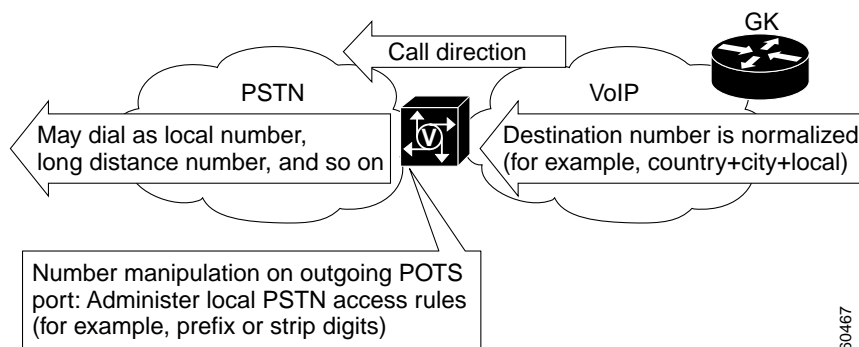
You can use translation rules to manipulate both automatic number identification (ANI) and dialed number identification service (DNIS) numbers. The following dial peer configuration commands can be used to match the ANI or DNIS of a call:

- **answer-address**
- **destination-pattern**
- **incoming called-number**
- **numbering-type**

You can test your translation rules by using the **test translation-rule** command.

The GW can perform number manipulation when calls come into the GW from the VoIP network. In this case, the dial peer on the POTS port can either strip or add digits when sending numbers out to the PSTN. [Figure 5](#) depicts number normalization from the VoIP network to the PSTN.

Figure 5 Number Normalization from VoIP Back to PSTN



60467

The following example of a POTS dial peer shows how the Cisco IOS **prefix** command can be used to add digits to a calling number:

```
dial-peer voice 20 pots
 destination-pattern 510.....
 prefix 1510
```

The preceding **prefix** command substitutes 1510 for the 510 and effectively adds a 1 to any 10-digit pattern that begins with 510.

Number Normalization for an International Dial Plan Example

Suppose you are a service provider that provides VoIP transport for calls originating from the San Jose area (408 area code). San Jose subscribers use the following digit patterns when making calls:

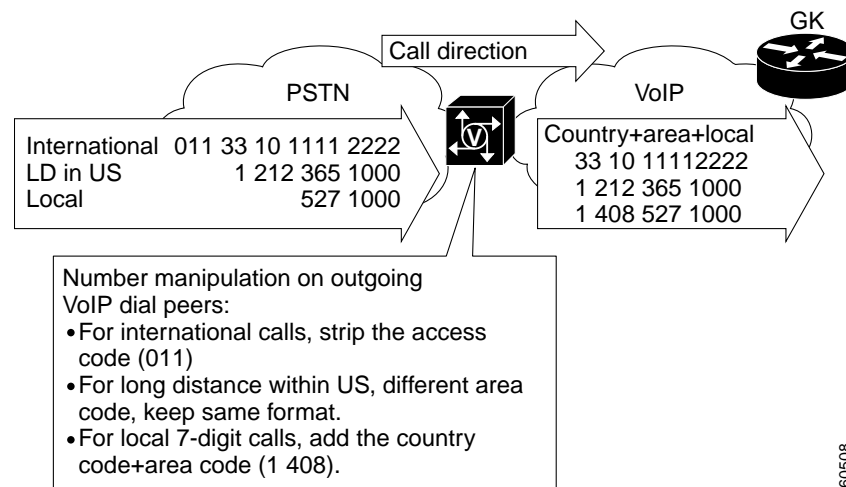
- For local calls within the San Jose area code: use a 7-digit number, for example, 555-1000
- For long distance calls within the United States: use an 11-digit number, for example, 1-212-555-1000
- For international calls: use a 011 access code, a country code, an area code, and the number, for example, 011-33-10-1111-2222

Suppose you want long distance calls to go through the VoIP network, but local calls to go back through the PSTN. The GK should always be queried to make this call routing decision. In this case, ARQs from the GW to the GK should be in the standard format:

country code + city (or area) code + local number

regardless of whether the user dialed 7 digits (local call), 11 digits (long distance call), or an international call with a 011 access code. You will need to configure the GW to normalize these patterns. The number normalization logic is shown in [Figure 6](#).

Figure 6 Number Normalization Logic



In the following configuration example, translation rules are applied to perform the number normalization:

```
Hostname SJC-GW
!
translation-rule 2
 Rule 0 ^2..... 14082
```

```

Rule 1 ^3..... 14083
Rule 2 ^4..... 14084
Rule 3 ^5..... 14085
Rule 4 ^6..... 14086
Rule 5 ^7..... 14087
Rule 6 ^8..... 14088
Rule 7 ^9..... 14089
!
translation-rule 1
Rule 0 ^0111.% 1
Rule 1 ^0112.% 2
Rule 2 ^0113.% 3
Rule 3 ^0114.% 4
Rule 4 ^0115.% 5
Rule 5 ^0116.% 6
Rule 6 ^0117.% 7
Rule 7 ^0118.% 8
Rule 8 ^0119.% 9
!
interface Ethernet0/0
 ip address 172.19.49.166 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719
 h323-gateway voip h323-id US-GW1
!
 ip classless
 ip route 0.0.0.0 0.0.0.0 172.19.49.129
 no ip http server
!
 voice-port 1/0/0
!
 voice-port 1/0/1
!
 dial-peer voice 1408 pots
 destination-pattern 14085551000
 port 1/0/0
!
 dial-peer voice 1 voip
 destination-pattern 011T
 translate-outgoing called 1
 session target ras
!
 dial-peer voice 2 voip
 destination-pattern 1T
 session target ras
!
 dial-peer voice 3 voip
 destination-pattern [2-9]T
 translate-outgoing called 2
 session target ras
!
 gateway
!
```

The following bullets summarize how number normalization works in the preceding example:

- For international calls, strip the access code

Translation rule 1 strips the 011 access code on numbers that begin with 011. The translation rule is applied to dial peer 1, which matches all numbers beginning with 011 (that is, 011T). The “T” acts as a wildcard with *interdigit timeout*; the digits will be collected when the user does not enter a DTMF tone within a certain time. The default value for this timeout is 10 seconds, and is

configurable (in seconds) on the voice port. (See the “[Interdigit Timeout](#)” section.) The user can also enter a termination character (#) after entering the full digit string, to indicate that digits are to be collected.

- For local 7-digit calls, add the country code + area code (1 408)

Translation rule 2 takes any 7-digit number that begins with 2 through 9 and adds a 1408 prefix to that number, where 1 is the country code and 408 is the local area code. This translation rule is applied to dial peer 3, which matches any digit pattern that begins with 2 through 9.

- For long distance calls within the United States (different area code), keep the same format

No translation rule is necessary for this case because the digit pattern is already in the desired format. Dial peer 2 is configured with no translation rule applied.

Interdigit Timeout

When the “T” timeout indicator is used at the end of the destination pattern in an outbound voice-network dial peer, the router accepts the specified digits and then waits for an unspecified number of additional digits. The router can collect up to 31 additional digits, as long as the interdigit timeout timer has not expired. When the interdigit timeout timer expires, the router places the call.

The default value for the interdigit timeout is 10 seconds. With this setting, all digits will be collected 10 seconds after the last digit is dialed. For example, if you dial 9195556789, but pause for 11 seconds between digits 8 and 9, only 919555678 will be collected by the GW. You can change the interdigit timeout value using the **timeouts interdigit** command in voice-port configuration mode.

Note that unless the # character is used as a terminator at the end of the **destination-pattern** command, the T-indicator by default adds 10 seconds to each call setup because the call is not attempted until the timer expires. We recommend therefore that you reduce the interdigit timeout value if you use variable-length dial plans, to reduce postdial delay.

The calling party can immediately terminate the interdigit timeout timer by entering the # character while the router is waiting for additional digits. However, if the # character is entered as part of the fixed-length destination pattern that is entered before the router begins waiting for additional digits, it is treated as a dialed digit and is sent across the network when the digits are collected. For example, if the destination pattern is configured as 222...T, the entire string of 222#99 is collected. But if the dialed string is 222#99#99, the #99 at the end of the dialed digits is not collected because the final # character is treated as the dial-peer terminator command.

Dial Peer Preference Command and Failover Options

You can configure failover options on the GW by using multiple dial peers with the **preference** command. The **preference** command allows the GW to select a desired dial peer first, and then, if the GW receives an admission reject (ARJ) message from the GK, the GW selects the next *preferred* dial peer. The default preference value is 0, which is the highest priority. For example, preference 2 is a higher priority than preference 3.

This configuration is commonly referred to as a *rotary dial peer*. This configuration is useful in cases where you want to perform some failover functionality—if the first GW dial peer is not able to resolve the termination, then the next preferred dial peer is used. See the section “[Use of Translation Rules, Technology Prefixes, and Dial Peer Failover Example](#)” for an example of failover functionality.

In the following sample configuration, preference commands are configured on two dial peers; dial peer 1 is tried first, then dial peer 2:

```
dial-peer voice 1 voip
 destination-pattern 1408.....
 session target ras
 preference 1
```

```

!
dial-peer voice 2 voip
 destination-pattern 1408.....
 session target osp
 preference 2

```

Technology Prefixes

Technology prefixes allow special characters to be included in the called number. These special characters are most commonly designated as 1#, 2#, 3#, and so on, and can be configured to prepend the called number on the outgoing VoIP dial peer. The GK can then check its GW technology prefix table for GWs that have registered with that particular technology prefix. Technology prefixes can also be used to identify a type, class, or pool of GWs.

Technology prefix commands can be entered on both GWs and GKs in two places, depending on how you want to design the technology prefix decision intelligence: the GW VoIP interface, or the GW dial peer.

Technology Prefix on the Gateway VoIP Interface

To realize the advantages of the routing efficiencies that technology prefixes provide, the GW needs to identify itself with a technology prefix number, such as 1#, 2#, and so on. This prefix number can be configured on the VoIP interface of the GW, as shown in the following example. Here the GWs register their technology prefix with a registration request (RRQ) message to the gatekeeper. This technology prefix registration determines the GK selection of a GW for an incoming call.

```

hostname gw1
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 h323-gateway voip tech-prefix 2#

```

In this example, GW1 registers to the GK with 2# as the technology prefix. This technology prefix registration determines which GW the GK selects for an incoming call.

You can display this registration on the GK with the **show gatekeeper gw-type-prefix** command:

```

vn-gk# show gatekeeper gw-type-prefix

```

```

GATEWAY TYPE PREFIX TABLE
=====
Prefix: 2#*
  Zone vn-gk master gateway list:
    10.71.3.101:1720 gw1

```

Technology Prefix on the Gateway Dial Peer

You can configure a technology prefix on a specific VoIP dial peer using the following commands:

```

dial-peer voice 1 voip
 destination-pattern 1408.....
 session target ras
 tech-prefix 2#

```

The preceding commands prepend a 2# to the 1408..... called number. A called number of 5554000 then becomes 2#14085554000.

When a call comes in, the GK first looks for a technology prefix match; then it tries to find a zone prefix match. It must find a GW that is registered with that zone prefix and that also matches the zone prefix table. If these two matches occur, then the GK will direct the call to that *egress gateway*.

The following example shows how to configure the technology prefix and how to display it on the GK, along with the technology prefixes that have been registered:

```
hostname vn-gw1
!
interface Ethernet0
 ip address 10.71.3.101 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id vn-gk ipaddr 10.71.3.201 1719
 h323-gateway voip h323-id vn-gw1
 h323-gateway voip tech-prefix 1#
!
hostname vn-gw2
!
interface Ethernet0/0
 ip address 10.71.3.105 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id vn-gk ipaddr 10.71.3.201 1719
 h323-gateway voip h323-id vn-gw2
 h323-gateway voip tech-prefix 2#
!
hostname vn-gk
!
gatekeeper
 zone local vn-gk cisco.com 10.71.3.201
 zone remote k-gk cisco.com 10.71.3.200 1719
 zone remote hopoff cisco.com 10.71.3.202 1719
 zone prefix vn-gk 1212*
 zone prefix k-gk 1212*
!
no shutdown

vn-gk# show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=====
Prefix: 2#*
  Zone vn-gk master gateway list:
    10.71.3.101:1720 vn-gw1

Prefix: 1#*
  Zone vn-gk master gateway list:
    10.71.3.105:1720 12125557777
```

The GK now has vn-gw1 (10.71.3.101) registered with the 1# prefix, and will consider this GW if incoming calls arrive with a 1# prepended to the DNIS. Vn-gw2 is registered with the 2# prefix.



Note

To be placed into the GW selection table on the GK, Cisco Trunking GWs must be configured to register with a technology prefix of 1#. Analog GWs register their full E.164 address, so they do not need to register a technology prefix to the GK.

Technology Prefix Commands on the Gatekeeper

The technology prefix commands described in the following sections are available on the GK to allow additional call control.

Default Technology Prefix

The following commands configure a default technology prefix on the GK:

```
gatekeeper
gw-type-prefix 1# default-technology
```

If no technology prefixes are sent with the called number, this configuration tells the GK to use GWs that are registered with 1#.

Forward LRQ to Hopoff Zone

The following commands configure the GK to receive a particular technology prefix and then forward an LRQ message to the hopoff zone:

```
gatekeeper
gw-type-prefix 7# hopoff spacezone
```

After receiving a called number with 7# preceding it, the device sends an LRQ message to the spacezone GK. The spacezone hopoff GK takes priority over other GW selections.

Static Technology Prefix

The following commands configure the GK with a static technology prefix:

```
gatekeeper
gw-type-prefix 8# gw ipaddr 10.1.1.1
```

This configuration creates a static entry into the GW type prefix table on the GK. It is the equivalent of having a GW (IP address 10.1.1.1) register with an 8#.

Gatekeeper Technology Prefix Commands Example

The following example shows use of the technology prefix commands discussed in the preceding sections:

```
gatekeeper
gw-type-prefix 7#* hopoff spacezone
gw-type-prefix 1#* default-technology
gw-type-prefix 8#* gw ipaddr 10.1.1.1 1720
```

```
vn-gk# show gatekeeper gw-type-prefix
```

```
GATEWAY TYPE PREFIX TABLE
=====
```

```
Prefix: 7#*                               (Hopoff zone spacezone)
  Zone vn-gk master gateway list:
    10.71.3.101:1720 vn-gw1

Prefix: 1#*                               (Default gateway-technology)
  Zone vn-gk master gateway list:
    10.71.3.105:1720 1212555777       (Here, 10.71.3.105 GW has registered with a 1#,
                                        so it belongs to the 1# pool)

Prefix: 8#*                               (Not necessarily currently registered)
  Statically-configured gateways:
    10.1.1.1:1720
```

Figure 7 shows technology prefix configurations. Figure 8 shows the use of technology prefixes in a network.

Figure 7 Technology Prefix Configurations

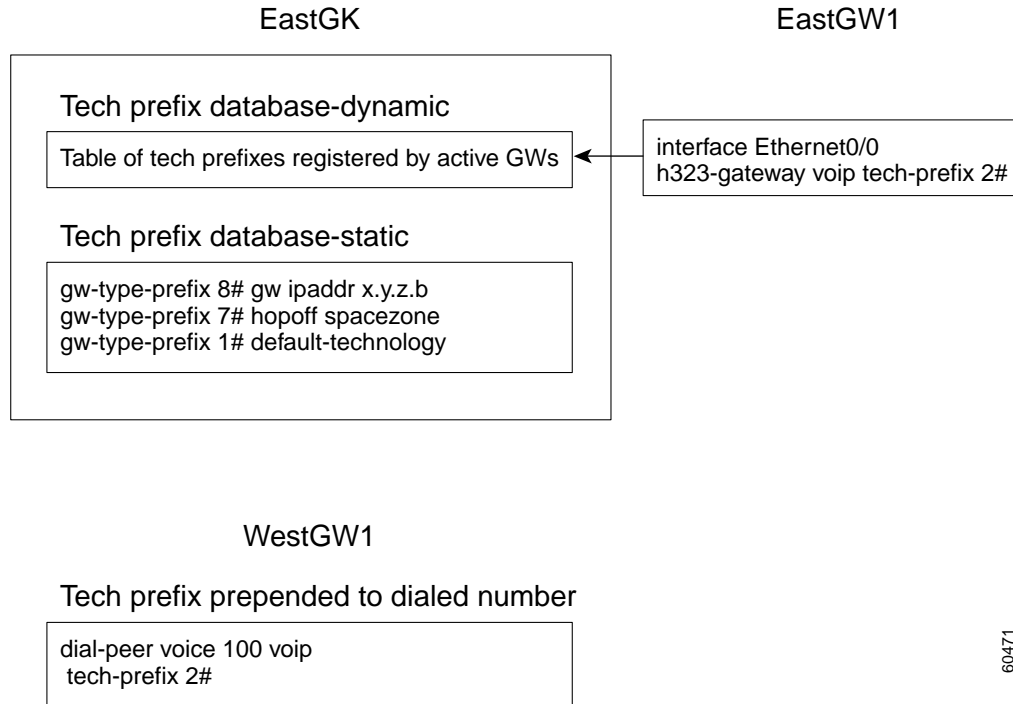
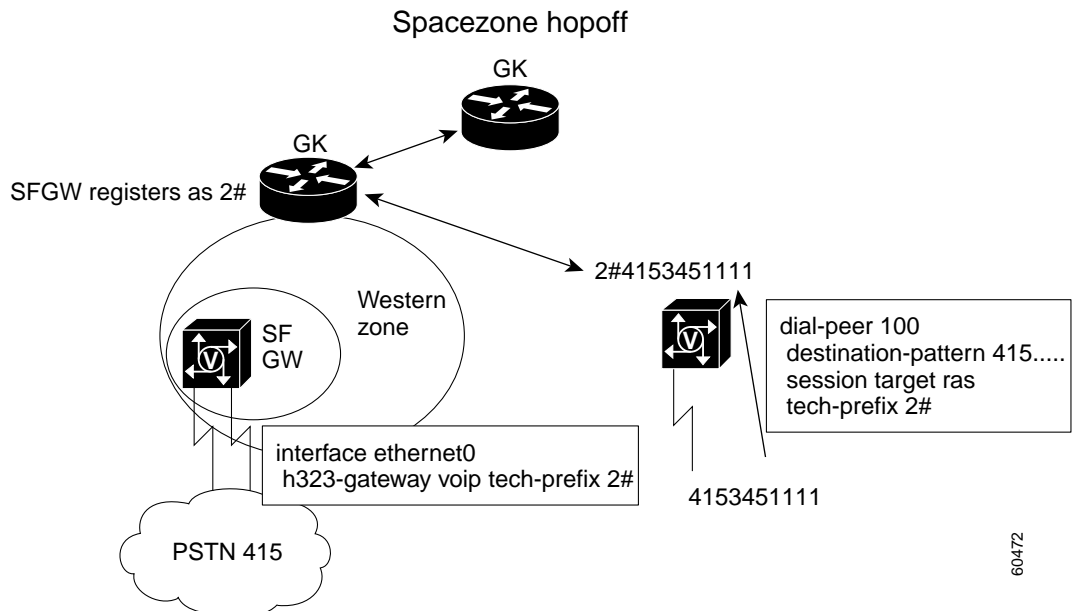


Figure 8 Use of Technology Prefixes in a Network



Note

Normally, when an endpoint or GW sends an ARQ message to its GK, the GK resolves the destination address by first looking for the technology prefix. When the technology prefix is matched, then the GK compares the remaining string against known zone prefixes. If the address resolves to a remote

zone, then the entire address, including both the technology and zone prefixes, is sent to the remote GK in an LRQ message. That remote GK then uses the technology prefix to decide which of its GWs to hop off of. You can override this behavior by associating a *forced hopoff zone* with a particular technology prefix. This association forces the call to the specified zone, regardless of the zone prefix in the address.

Zone Prefixes

A *zone prefix* is the part of a called number that identifies the zone where a call hops off. The zone prefix usually comprises the numbering plan area (NPA), known also as the area code, or the NPA-NXX (area code and local office). Because there is no protocol by which gatekeepers can advertise which zone prefixes can be accessed from their zones, these zone prefixes must be statically configured.

Zone prefixes are typically used to associate an area code or a set of area codes with a particular configured zone. First, local and remote zones are defined on the gatekeeper by the following commands:

```
gatekeeper
zone local west-gk cisco.com 10.1.1.1
zone remote east-gk cisco.com 10.1.1.2 1719
zone remote central-gk cisco.com 10.1.1.3 1719
```

Then, the zone prefixes are configured on the GW to identify which GK manages remote area codes:

```
zone prefix east-gk 312.....
zone prefix west-gk 408.....
zone prefix central-gk 212*
```

Configuring zone prefixes is similar to configuring static routes in an IP environment. Note that currently there is no method for dynamically propagating dial plans to routers in a network. Therefore, you must configure these static zone prefixes to let GKs know where they should forward LRQs to resolve the GW or endpoint IP address.

The purpose of a zone prefix on the GK is to associate an E.164 address to a particular *trunking gateway*. Because the trunking GWs can terminate a range of addresses, the range must be manually defined on the GK.

Another type of endpoint that can register with the GK is an *analog gateway* or H.323 endpoint. These devices typically will register with the full E.164 address. In this case, the zone prefix is used to partition a specific H.323 zone that will manage this set of addresses.

You can display the statically configured zone prefixes on the GK by using the **show gatekeeper zone prefix** command, as follows:

```
NA-GK# show gatekeeper zone prefix
```

```

      ZONE PREFIX TABLE
      =====
GK-NAME          E164-PREFIX
-----          -
east-gk          312.....
west-gk          408.....
Central-gk       212*
```

For a specific zone prefix (range of E.164 addresses), you can configure the GK to hand a call to a specific GW, or pool of GWs, each at configured levels of priority. Note that only currently registered GWs from the priority list will be considered by the GK. GWs that are too busy, as indicated by a resource availability indication (RAI) message, will be excluded from the selection.

You can specify GW priorities ranging from 10 (highest priority) to 0 (usage prohibited) for different zone prefixes within a zone. GW priorities are implemented with the **gw-pri** command, as shown in the following configuration example:

```
router-sj(config-gk)# zone local west-gk cisco.com 10.1.1.1
router-sj(config-gk)# zone prefix west-gk 408..... gw-pri 10 gw408
router-sj(config-gk)# zone prefix west-gk 415..... gw-pri 10 gw415
router-sj(config-gk)# zone prefix west-gk 650..... gw-pri 10 gw650
router-sj(config-gk)# zone prefix west-gk 510.....
```

All three GWs in the example can now register in the same zone. If a zone prefix has any defined GW priorities, a separate GW list is kept for that zone prefix. The list contains all registered GWs, ordered by priority. When a GW is inserted in such a list, a default priority of 5 is used for unnamed GWs.

Zone prefixes that do not have any priorities defined (for example, the 510 area code in the preceding example) do not have any special lists associated with them. Calls to the 510 area code will be serviced out of the master GW list for the zone.

With the preceding configuration, when gw408 registers, it is placed in the 408 list at priority 10, and in the 415 and 650 lists at the default priority of 5. When all three GWs are registered, the zone list will look like the following:

```
resultant Master list
master list: gw408, gw415, gw650
408 list: pri 10 gw408; pri 5 gw650, gw415
415 list: pri 10 gw415; pri 5 gw650, gw408
650 list: pri 10 gw650; pri 5 gw408, gw415
```

Any call to the 408 area code will be directed to gw408 because it has the highest priority. However, if gw408 is busy (for example, it has sent an RAI message saying that it is almost out of resources), the call will be routed to either gw415 or gw650. If you do not want either of these GWs to be used for 408 calls, then you can specify that they have a zero priority for that area code as shown in the following configuration:

```
router-sj(config-gk)# zone prefix west-gk 408..... gw-pri 10 gw408
router-sj(config-gk)# zone prefix west-gk 408..... gw-pri 0 gw415 gw650
```

This configuration ensures that only gw408 will be used for calls to the 408 area code.

You should be aware that GW priority lists come with some overhead costs and that they should be used with discretion. If you can partition your zones to avoid using GW priorities, then you should do so. If you must use this feature, try to keep the number of zone prefixes with priority definitions to fewer than 50 per zone because any GW registering in a zone will need to be inserted into each prioritized list in that zone, and removed from all the lists when it unregisters.

As we have seen, zone prefixes are created to identify particular area codes with zones that have been established. Specific GWs within the zone can be prioritized so that the GK will hand off the call to those GWs first.

Reduction in Postdial Delay

When you design a large-scale dial plan, you should consider the effects of postdial delay in the network. Postdial delay is the time from when the last digit is dialed to the moment the phone rings at the receiving location. GW and GK zone design, translation rules, and sequential LRQs all affect postdial delay. Strive to use these tools most efficiently to reduce postdial delay.

Hopoff Zones

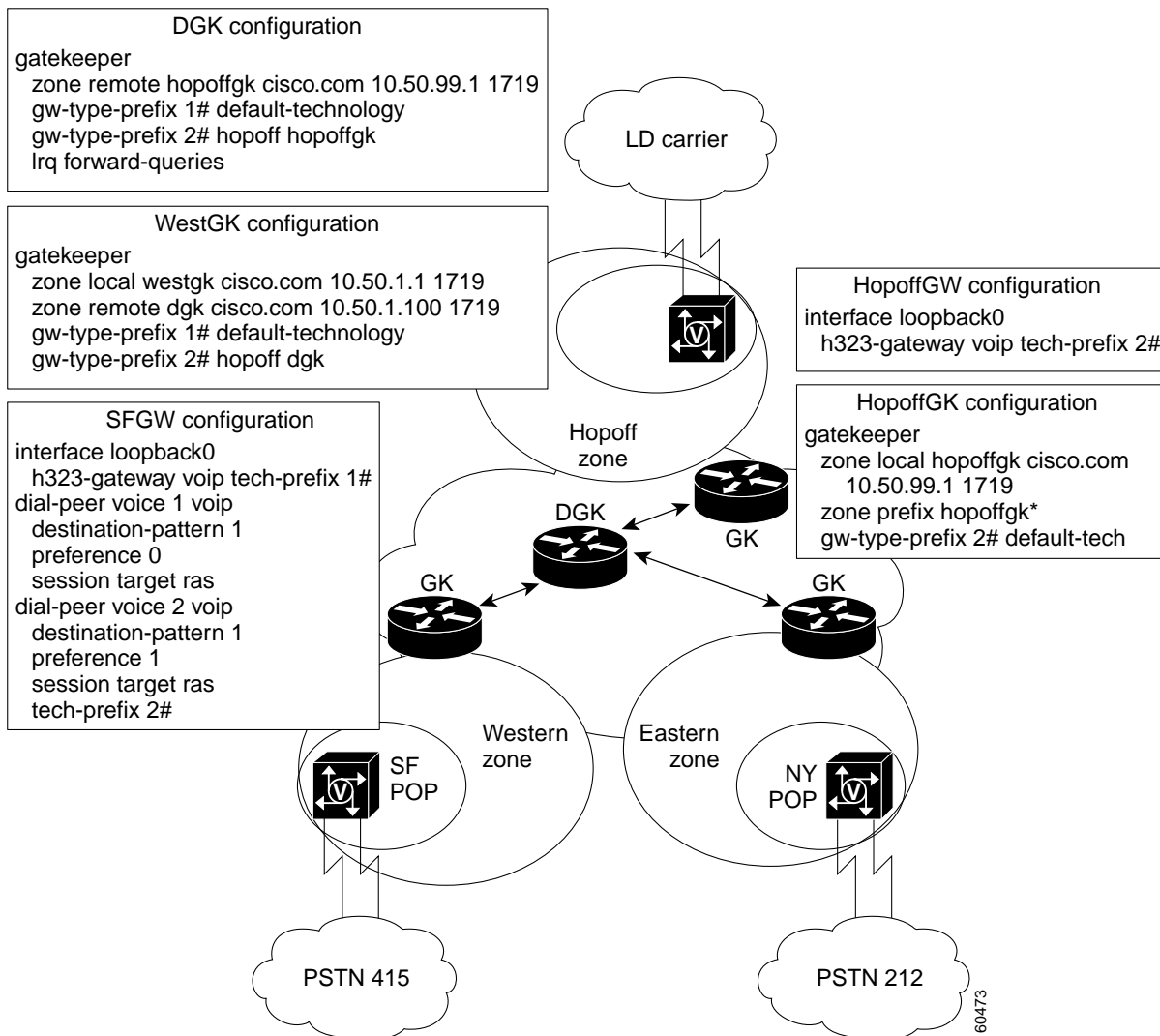
The *hopoff zone* refers to the point where a call makes the transition from H.323 to non-H.323 (for example, PSTN or H.320) via a GW. You can configure a GK to administer a zone dedicated for servicing traffic that is not local. For example, if phone A calls 3155559999, which is outside of the local area codes defined by GK X, then a hopoff zone can be configured to handle such phone numbers. Think of a hopoff zone as a default GW in the IP world.

The hopoff zone is used in conjunction with technology prefixes and is configured as an option with the **gw-type-prefix** command, as shown in the following example:

```
gatekeeper
 gw-type-prefix 2# hopoff hopoffgk
```

This configuration is often referred to as *technology prefix forced hopoff*. An example configuration is depicted in [Figure 9](#).

Figure 9 Application of the Hopoff Zone



60473

In [Figure 9](#), a hopoff zone has been added, consisting of a hopoff GW and a hopoff GK. WestGK and DGK are configured with a static **gw-type-prefix** command. This command will cause all called numbers with a 2# technology prefix to send an LRQ message to their next hopoff GK. In this case, WestGK will forward these LRQ messages to DGK, and DGK will forward them to HopoffGK.

Note that SFGW has been configured with two dial peers. The **preference** command assigns the dial peer order. This command is generally used for failover purposes when you have the same destination pattern assigned to multiple dial peers.

Dial peer 1 first sends an ARQ message to WestGK to determine if it knows the called number terminating GW address. If WestGK does not know the terminating GW address, then WestGK will send an ARJ message to the GW. The second dial peer will then prepend a 2# technology prefix to the called number and again try an ARQ message to WestGK. This time, the 2# matches the **gw-type-prefix 2#** command to hop off to DGK. DGK also recognizes the 2# and matches its **gw-type-prefix 2#** command to hop off to HopoffGK. Note that the 2# gets propagated with the called number.

You can enter the **hopoff** keyword and gatekeeper ID multiple times in the same command to define a group of GKs that will service a given technology prefix. Only one of the GKs in the hopoff list can be local.

If the technology prefix does not have any forced zone attribute, the GK uses *zone prefix matching* to determine the zone. If the matching zone prefix is associated with a remote zone, an LRQ message is sent to the remote GK. The LRQ message contains the entire called number, including the previously stripped technology prefix. If the matching prefix is for a local zone, that zone is used to satisfy the request.

If no zone prefix match is found, the default behavior is to attempt to use a local zone for hopoff rather than to fail the call. However, the default behavior might not be the desired behavior. You may prefer that an ARJ message be returned to the GW so that it can fall through to an alternate dial peer—for example, one that specifies that the next hop is through a special-rate PSTN. To override the default behavior, use the **arq reject-unknown-prefix** command in gatekeeper configuration mode.

Availability and Fault Tolerance

During your dial plan design, you should consider overall network availability and call success rate. Fault tolerance and redundancy within H.323 networks are most important at the gatekeeper level. Use of an alternate GK, sequential LRQs, and Hot Standby Routing Protocol (HSRP) help provide redundancy and fault tolerance in the H.323 network. As of Cisco IOS Release 12.2, GK redundancy can be configured for alternate GKs and HSRP for GKs.

Gatekeepers with HSRP

Because the GK maintains the majority of the call routing intelligence (zone prefix tables, technology prefix tables, and E.164 registrations), the GK should be fault tolerant. You can configure GKs to use HSRP so that when one GK fails, the standby GK assumes its role, as shown in [Figure 10](#).

Configure an active GK and a standby GK to be on the same subnet. Therefore, locate the GKs together. HSRP uses a priority scheme to determine which HSRP-configured router is the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of the other HSRP-configured router. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

HSRP works by the exchange of multicast messages that advertise priority among HSRP-configured routers. When the active router fails to send a hello message within a configurable period, the standby router with the highest priority becomes the active router after the expiration of a hold timer. The

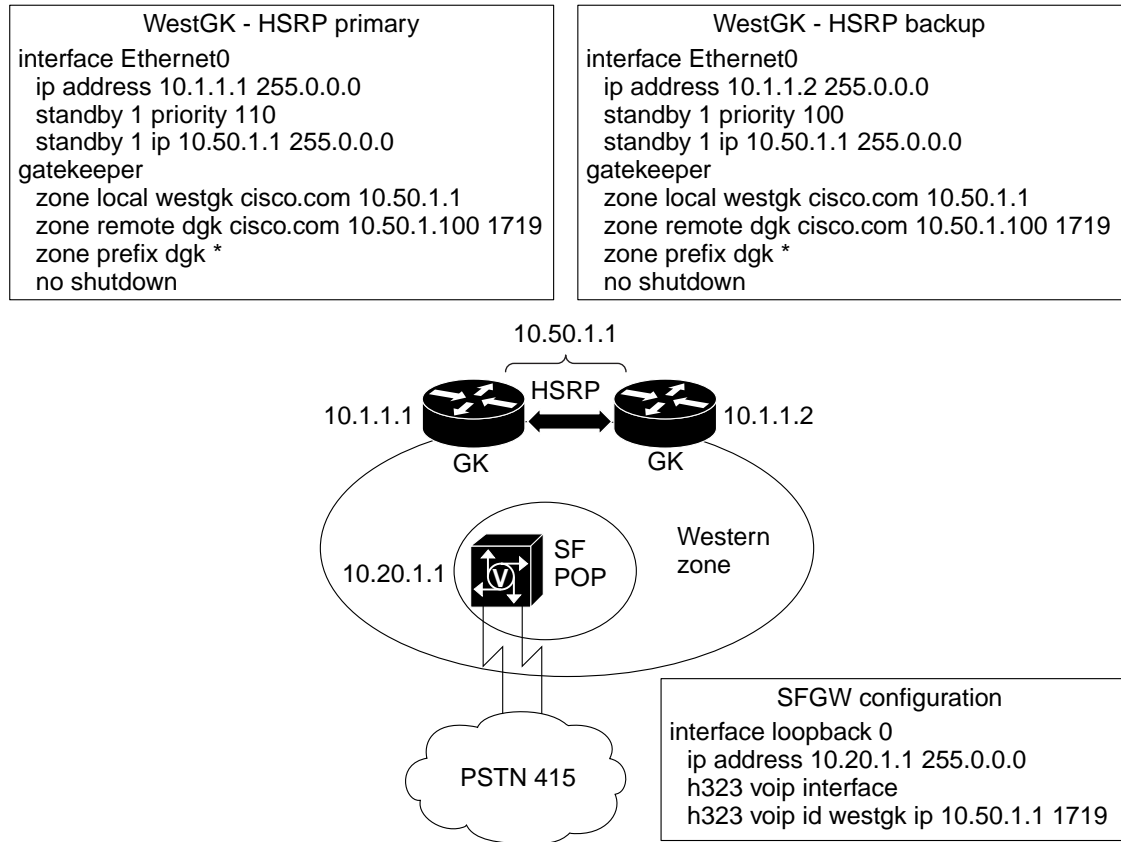
standby timers interface configuration command sets the interval (1 to 255 seconds) between hello messages, and sets the time (1 to 255 seconds) that a router waits before it declares the active router to be down. The defaults are 3 seconds and 10 seconds, respectively. If you decide to modify the default values, you must configure each router to use the same hello time and hold time.



Note

During the time that the active HSRP gatekeeper transfers to the standby HSRP GK, the GK functionality will be lost and will not be able to respond to new LRQs. The secondary directory gatekeeper will address this issue when HSRP is applied to a directory gatekeeper.

Figure 10 HSRP on the Gatekeeper



In Figure 10, notice that a *virtual address* of 10.50.1.1 has been configured on both WestGK and the backup GK. SFGW registers with this virtual address with the **h323 voip id** command.

We recommend the use of HSRP at the DGK level because failover from the primary HSRP DGK to the secondary HSRP DGK will take less time than using an alternate GK as the main backup because of the time required to send sequential LRQs. Later in this document we will discuss the recommended use of a secondary DGK.

Alternate Gatekeepers

In a system where GKs are used, the *alternate gatekeeper* feature provides redundancy. This enhancement allows a GW to use up to two alternate GKs to provide a backup if the primary GK fails. More specifically, you can configure a GW to register with two GKs. If the first GK fails, the alternate GK can then be used for call routing, and will maintain call routing without call failure.

In the following example, the GW is configured to register with two GKs. The default priority is 127 (the lowest priority); 1 is the highest priority.

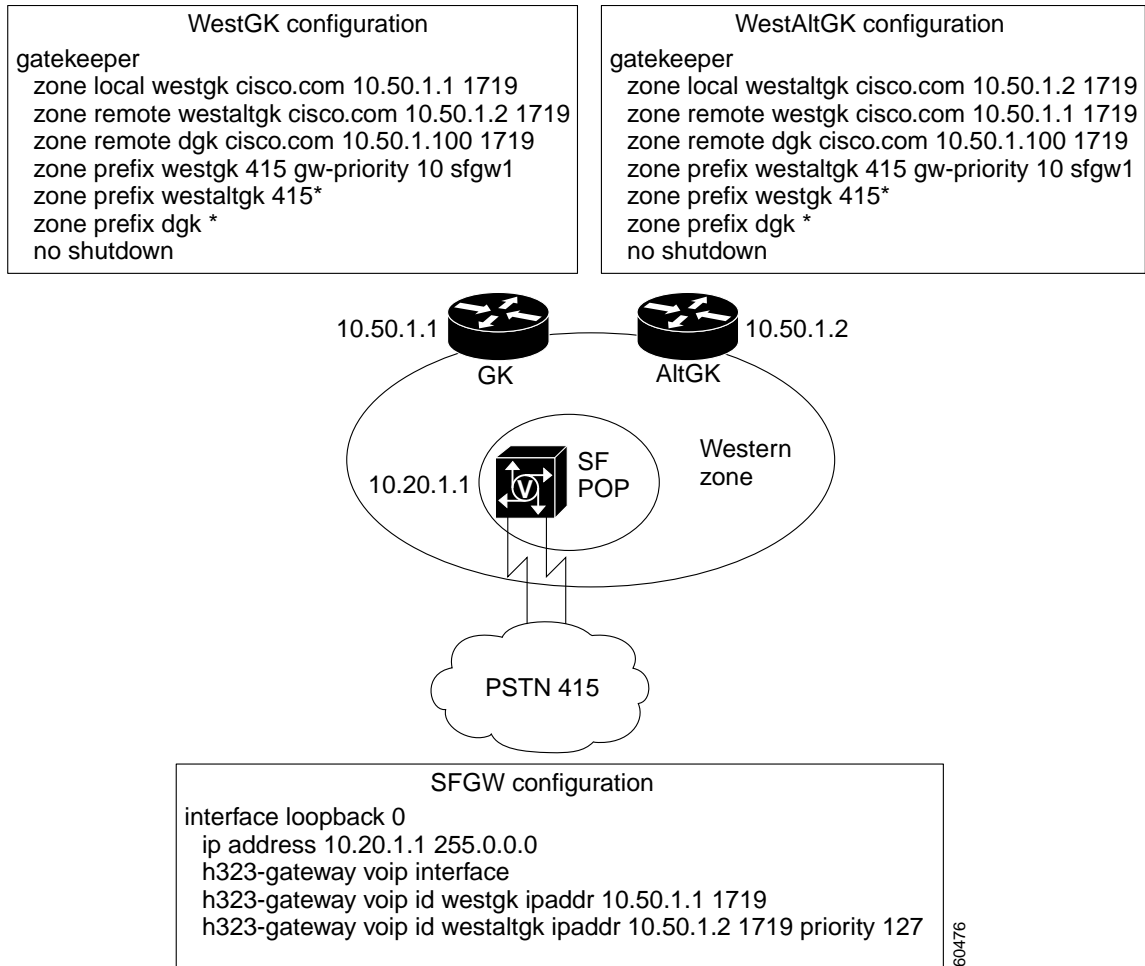
```
interface Ethernet 0/1
 ip address 172.18.193.59 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK1 ipaddr 172.18.193.65 1719 priority 120
 h323-gateway voip id GK2 ipaddr 172.18.193.66 1719
 h323-gateway voip h323-id cisco2
```

In this example, we have configured 172.18.193.65 to be the primary GK, and 172.18.193.66 as the secondary GK.

In [Figure 11](#), note that the configurations on WestGK and WestAltGK are very similar with respect to their local and remote zones. Note that there is an entry **zone prefix westaltgk 415*** on WestGK and **zone prefix westgk 415*** on WestAltGK. These entries become necessary in the situation described as follows.

Suppose you have two GWs at the SF POP that are both registered to WestGK (the primary gatekeeper). WestGK experiences a failure for 30 seconds, then becomes active again. During the 30-second failure, GW1 reregisters to WestAltGK because its 60-second RRQ timer expires. However, the GW2 RRQ timer does not expire within this time window and GW2 remains registered with WestGK. We then have a case where the GWs are registered to two different GKs. The extra zone prefix statement ensures that the GK will check the adjacent GK for GWs that are not registered with it.

Figure 11 Alternate GK on the Zone GKs

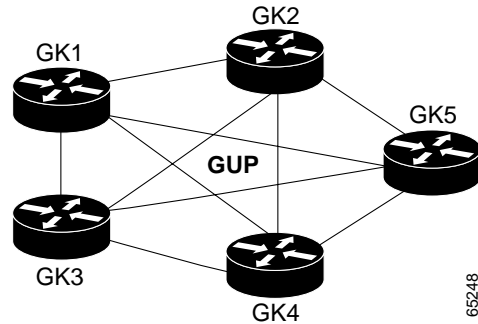


Cisco IOS Release 12.2 introduced a feature that can send LRQs in a sequential fashion instead of in a unicast blast of LRQs. This is a significant advantage over HSRP because backup GKs no longer need to be located in the same geographic area.

Gatekeeper Clusters

Another way to provide GK redundancy and load sharing is to configure GKs in a *cluster*. You can have as many as five GKs in a cluster. Members of a GK cluster communicate with each other by using Gatekeeper Update Protocol (GUP), a Cisco proprietary protocol based on TCP. [Figure 12](#) depicts five GKs in a cluster.

Figure 12 A Gatekeeper Cluster



Each GK in the cluster is configured to know the IP addresses of the member GKs. Upon boot-up, each GK receives a gatekeeper request (GRQ) message from the other GKs. This GRQ message has the alternate GK information embedded in the nonstandard portion of the message. At this point, a GK in a cluster opens a TCP connection with all other GKs in the cluster. GUP updates are sent by each GK at 30-second intervals.

GUP Messages

The following messages are sent by GKs in a cluster:

- **AnnouncementIndication**—Sent periodically, every 30 seconds by default, by each member GK of the cluster. When a GK receives this message, it updates the information about call capacity, endpoint capacity, CPU load, memory usage, number of calls, and number of registered endpoints of the alternate GK (sender).
- **AnnouncementReject**—Sent when there is a configuration mismatch. The receiver will display the error and terminate the GUP connection with the sender.
- **RegistrationIndication**—Sent when the GUP connection is made with a new alternate GK, or when a new endpoint registers with the GK.
- **UnregistrationIndication**—Sent when an endpoint is aged out or the GK is shut down, or when an endpoint unregisters with the GK.
- **ResourceIndication**—Sent when a GK receives an RAI message from the GW.

The GUP Protocol

GUP announcements inform other GKs about a GK memory and CPU utilization, number of endpoints registered, and the used and available bandwidth. The memory and CPU utilization information helps in resource management of the cluster because at any given time any GK in the cluster has the load, CPU, memory, and call capacity information. If this GK is overloaded, it can ask the endpoint to use the resources of the alternate GK with the lowest load.

Each GK gets the registered endpoint information from all other GKs. Thus the information about any endpoint, registered to any GK in a cluster, can be obtained from any member GK, which helps in LRQ processing. Now any GK in the cluster can resolve the LRQ requests sent from an external GK.

When a new endpoint registers with a GK in a cluster, that GK sends a registrationIndication message by GUP. Similarly, an unregistrationIndication message is sent when an endpoint unregisters. If a GK in a cluster does not send six consecutive GUP updates, it is marked as down by all member GKs.

When an endpoint informs a GK about a new call by an information request response (IRR) message, the GK increments the total number of active calls it is monitoring, and sends this data by GUP.

If a GK fails due to a software exception or a power outage, the endpoints are load balanced. Load balancing is achieved during the initial registration confirmation (RCF) message. The initial RCF message contains a list of alternate GKs, listed in order of priority, to which the endpoint can try to register if this (primary) GK does not respond to RAS messages.

When the primary GK fails to respond to registration request (RRQ) messages, the endpoint will then try to register with other GKs in the cluster, in order of priority, as dictated in the RCF. As soon as the endpoint is registered, an information request (IRQ) message is sent by the GK to get the information for all calls currently in progress at the endpoint, ensuring that the call information is not lost because of an outage at the GK.

When a GK resources are overloaded (no more call capacity), it can redirect its endpoints to an alternate GK in the cluster that has sufficient resources. Redirecting endpoints is achieved by sending an ARJ or RRJ reject message in response to an ARQ or RRQ message. The ARJ or RRJ message contains the IP address of the alternate GK to be used. Upon the receipt of this message, the endpoint will then try to register with the new alternate GK and proceed with new call processing.

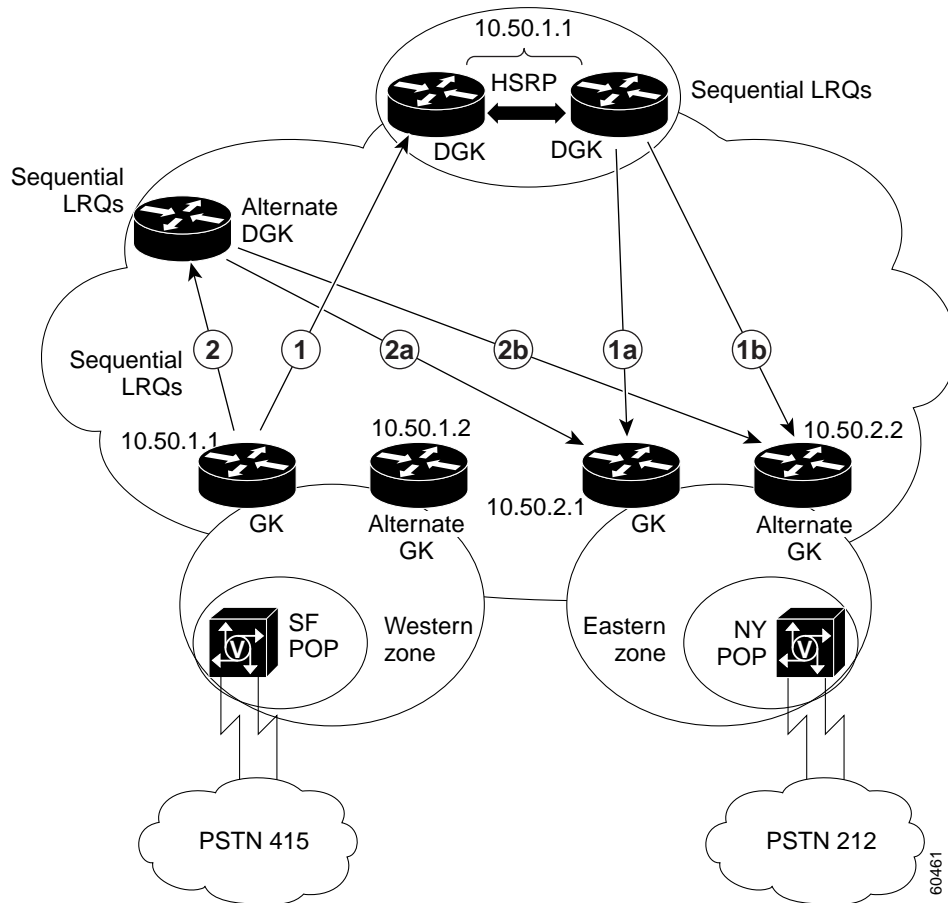
Secondary Directory Gatekeeper

A *secondary directory gatekeeper* can be used to back up another directory gatekeeper by using the *sequential LRQ* feature. For example, if a zone GK sends an LRQ to a primary DGK and fails to receive an LCF, another (sequential) LRQ can be sent from the zone GK to this alternate GK. The secondary DGK will then provide the normal DGK prefix lookup and call routing in the network until the primary DGK is able to function again. We apply this design in the example in [Figure 13](#).

Directory Gatekeeper Design Recommendations

We recommend that you use a combination of the alternate GK, HSRP DGK, and secondary DGK to provide fault tolerance and redundancy in larger H.323 networks. [Figure 13](#) illustrates the network topology.

Figure 13 Fault-Tolerant Design Recommendation



In the network topology shown in [Figure 13](#), fault tolerance and redundancy have been implemented as follows:

- Alternate GK at the zone level

The GWs are configured to register to a primary GK and to an alternate GK in case the primary GK fails. At any given time, a GW might be registered to either its primary or its alternate GK. To accommodate zone fragmentation, you must configure sequential LRQs on the GKs and DGKs because Cisco GKs do not communicate registration states to each other.

- HSRP pair at the DGK level

HSRP is used to provide fault tolerance for the DGK. The HSRP failover time can be configured as specified in the HSRP section of this document. A single virtual IP address is shared between the two HSRP DGKs. Zone GKs need only point to this virtual address.

- Secondary DGK at the DGK level

HSRP failover detection may take some time, during which no calls will be processed. To cover this case, you can configure the local GKs to point to an additional secondary DGK. Use of sequential LRQs at the GK level is required. During this time, calls will still be completed, but with additional postdial delay. The alternate DGK is configured the same as the primary HSRP DGK pair (see messages 2a and 2b later in this section).

The following is the high-level failover flow for the topology shown in [Figure 13](#). Assume that a user in the SF POP calls 12125551000 at the NY POP.

1. LRQ is sent from WesternGK to DGK.
 - 1a. LRQ is sent from DGK to EasternGK, with no response from EasternGK.
 - 1b. LRQ is sent from DGK to EasternAltGK (sequential LRQ).

Either EasternGK or EasternAltGK will send the LCF back to WesternGK, depending on whether there is a 1a or a 1b condition.

Suppose one of the DGKs fails. In this case, assume DGK1 is the primary and it experiences a failure. HSRP will function to activate the secondary, DGK2. Some time will elapse during this failover. During this failover time, no new calls can be processed because neither DGK will respond. To provide redundancy for this interval, use a secondary DGK to receive the LRQ during this time.

The following is the call flow from the Western Zone to the Eastern Zone:

1. LRQ is sent from WesternGK to DGK; no response from DGK (HSRP failover interval).
2. Second LRQ is sent from WesternGK to AltDGK (sequential LRQ).
 - 2a. LRQ is sent from AltDGK to EasternGK; no response from EasternGK.
 - 2b. LRQ is sent from AltDGK to EasternAltGK.

Either the EasternGK or EasternAltGK will send the LCF back to the WesternGK, depending on whether there is a 2a or a 2b condition.

H.323 Network Components in Large-Scale Dial Plans

This section discusses the basic components of an H.323 network and some of the advanced Cisco IOS commands that can be used when large-scale service provider network dial plans are designed. These components are gateways, gatekeepers, and directory gatekeepers.

Gateways in Large-Scale Dial Plans

As the interface between the PSTN and the IP network, a GW is responsible for edge routing decisions. The GW contains the dial peer configuration and normalizes numbers from the PSTN before they enter the IP network, and normalizes numbers from the IP network before they enter the PSTN. The GW registers to a GK for management of its resources by the exchange of RAS messages.

Gatekeepers in Large-Scale Dial Plans

As more VoIP gateways are added to the network, the administration of adding and changing dial peers on all remote VoIP GWs can become unmanageable. You can add a gatekeeper to the gateway-to-gateway network to provide centralized dial plan administration. Gatekeepers allow you to logically partition the network into *zones* and centrally manage the dial plan.



Note

A *zone* is a collection of endpoints, gateways, or multipoint control units (MCUs) registered to a single GK. A single Cisco IOS GK can control several zones. Think of a single GK controlling several zones as several logical GKs coexisting on a single router. The logical GK is identified by a

GK name, which is also the name of the zone. When a Cisco IOS GK is configured, any zone controlled by this router is referred to as a *local zone*. Any zone controlled by a different router is called a *remote zone*.

Without the GK, explicit IP addresses for each terminating GW would need to be configured on the originating GW and matched to a VoIP dial peer. With the GK in place, the remote VoIP GWs simply reference the dial plan on the GK when they are trying to establish VoIP calls with other remote VoIP GWs.

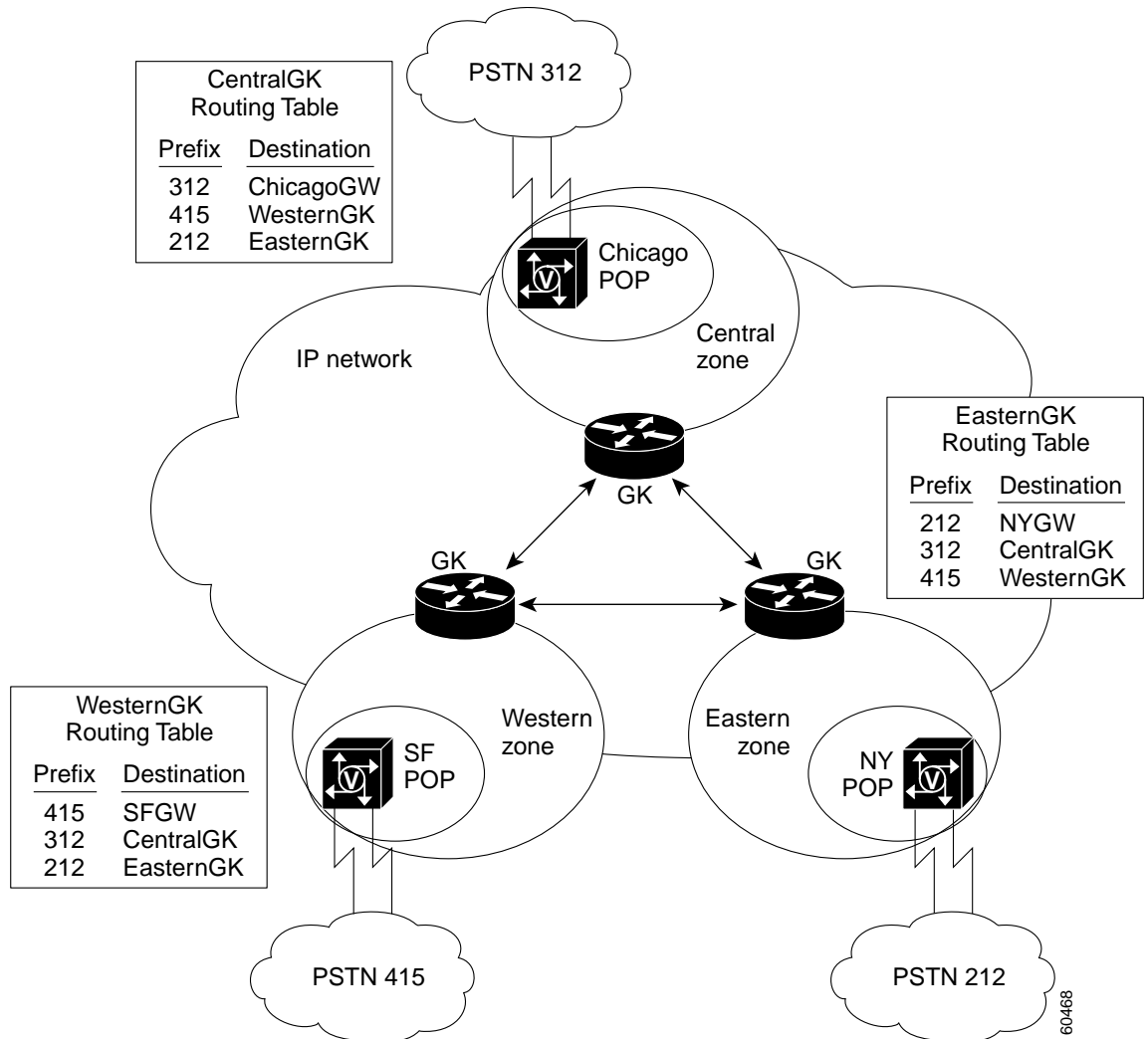
When a GK is added to the network, GWs will register to that GK in the form of an E.164 address, e-mail alias, or H.323 ID. The GK will then maintain the call routing information. GWs can query this information in the RAS ARQ message by pointing the session target to the **ras** keyword. This configuration reduces the number of dial peers necessary on the GW.

For each locally registered GW, the GK has information about which prefixes that GW supports. On the GK, these prefixes are statically defined using the **zone prefix** command. In the United States, area codes are typically represented by the zone prefix. In European countries, prefixes might be represented as a city or zone code. In addition to containing the local prefixes, the GK contains information about the prefixes supported by any remote GKs in the network. The GK is responsible for ultimately providing the terminating GW address to the originating GW. This address can be a local resource, or the GK can query any one of its remote GKs to supply a terminating GW address.

The GK needs to track routing calls that enter the IP cloud. This routing is typically done on E.164 prefixes. The GK must track which GWs service which prefixes, and which prefixes reside on remote GKs, and must maintain resource administration and GW registrations.

[Figure 14](#) illustrates a gatekeeper-to-gatekeeper H.323 network with three GKs. Each GK manages a zone and is responsible for administering calls to its dedicated zone. GWs reside within each zone and register to their respective GKs by RAS messages.

Figure 14 Gatekeeper-to-Gatekeeper Network, Fully Meshed



A static zone prefix table has been configured on each of the GKs in Figure 14. Each GK is configured with the zone prefixes shown in the following configuration:

```
hostname WesternGK
!
gatekeeper
zone local WesternGK cisco.com 10.1.1.1
zone remote CentralGK cisco.com 10.2.1.1 1719
zone remote EasternGK cisco.com 10.3.1.1 1719
zone prefix WesternGK 415* gw-priority 10 SFGW
zone prefix CentralGK 312*
zone prefix EasternGK 212*
!
hostname CentralGK
!
gatekeeper
zone local CentralGK cisco.com 10.2.1.1
zone remote WesternGK cisco.com 10.1.1.1 1719
zone remote EasternGK cisco.com 10.3.1.1 1719
zone prefix CentralGK 312* gw-priority 10 ChicagoGW
zone prefix WesternGK 415*
```

```

zone prefix EasternGK 212*
!
hostname EasternGK
!
gatekeeper
zone local EasternGK cisco.com 10.3.1.1
zone remote CentralGK cisco.com 10.2.1.1 1719
zone remote WesternGK cisco.com 10.1.1.1 1719
zone prefix EasternGK 212* gw-priority 10 NYGW
zone prefix CentralGK 312*
zone prefix WesternGK 415*
!

```

**Note**

The **zone prefix** command is covered in more detail in the “[Zone Prefixes](#)” section of this document.

The following is the call flow for [Figure 14](#). For this example, assume that a phone from SFGW (408-555-1000) calls a phone at the NYGW (212-555-3400).

1. SFGW will send an ARQ message to WesternGK, requesting the NYGW address.
2. WesternGK will look in its zone prefix table to determine if it knows where the 212 prefix resides.
3. From the routing table, WesternGK confirms that 212 area codes reside in EasternGK, so it then sends an LRQ message to EasternGK.
4. EasternGK checks its routing table and confirms that its local zone serves the 212 area code. It also confirms that NYGW is the exact terminating GW for area code 212 phone numbers.
5. EasternGK sends an LCF message containing the NYGW IP address to WesternGK.
6. WesternGK receives this LCF message and sends an ACF message, containing the NYGW address, to SFGW.
7. SFGW sends a RAS setup message to NYGW to begin the peer-to-peer voice communication and RTP stream.

The preceding example shows routers configured for a fully meshed configuration for the routing tables. Each GK must have a static zone prefix configured for each of the adjacent remote zones.

However, this fully meshed configuration does have limitations. If one of the local GKs were to add another prefix or change a prefix, zone prefix changes would need to be made to every GK in the fully meshed network. Likewise, if a new zone or GK were added, all of the GKs would need to reflect this change. Reconfiguring these GKs would be an administrative burden every time one of these changes occurred.

Directory Gatekeepers in Large-Scale Dial Plans

Directory gatekeepers simplify the provisioning of large networks. They allow you to confine the configuration requirements to a local area without needing to provision the entire network for local changes. Confining configuration requirements to a local area is especially important in networks where local numbers might change more often compared to the general country dial plan. For example, if exchanges are added or rate centers change, these configurations can be isolated to the local area and not propagated through the rest of the network.

Figure 15 shows the fully meshed network from Figure 14 with a DGK added. Notice that each local GK needs to be configured only with its local information. The rest of the network is “star-routed” out of the DGK for resolution. This configuration allows the GKs to be aware of only their own local changes, and isolates the rest of the network from needing to cope with any local changes. The DGK is the only device that needs to know the overall dial plan.

The concept is similar to a Frame Relay WAN. Suppose you need to configure a fully meshed network with many dialer maps pointing to each of the adjacent routers in the cloud. By using the Frame Relay hub and spoke configuration, you can have all of the traffic flow through a hub router to get to the adjacent routers. You need only configure dialer maps to the hub router.

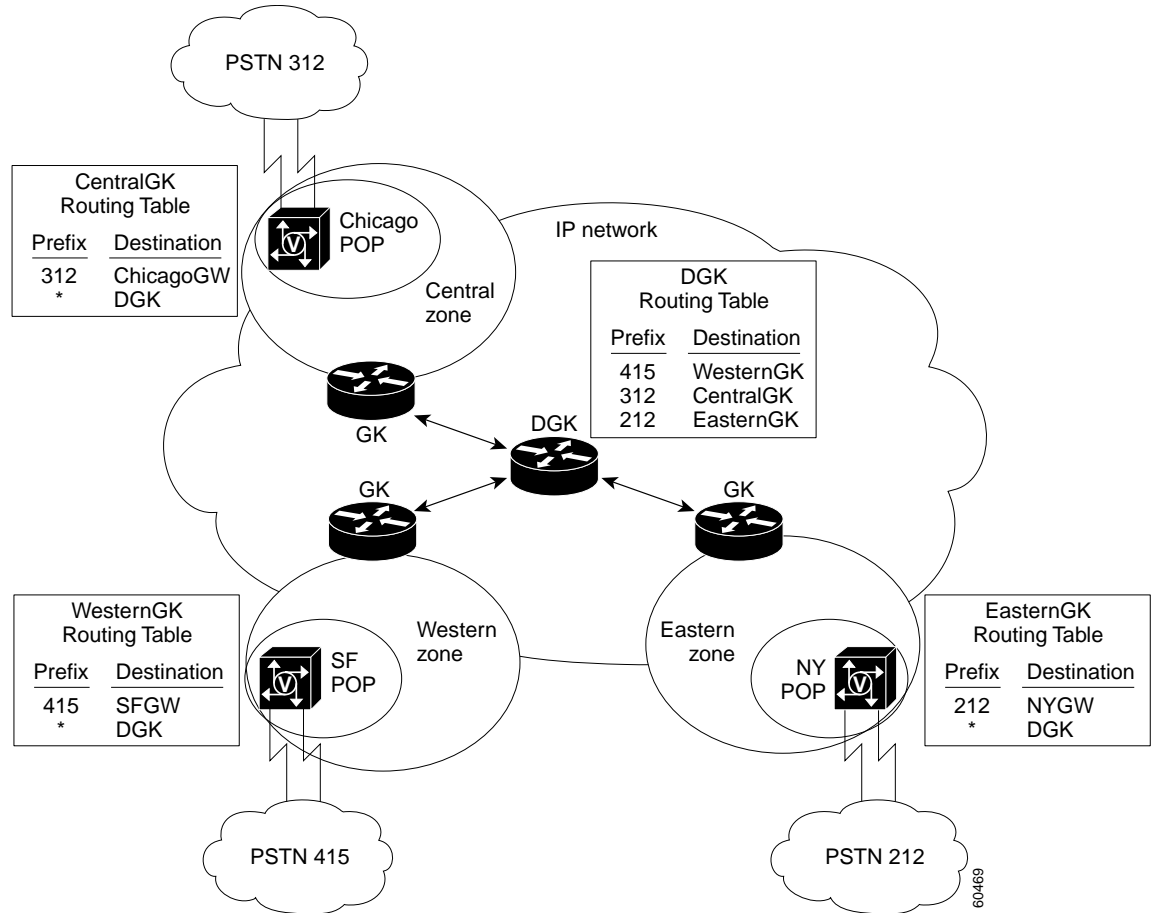
The same concept can be applied in H.323 networks with the introduction of the DGK. The DGK will be the hub for the zone prefix routing tables. The remote GKs need to configure only their local zone prefixes and a wildcard (*) default route to the DGK.

By adding the DGK, we have generated a hierarchical structure with the DGK as the highest level component. We are still able to achieve full connectivity, but with a minimum number of remote zone entries on each of the GKs. The bulk of the remote zone configuration is performed on the DGK.

A large service provider network should be divided into various regions to support scaling issues with performance and management. Each regional GK is responsible for maintaining GW registrations within its region in addition to making the final routing decisions for the terminating and originating GWs. The DGKs are responsible for interzone communication across GK regions and for selecting the proper zone in which to terminate the call.

In Figure 15, WesternGK knows of local area code 415, and EasternGK is responsible for its own area code 212 within its local zone. Using zone prefix commands, a routing table is statically configured on each GK. For area codes local to that particular GK, the actual GW can be configured to match the local area code. For area codes that are remote (not within that GK), use a “star route” or a zone prefix wildcard (*) to the DGK. The DGK will now maintain the master zone prefix table.

Figure 15 Addition of a Directory Gatekeeper



The static zone prefix table on each of the GKs has been simplified from Figure 14. The zone GKs and DGK are now configured as shown in the following configuration:

```
hostname WesternGK
!
gatekeeper
 zone local WesternGK cisco.com 10.1.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix WesternGK 415* gw-priority 10 SFGW
 zone prefix DGK *
!
hostname CentralGK
!
gatekeeper
 zone local CentralGK cisco.com 10.2.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix CentralGK 312* gw-priority 10 ChicagoGW
 zone prefix DGK *
!
hostname EasternGK
!
gatekeeper
 zone local EasternGK cisco.com 10.3.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix EasternGK 212* gw-priority 10 NYGW
 zone prefix DGK *
```

```

!
hostname DGK
!
gatekeeper
zone local DGK cisco.com 10.4.1.1
zone remote WesternGK cisco.com 10.1.1.1 1719
zone remote CentralGK cisco.com 10.2.1.1 1719
zone remote EasternGK cisco.com 10.3.1.1 1719
zone prefix WesternGK 415*
zone prefix CentralGK 312*
zone prefix EasternGK 212*
lrq forward-queries

```

To enable a GK to forward LRQ messages that contain E.164 addresses that match zone prefixes controlled by remote GKs, use the **lrq forward-queries** command in gatekeeper configuration mode in the gatekeeper configurations.

Directory Gatekeeper Performance

On average, the DGK requires 25 percent of the CPU needed by the local zone GKs. Therefore, if the CPU load on the GK is 40 percent, then you need only 10 percent CPU allocation on the DGK. Cisco IOS software has a limit of five recursive LRQs; an LRQ is limited to five hops. Local zones and LRQ forwarding zones can be mixed.

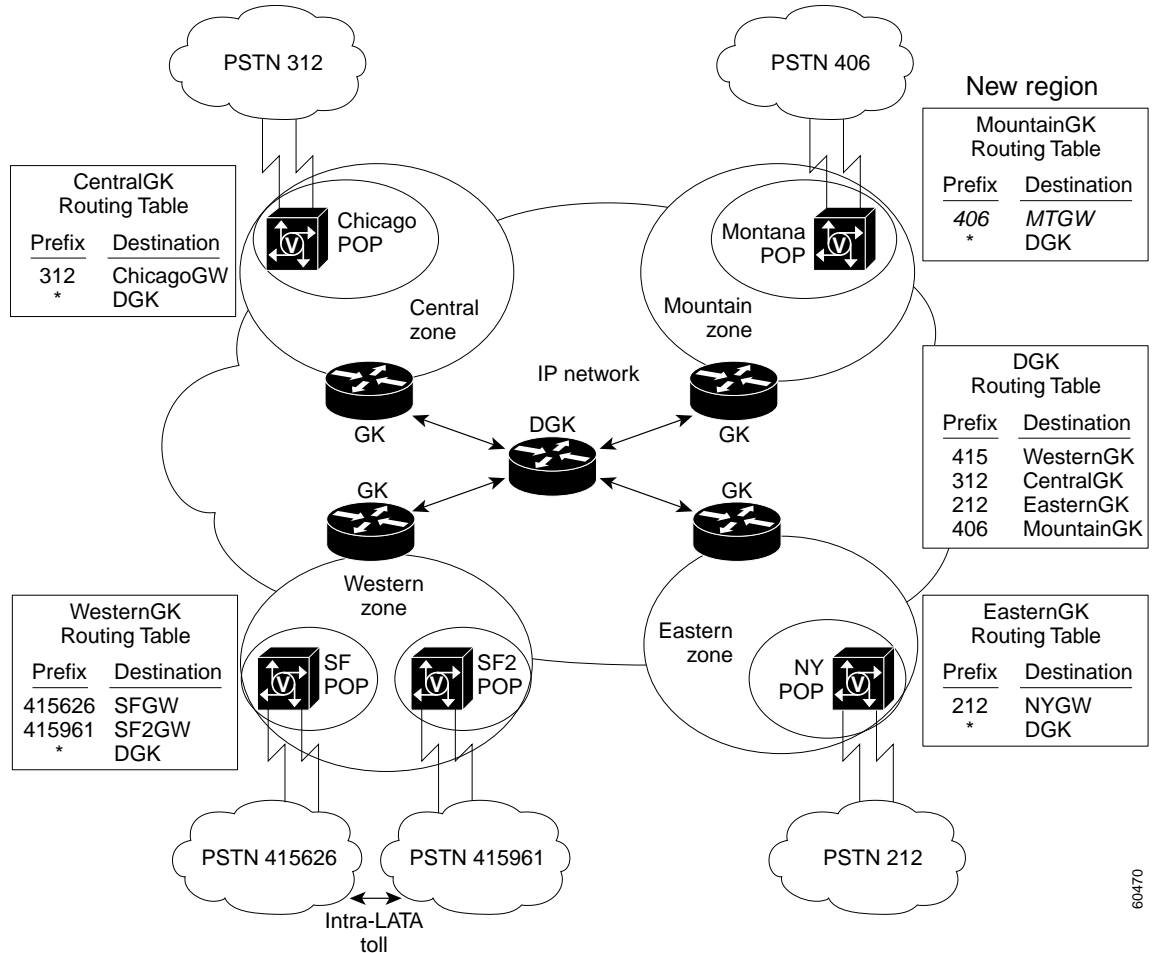
Adding a New Zone and a New Rate Center Example

Suppose you are a service provider that provides VoIP transport for users in San Francisco, Chicago, and New York. The business is growing and you want to design your dial plan to accommodate the following changes:

- Add a new region in the Mountain time zone to service area code 406.
- Add a new rate center in the San Francisco area.

San Francisco has added a new set of local numbers in the 415 area code. However, toll charges in the PSTN are applied when callers with 415-626-xxxx numbers call subscribers with 415-961-xxxx numbers. It is less expensive for users to use the VoIP transport than the PSTN when making these calls. [Figure 16](#) depicts the addition of the new region and the new rate center.

Figure 16 Adding a Rate Center and a New Mountain Zone into the Network



60470

In the following configuration example, a new zone (Mountain zone) and a new rate center (San Francisco) are added:

```
hostname WesternGK
!
interface Ethernet0/0
 ip address 172.19.49.168 255.255.255.192
!
gatekeeper
 zone local WesternGK netman.com 172.19.49.168
 zone remote DGK netman.com 172.19.49.190 1719
 zone prefix WesternGK 1415626* gw-priority 10 SFGW
 zone prefix WesternGK 1415961* gw-priority 10 SF2GW
 zone prefix DGK *
 gw-type-prefix 1#* default-technology
 lrq forward-queries
 no shutdown
```

DGK Configuration

```
gatekeeper
 zone local DGK netman.com 172.19.49.190
 zone remote WesternGK netman.com 172.19.49.168 1719
 zone remote CentralGK netman.com 172.19.49.172 1719
```

```
zone remote EasternGK netman.com 172.19.49.176 1719
zone remote MountainGK netman.com 172.19.49.200 1719
zone prefix WesternGK 1415*
zone prefix CentralGK 1312*
zone prefix EasternGK 1212*
zone prefix MountainGK 1406*
lrq forward-queries
no shutdown
```

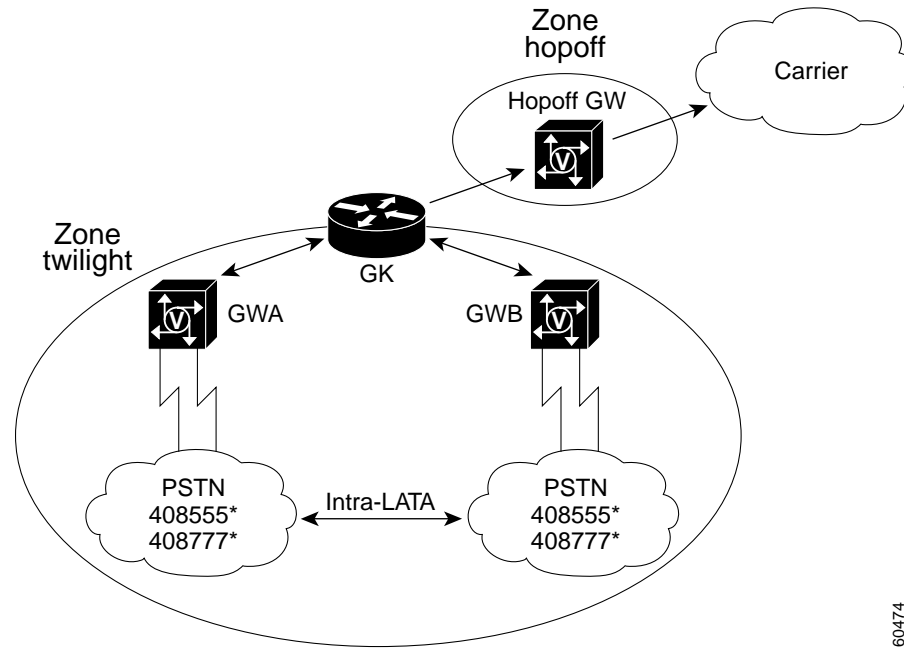
MountainGK Configuration

```
hostname MountainGK
!
interface Ethernet0/0
 ip address 172.19.49.200 255.255.255.192
!
!
gatekeeper
 zone local MountainGK netman.com 172.19.49.168
 zone remote DGK netman.com 172.19.49.190 1719
 zone prefix MountainGK 1496* gw-priority 10 MTGW
 zone prefix DGK *
 gw-type-prefix 1#* default-technology
 lrq forward-queries
 no shutdown
```

Use of Translation Rules, Technology Prefixes, and Dial Peer Failover Example

This example demonstrates the use of Cisco IOS tools and features to provide better call-routing control with hierarchical design, and to minimize dial peer configuration. [Figure 17](#) illustrates the topology of the example network.

Figure 17 Example Network Using Failover Scenarios



60474

Business Case

In this example, the service provider has two GWs that serve both the 408555* and the 408777* NPA-NXX zones. The GK has two local zones, twilight and hopoff.

Calls from GWA to GWB should be made through the gatekeeper VoIP network. However, if GWB is unavailable because of failure or a resource allocation issue, you should make the following provisions:

- Calls to 408555* should be hairpinned back through the PSTN (GWA POTS) and completed to the destination. These calls through the PSTN do not incur any intra-LATA toll charges.
- Calls to 408777* should be sent through to the hopoff zone, not to the PSTN. There is an intra-LATA toll charge associated with these calls, so the customer wants to redirect these calls to the hopoff zone, which has a better rate.

Cisco IOS Tools

The following tools are used in this example:

- Translation rules: Use translation rules to strip or add a 1 to the calling number to allow additional call-routing control in the GW selection order.
- Preference command: Use the **preference** command on dial peers to allow a dial peer selection order. For instance, the gateway will match first on dial peer 1. If the GW receives a location reject (LRJ) message from the GK, the next preferred dial peer will be used. Use of the **preference** command will allow for failover scenarios and greater call control.
- Technology prefixes: Use technology prefixes to allow certain dial peers to use a hopoff zone technology prefix (that is, 27#). When dial peer failover occurs, the 27# technology prefix will force the call to go to the hopoff zone.

- Hopoff zone: Create a hopoff zone and a hopoff GW within the network. This zone has a special negotiated rate for VoIP calls, so the calls cost less than those going through the PSTN.

Example Configurations

The following configurations show the use of translation rules, technology prefixes, and dial peer failover:

GWA Configuration

```
hostname GWA
!
translation-rule 1
  Rule 0 ^2.% 12
  Rule 1 ^3.% 13
  Rule 2 ^4.% 14
  Rule 3 ^5.% 15
  Rule 4 ^6.% 16
  Rule 5 ^7.% 17
  Rule 6 ^8.% 18
  Rule 7 ^9.% 19
!
translation-rule 2
  Rule 0 ^12.% 2
  Rule 1 ^13.% 3
  Rule 2 ^14.% 4
  Rule 3 ^15.% 5
  Rule 4 ^16.% 6
  Rule 5 ^17.% 7
  Rule 6 ^18.% 8
  Rule 7 ^19.% 9
!
interface loopback0
  h323-gateway voip interface
  h323-gateway voip id GK ipaddr 172.20.10.9 1719
  h323-gateway voip h323-id GWA
  h323-gateway voip tech-prefix 1#
!
voice-port 0:D
  translate called 1
  no modem passthrough
!
dial-peer voice 2 voip
  preference 5
  destination-pattern 1408.....
  session target ras
  tech-prefix 27#
!
dial-peer voice 100 pots
  destination-pattern .....
  direct-inward-dial
  port 0:D
  prefix 1408
!
dial-peer voice 1 voip
  preference 1
  destination-pattern 1408.....
  translate-outgoing called 2
  session target ras
```

GWB Configuration

```

hostname GWB
!
interface loopback0
 h323-gateway voip interface
 h323-gateway voip id GK ipaddr 172.20.10.9 1719
 h323-gateway voip h323-id GWB
 h323-gateway voip tech-prefix 1#

```

Hopoff GW Configuration

```

hostname hopoff-gw
!
interface loopback0
 h323-gateway voip interface
 h323-gateway voip id GK ipaddr 172.20.10.9 1719
 h323-gateway voip h323-id hopoff-gw

```

GK Configuration

```

hostname GK
!
gatekeeper
 zone local twilight-zone cisco.com 172.20.10.10
 zone local hopoff-zone cisco.com
 zone prefix twilight-zone 408555* gw-priority 10 GWB
 zone prefix twilight-zone 408555* gw-priority 5 GWA
 zone prefix twilight-zone 408777* gw-priority 10 GWB
 zone prefix twilight-zone 408777* gw-priority 0 GWA
 zone prefix hopoff-zone 1408777* gw-priority 10 hopoff-gw
 gw-type-prefix 1#* default-technology
 gw-type-prefix 27#* hopoff hopoff-zone
 no shutdown

```

GK# **show gatekeeper gw-type-prefix**

GATEWAY TYPE PREFIX TABLE

=====

Prefix: 1#* (Default gateway-technology)

Zone twilight-zone master gateway list:

172.20.10.3:1720 GWA

172.20.10.5:1720 GWB

Zone twilight-zone prefix 408777* priority gateway list(s):

Priority 10:

172.20.10.5:1720 GWB

Zone twilight-zone prefix 408555* priority gateway list(s):

Priority 10:

172.20.10.5:1720 GWB

Priority 5:

172.20.10.3:1720 GWA

Prefix: 27#* (Hopoff zone hopoff-zone)

Zone hopoff-zone master gateway list:

172.20.10.4:1720 hopoff-gw

Zone hopoff-zone prefix 1408777* priority gateway list(s):

Priority 10:

172.20.10.4:1720 hopoff-gw

Configuration Review and Dial Plan Logic

This section shows the following flows:

- GWA calls 1408555* on GWB—Success
- GWA calls 1408555* on GWB—Failover through zone prefixes
- GWA calls 1408777* on GWB—Success
- GWA calls 1408777* on GWB—Failover using dial peer failover (**preference** command)

Flow 1: Success

GWA calls 1408555* on GWB:

1. Voice-port translation rule 1 adds 1 to the NPA.
2. Match dial peer 1 translation rule 2, which strips the digit 1. Send an ARQ message to the GK.
3. Match zone prefix twilight-zone 408555* gw-priority 10 GWB.

The call is successful through VoIP.

Flow 2: Failover Through Zone Prefixes

GWA calls 1408555* on GWB:

1. Voice-port translation rule 1 adds 1 to the NPA.
2. Match dial peer 1 translation rule 2, which strips the digit 1. Send an ARQ message to the GK.
3. Match zone prefix twilight-zone 408555* gw-priority 10 GWB.
4. GWB is down (or RAI unavailable), so GWB is removed from the GK selection table. Look for the next match.
5. Match zone prefix twilight-zone 408555* gw-priority 5 GWA.
6. Select GWA (itself).
7. Match on POTS dial peer, and destination pattern
8. Hairpin the call back through the PSTN.

The call is successful through the PSTN.

Flow 3: Success

GWA calls 1408777* on GWB:

1. Voice-port translation rule 1 adds 1 to the NPA.
2. Match dial peer 1 translation rule 2, which strips the digit 1. Send an ARQ message to the GK.
3. Match zone prefix twilight-zone 408777* gw-priority 10 GWB.

The call is successful through VoIP.

Flow 4: Failover Using Dial Peer Failover (preference Command)

GWA calls 1408777* on GWB:

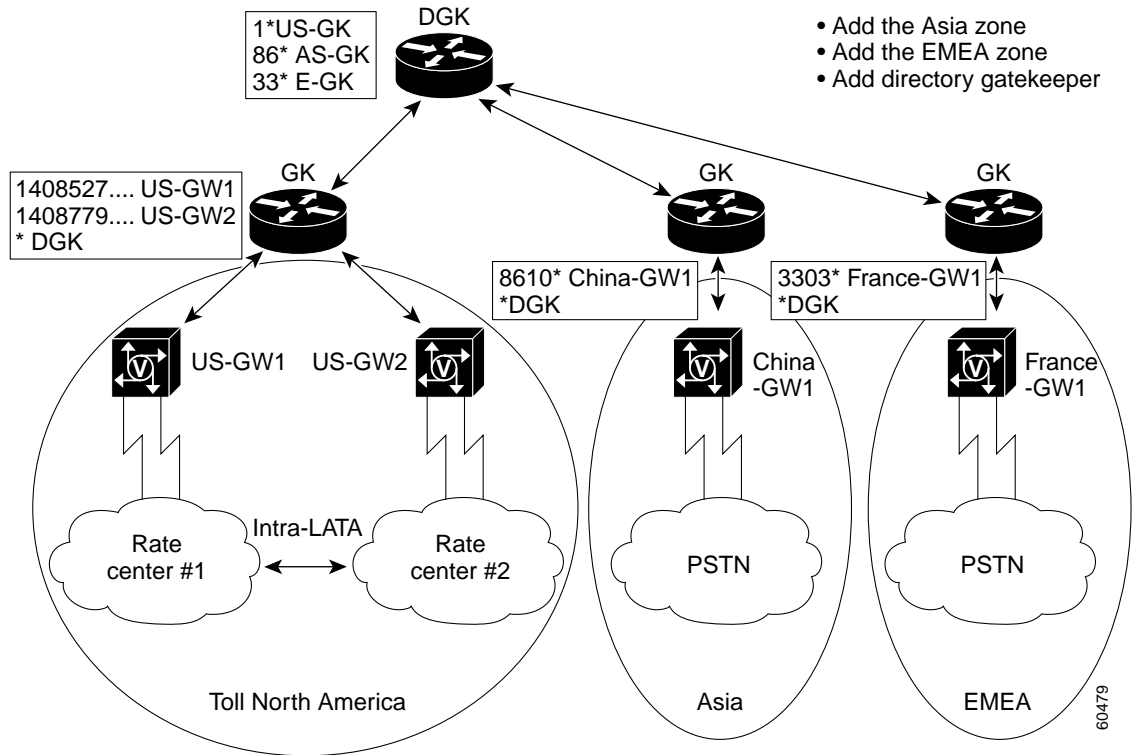
1. Voice-port translation rule 1 adds 1 to the NPA.
2. Match dial peer 1 translation rule 2, which strips the digit 1. Send an ARQ message to the GK.
3. Match zone prefix twilight-zone 408777* gw-priority 10 GWB.
4. GWB is down (or RAI unavailable), so GWB is removed from the GK selection table. Look for the next match.
5. Match, but zone prefix twilight-zone 408777* gw-priority 0 GWA.
6. The GK sends an ARJ message to GWA.
7. Roll over to next preferred dial peer, dial peer 2.
8. Dial peer 2 does not strip the 1 (no translation rule) but does add a technology prefix of 27#, resulting in the number 27#14087771000.
9. GWA sends an ARQ message to the GK.
10. Match the gw-type-prefix 27#* hopoff hopoff-zone.
11. Match the zone prefix hopoff-zone 1408777* gw-priority 10 hopoff-gw.
12. In an ACF message, the GK sends the hopoff-gw address to GWA.

The call is successful to the hopoff GW.

Implementing an International Dial Plan Example

This implementation provides an example of an international dialing plan using several of the methods covered to reduce dial peer configuration at the GW, simplify prefix searches at the GK, and provide fault tolerance at the GK and the DGK level. [Figure 18](#) depicts the topology of the example network.

Figure 18 Topology of an International Service Provider Network



The service provider wants to provide wholesale voice services with a presence in North America, Asia, and EMEA. You need to design and configure a gateway, gatekeeper, and directory gatekeeper H.323 network that will provide for the following POP locations:

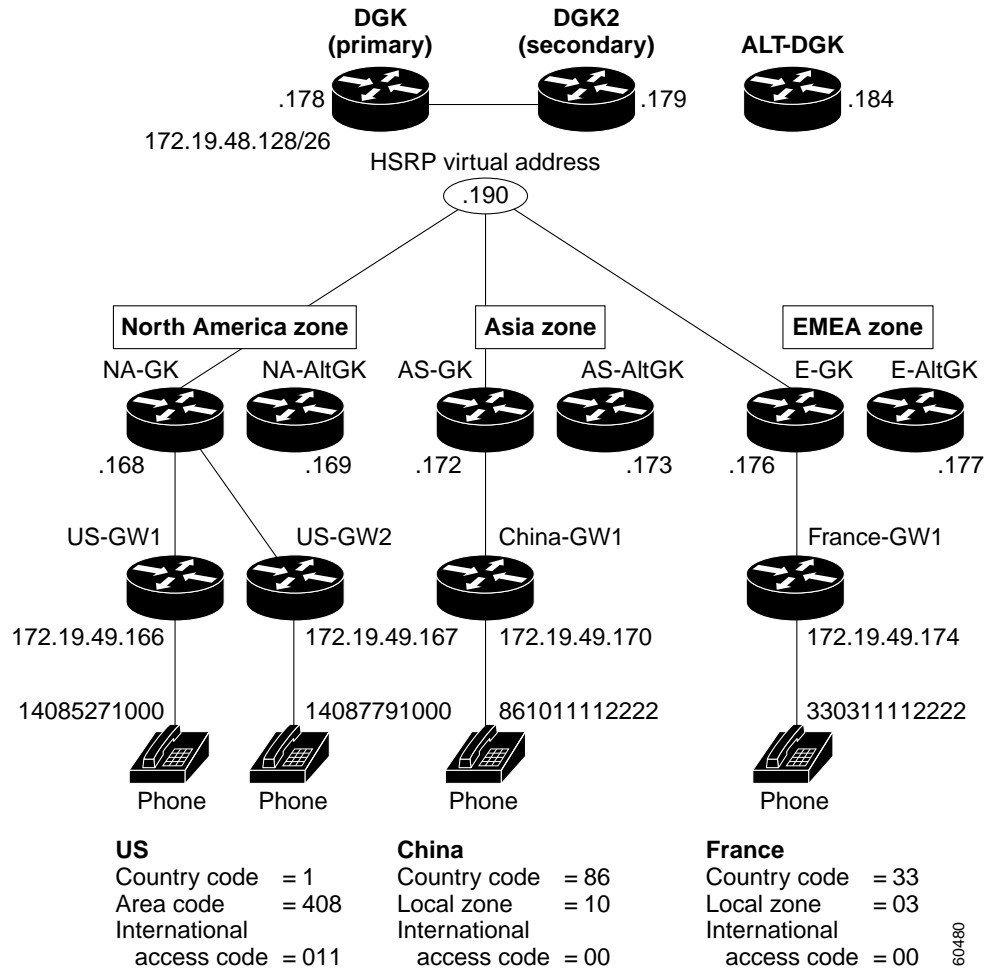
- North America—the GW is in the United States
- Asia—the GW is in China
- EMEA—the GW is in France

The design goals of the network are as follows:

- Successful intercarrier calls between countries
- Hierarchical GW, GK, DGK design
- Number normalization into the VoIP from the PSTN
- Fault tolerance at the GK and DGK level

Figure 19 shows an example topology with these design goals implemented.

Figure 19 Network Topology with Country-Specific Calling Information



To accomplish the design goals of the network, implement the design strategies described in the following sections:

- [Number Normalization to Reduce the Number of Dial Peers on the Gateway](#)
- [Directory Gatekeeper and Local Zone Prefix Search](#)
- [Alternate Gatekeepers and HSRP Pairs for Fault Tolerance](#)

Number Normalization to Reduce the Number of Dial Peers on the Gateway

To reduce the number of GW dial peers, create translation rules on each GW to accommodate the local country dialing habits.

US Gateways

The setup includes the following elements:

- Two GWs are located in the US POP.
- US-GW1 has phone 14085271000.

- US-GW2 has phone 14087791000.

The local dialing habits in the United States are as follows:

- For local numbers in the 408 area code, use 7-digit dialing.
- For long distance numbers within the United States, use 1 + area code + local number.
- For international numbers (outside of North America), use 011 (access code) + country code + local city code + local number.

Normalize these numbers into the following formula:

country code + city code + local number

China Gateway

The setup for China is as follows:

- One GW is located in the China POP.
- The country code = 86, the local city code = 010.
- CHINA-GW1 has phone 861011112222.

The local dialing habits in China are as follows:

- For local numbers in the 010 city code, use 8-digit dialing, beginning with digits 1 to 9.
- For long distance numbers within China, use the area code (dialed with 0x or 0xx) + local number.
- For international numbers (outside of China), use 00 (access code) + country code + local city code + local number.

Normalize these numbers into the following formula:

country code + city code + local number

France Gateway

The setup for France is as follows:

- One GW is located in the France POP.
- The country code = 33, the local city code = 03.
- FRANCE-GW1 has phone 330311112222.

The local dialing habits in France are as follows:

- For local numbers in the 03 area code, use the area code (0x) + 8-digit dialing.
- For long distance numbers within France, use the area code (dialed with 0x) + 8-digit local number.
- For international numbers (outside of France), use 00 (access code) + country code + local city code + local number.

Normalize these numbers into the following formula:

country code + city code + local number

The translation rules should be configured to match the local dialing habits within the country in which the GW resides. Match the translation rule with the appropriate outgoing VoIP dial peer.

Directory Gatekeeper and Local Zone Prefix Search

Gatekeepers are configured to administer their local country zones and city or area codes (for example, 8610*) to their specific GWs. A DGK is used to handle call routing on just the country code number. This hierarchical functionality is possible because the GK applies translation rules to present this country code first, before it enters the VoIP gatekeeper core. In addition, zone prefix tables on the zone GKs are greatly simplified because the DGK has been designed in.

Alternate Gatekeepers and HSRP Pairs for Fault Tolerance

Alternate gatekeepers are configured at the zone GK level to back up the primary GKs. A primary and secondary HSRP pair is used at the DGK level to back up each other. A secondary DGK is used to back up the DGK pair.



Note

The configurations for the alternate GK in the US POP are shown. The configurations for the alternate GK in the Asia and France POPs are not shown.

Configuration Listings

The following are the configurations for implementing the international dial plan:

US-GW1 Configuration

```
Current configuration:
!
! No configuration change since last restart
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname US-GW1
!
enable password xxx
!
username cisco password 0 xxx
!
clock timezone PDT -7
ip subnet-zero
no ip domain-lookup
!
translation-rule 2
  Rule 0 ^2..... 14082
  Rule 1 ^3..... 14083
  Rule 2 ^4..... 14084
  Rule 3 ^5..... 14085
  Rule 4 ^6..... 14086
  Rule 5 ^7..... 14087
  Rule 6 ^8..... 14088
  Rule 7 ^9..... 14089
!
translation-rule 1
  Rule 0 ^0111.% 1
  Rule 1 ^0112.% 2
```

```

Rule 2 ^0113.% 3
Rule 3 ^0114.% 4
Rule 4 ^0115.% 5
Rule 5 ^0116.% 6
Rule 6 ^0117.% 7
Rule 7 ^0118.% 8
Rule 8 ^0119.% 9
!
interface Ethernet0/0
 ip address 172.19.49.166 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719 priority 1
 h323-gateway voip id NA-ALTGK ipaddr 172.19.49.169 1719 priority 2
 h323-gateway voip h323-id US-GW1
 h323-gateway voip tech-prefix 1#
!
 ip classless
 ip route 0.0.0.0 0.0.0.0 172.19.49.129
 no ip http server
!
 voice-port 1/0/0
  timeouts interdigit 3
!
 voice-port 1/0/1
!
 dial-peer cor custom
!
 dial-peer voice 1408 pots
  destination-pattern 14085271000
  port 1/0/0
!
 dial-peer voice 1 voip
  destination-pattern 011T
  translate-outgoing called 1
  session target ras
!
 dial-peer voice 4 voip
  destination-pattern [2-9].....
  translate-outgoing called 2
  session target ras
!
 dial-peer voice 99 voip
  destination-pattern 2601
  session target ipv4:172.19.49.4
!
 dial-peer voice 2 voip
  destination-pattern 1T
  session target ras
!
 gateway
!
 line con 0
  transport input none
 line aux 0
 line vty 0 4
  exec-timeout 0 0
  password xxx
!
end

```

US-GW2 Configuration

```

Current configuration:
!

```

```

version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname US-GW2
!
enable password xxx
!
username cisco password 0 xxx
!
ip subnet-zero
no ip domain-lookup
!
call rsvp-sync
!
translation-rule 1
  Rule 0 ^0111.% 1
  Rule 1 ^0112.% 2
  Rule 2 ^0113.% 3
  Rule 3 ^0114.% 4
  Rule 4 ^0115.% 5
  Rule 5 ^0116.% 6
  Rule 6 ^0117.% 7
  Rule 7 ^0118.% 8
  Rule 8 ^0119.% 9
!
translation-rule 4
  Rule 0 ^2..... 14082
  Rule 1 ^3..... 14083
  Rule 2 ^4..... 14084
  Rule 3 ^5..... 14085
  Rule 4 ^6..... 14086
  Rule 5 ^7..... 14087
  Rule 6 ^8..... 14088
  Rule 7 ^9..... 14089
!
interface Ethernet0/0
  ip address 172.19.49.167 255.255.255.192
  h323-gateway voip interface
  h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719 priority 1
  h323-gateway voip id NA-ALTGK ipaddr 172.19.49.169 1719 priority 2
  h323-gateway voip h323-id US-GW2
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer cor custom
!
dial-peer voice 1 voip
  destination-pattern 011T
  translate-outgoing called 1
  session target ras
!
dial-peer voice 2 voip
  destination-pattern 1T
  session target ras
!
dial-peer voice 1408 pots

```

```

destination-pattern 14087791000
port 1/0/0
!
dial-peer voice 4 voip
destination-pattern [2-9].....
translate-outgoing called 4
session target ras
!
gateway
!
line con 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
password xxx
!
end

```

China-GW1 Configuration

Current configuration:

```

!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CHINA-GW1
!
username cisco password 0 xxx
!
ip subnet-zero
no ip domain-lookup
!
translation-rule 2
Rule 0 ^01.% 8601
Rule 1 ^02.% 8602
Rule 2 ^03.% 8603
Rule 3 ^04.% 8604
Rule 4 ^05.% 8605
Rule 5 ^06.% 8606
Rule 6 ^07.% 8607
Rule 7 ^08.% 8608
Rule 8 ^09.% 8609
!
translation-rule 1
Rule 0 ^001.% 1
Rule 1 ^002.% 2
Rule 2 ^003.% 3
Rule 3 ^004.% 4
Rule 4 ^005.% 5
Rule 5 ^006.% 6
Rule 6 ^007.% 7
Rule 7 ^008.% 8
Rule 8 ^009.% 9
!
interface Ethernet0/0
ip address 172.19.49.170 255.255.255.192
h323-gateway voip interface
h323-gateway voip id AS-GK ipaddr 172.19.49.172 1719
h323-gateway voip h323-id CHINA-GW1
h323-gateway voip tech-prefix 1#
!

```

```

interface Ethernet0/1
  no ip address
  shutdown
  !
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
voice-port 1/0/0
  timeouts interdigit 3
  !
voice-port 1/0/1
  !
dial-peer cor custom
  !
dial-peer voice 1 voip
  destination-pattern 00T
  translate-outgoing called 1
  session target ras
  !
dial-peer voice 2 voip
  destination-pattern 86T
  session target ras
  !
dial-peer voice 3 voip
  destination-pattern 0[1-9]T
  translate-outgoing called 2
  session target ras
  !
dial-peer voice 8610 pots
  destination-pattern 861011112222
  port 1/0/0
  !
gateway
  !
line con 0
  transport input none
line aux 0
line vty 0 4
  exec-timeout 0 0
  password xxx
  !
end

```

France-GW1 Configuration

```

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname FRANCE-GW1
!
no logging console
enable password xxx
!
username cisco password 0 xxx
!
ip subnet-zero
no ip domain-lookup
!
call rsvp-sync

```

```

!
dial-control-mib retain-timer 60
dial-control-mib max-size 1200
!
translation-rule 2
  Rule 0 ^01.% 3301
  Rule 1 ^02.% 3302
  Rule 2 ^03.% 3303
  Rule 3 ^04.% 3304
  Rule 4 ^05.% 3305
  Rule 5 ^06.% 3306
!
translation-rule 1
  Rule 0 ^0011.% 1
  Rule 1 ^0012.% 2
  Rule 2 ^0013.% 3
  Rule 3 ^0014.% 4
  Rule 4 ^0015.% 5
  Rule 5 ^0016.% 6
  Rule 6 ^0017.% 7
  Rule 7 ^0018.% 8
  Rule 8 ^0019.% 9
!
translation-rule 3
  Rule 0 ^001.% 1
  Rule 1 ^002.% 2
  Rule 2 ^003.% 3
  Rule 3 ^004.% 4
  Rule 4 ^005.% 5
  Rule 5 ^006.% 6
  Rule 6 ^007.% 7
  Rule 7 ^008.% 8
  Rule 8 ^009.% 9
!
interface Ethernet0/0
  ip address 172.19.49.174 255.255.255.192
  h323-gateway voip interface
  h323-gateway voip id E-GK ipaddr 172.19.49.176 1719
  h323-gateway voip h323-id FRANCE-GW1
  h323-gateway voip tech-prefix 1#
!
interface Ethernet0/1
  no ip address
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
voice-port 1/0/0
  timeouts interdigit 3
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer cor custom
!
dial-peer voice 3301 pots
  destination-pattern 330311112222
  port 1/0/0
!

```



```

dial-peer voice 1 voip
 destination-pattern 00T
 translate-outgoing called 3
 session target ras
!
dial-peer voice 2 voip
 destination-pattern 0[1-6].....
 translate-outgoing called 2
 session target ras
!
gateway
!
line con 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 password xxx
 login local
!
no scheduler allocate
end

```

NA-GK (North America Gatekeeper) Configuration

```

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname NA-GK
!
no logging console
enable password xxx
!
username cisco password 0 xxx
!
ip subnet-zero
no ip domain-lookup
!
dial-control-mib retain-timer 60
dial-control-mib max-size 1200
!
interface Ethernet0/0
 ip address 172.19.49.168 255.255.255.192
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
snmp-server engineID local 0000000902000001969C63E0
snmp-server community public RW
snmp-server packetsize 4096
!
dial-peer cor custom
!
gatekeeper
 zone local NA-GK netman.com 172.19.49.168

```

```

zone remote NA-ALTGK netman.com 172.19.49.169 1719
zone remote DGK netman.com 172.19.49.190 1719
zone remote ALTDGK netman.com 172.19.49.180 1719
zone prefix NA-GK 1408527* gw-priority 10 US-GW1
zone prefix NA-GK 1408779* gw-priority 10 US-GW2
zone prefix NA-GK 1408*
zone prefix NA-ALTGK 1408*
zone prefix DGK *
zone prefix ALTDGK *
gw-type-prefix 1#* default-technology
lrq forward-queries
no shutdown
!
line con 0
  transport input none
line aux 0
line vty 0 4
  exec-timeout 0 0
  password xxx
  login local
!
no scheduler allocate
end

```

NA-AltGK (North America Alternate Gatekeeper) Configuration

Current configuration:

```

!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname NA-ALTGK
!
enable password xxx
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 172.19.49.169 255.255.255.0
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
no ip http server
!
dial-peer cor custom
!
gatekeeper
 zone local NA-ALTGK netman.com 172.19.49.169
 zone remote NA-GK netman.com 172.19.49.168 1719
 zone remote DGK netman.com 172.19.49.190 1719
 zone remote ALTDGK netman 172.19.49.180 1719
 zone prefix NA-ALTGK 1408527* gw-priority 10 US-GW1
 zone prefix NA-ALTGK 1408779* gw-priority 10 US-GW2
 zone prefix NA-GK 1408*
 zone prefix DGK *
 zone prefix ALTDGK *
 gw-type-prefix 1#* default-technology
 lrq forward-queries
 no shutdown

```

```

!
line con 0
  transport input none
line aux 0
line vty 0 4
  password xxx
  login
!
end

```

AS-GK (Asia Gatekeeper) Configuration

```

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname AS-GK
!
no logging console
enable password xxx
!
username cisco password 0 xxx
!
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0/0
  ip address 172.19.49.172 255.255.255.192
!
interface Ethernet0/1
  no ip address
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
snmp-server engineID local 0000000902000001969C63A0
snmp-server community public RW
!
dial-peer cor custom
!
gatekeeper
  zone local AS-GK netman.com 172.19.49.172
  zone remote DGK netman.com 172.19.49.190 1719
  zone remote ALTDGK netman.com 172.19.49.184 1719
  zone prefix AS-GK 8610* gw-priority 10 CHINA-GW1
  zone prefix DGK *
  zone prefix ALTDGK *
  no shutdown
!
line con 0
  transport input none
line aux 0
line vty 0 4
  exec-timeout 0 0
  password xxx
  login local
!
no scheduler allocate
end

```

E-GK (EMEA Gatekeeper) Configuration

```

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname E-GK
!
no logging console
enable password xxx
!
username cisco password 0 xxx
!
clock timezone PDT -7
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0/0
 ip address 172.19.49.176 255.255.255.192
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
snmp-server engineID local 00000009020000024B8FEF60
snmp-server community public RW
!
dial-peer cor custom
!
gatekeeper
 zone local E-GK netman.com 172.19.49.176
 zone remote DGK netman.com 172.19.49.190 1719
 zone remote ALTDGK netman.com 172.19.49.180 1719
 zone prefix E-GK 3303* gw-priority 10 FRANCE-GW1
 zone prefix DGK *
 zone prefix ALTDGK *
 no shutdown
!
line con 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 password xxx
 login local
!
ntp clock-period 17207746
ntp server 172.19.49.166
no scheduler allocate
end

```

DGK (Directory Gatekeeper—Primary HSRP) Configuration

```

Current configuration:
!
version 12.1
service timestamps debug uptime

```

```

service timestamps log uptime
no service password-encryption
!
hostname DGK
!
enable password xxx
!
ip subnet-zero
!
interface FastEthernet0/0
 ip address 172.19.49.178 255.255.255.192
 duplex auto
 speed auto
 standby 1 priority 110
 standby 1 ip 172.19.49.190
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
no ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
dial-peer cor custom
!
gatekeeper
 zone local DGK netman.com 172.19.49.190
 zone remote NA-GK netman.com 172.19.49.168 1719
 zone remote AS-GK netman.com 172.19.49.172 1719
 zone remote E-GK netman.com 172.19.49.176 1719
 zone remote NA-AGK netman.com 172.19.49.169 1719
 zone prefix NA-GK 1*
 zone prefix E-GK 33*
 zone prefix AS-GK 86*
 lrq forward-queries
 no shutdown
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password xxx
 login

```

DGK2 (Directory Gatekeeper—Secondary HSRP) Configuration

Current configuration:

```

!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname DGK2
!
boot system flash c3640-ix-mz.121-2.T.bin
enable password xxx
!
ip subnet-zero
!
interface FastEthernet0/0
 ip address 172.19.49.179 255.255.255.192

```

```

no ip redirects
duplex auto
speed auto
standby 1 ip 172.19.49.190
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
no ip classless
no ip http server
!
gatekeeper
zone local DGK netman.com 172.19.49.190
zone remote NA-GK netman.com 172.19.49.168 1719
zone remote AS-GK netman.com 172.19.49.172 1719
zone remote E-GK netman.com 172.19.49.176 1719
zone remote NA-AGK netman.com 172.19.49.169 1719
zone prefix NA-GK 1*
zone prefix E-GK 33*
zone prefix AS-GK 86*
lrq forward-queries
no shutdown
!
line con 0
transport input none
line aux 0
line vty 0 4
password xxx
login
!
end

```

ALT-DGK (Secondary Directory Gatekeeper) Configuration

```

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ALT-DGK
!
boot system flash c3640-ix-mz.121-2.T.bin
enable password xxx
!
ip subnet-zero
no ip domain-lookup
!
interface FastEthernet0/0
ip address 172.19.49.184 255.255.255.192
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
no ip classless

```

```
no ip http server
!
gatekeeper
zone local DGK netman.com 172.19.49.190
zone remote NA-GK netman.com 172.19.49.168 1719
zone remote AS-GK netman.com 172.19.49.172 1719
zone remote E-GK netman.com 172.19.49.176 1719
zone remote NA-AGK netman.com 172.19.49.169 1719
zone prefix NA-GK 1*
zone prefix E-GK 33*
zone prefix AS-GK 86*
lrq forward-queries
no shutdown
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password xxx
  login
!
end
```

Related Documents

- *Cisco IOS Voice, Video, and Fax Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/index.htm
- *Cisco IOS Voice, Video, and Fax Command Reference*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_r/index.htm

