Cisco Voice Routing Center User Guide

Version 1.2.1

April 2003

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2497-02

About This Guide

The Cisco Voice Routing Center (VRC) software product is a graphical user interface (GUI) network tool for managing dial plans in a Voice-over-IP (VoIP) network-based system. VRC is used as an integrated product with Packet Telephony Center (PTC). VRC provides basic dial plan provisioning and network configuration.

Document Audience

This guide is intended as a technical resource for service provider and enterprise users who are responsible for managing network dial plans for H.323-based VoIP networks.

Note To use this publication, you should have a basic understanding of network design, operation, and terminology of the Cisco Voice-over-IP technology. You must also be familiar with your own network configurations.

Document Organization

This guide is organized as follows:

Chapter 1, "Introduction," introduces the Cisco Voice Routing Center (VRC) application, provides an overview of its key features, concepts, architecture, and lists most commonly used VRC operations.

Chapter 2, "VRC Client," describes the different ways to access the VRC user interface.

Chapter 3, "Baseline View," provides the baseline dial plan and topology for the entire managed network and allows you to view the baseline dial plan and populate the Baseline View.

Chapter 4, "Design View," describes how to start a new dial plan design and open and modify an existing dial plan design.

Chapter 5, "Managing Dial Plan Components," defines the components of a VRC dial plan, their attributes, and how to use the components.

Chapter 6, "Opening the VRC Console," describes how to access the VRC application from a console and how to use VRC functions through the console.

Appendix A, "Frequently Used VRC Operations," lists VRC functions that you use most often in your environment.

Appendix B, "Troubleshooting Cisco VRC," describes installation error messages and frequently asked installation questions.

Document Conventions

Screen examples use the following conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface` font	Information you must enter is in **boldface** font.
`italic screen` font	Arguments for which you supply values are in *italic* font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

The following is a list of documentation that is related to the Cisco VRC software.

- *Cisco Voice Routing Center Online Help, Software Version 1.2.1*
- *Cisco Voice Routing Center User Guide, Software Version 1.2.1*
- *Release Notes for the Cisco Voice Routing Center Software Version 1.2.1*

The Cisco Packet Telephony Center - Virtual Switch 3.0 documentation can be found at the following URL: www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ptc/3_0.

Documentation for Cisco Packet Telephony Center - Virtual Switch:

- *Documentation Guide for Cisco Packet Telephony Center - Virtual Switch, 3.0*
- *Release Notes for Cisco Packet Telephony Center - Virtual Switch, 3.0*
- *Cisco Packet Telephony Center - Virtual Switch Installation and Configuration Guide, 3.0*
- *Cisco Packet Telephony Center - Virtual Switch User Guide, 3.0*
- *Cisco Packet Telephony Center - Virtual Switch API Reference and Programmer Guide, 3.0*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Introduction

This chapter provides an overview of the Cisco Voice Routing Center (VRC). The Cisco VRC is a graphical user interface (GUI) based network management tool specifically designed for managing dial plans in a Voice-over-IP (VoIP) network.

VRC Version 1.2.1 is targeted for H.323-based networks. H.323 VoIP dial plans are statically configured and managed on gateway and gatekeeper platforms. The infrastructure of a typical H.323 VoIP network includes gateways and gatekeepers.

In a typical service provider network, a number of gateways are deployed at points of presence (POPs) throughout the service provider coverage area. A gatekeeper is used to group these gateways into a logical zone of control and perform all call routing among them.

To simplify dial plan administration for these multiple gatekeeper networks, Cisco introduced the concept of a directory gatekeeper to handle call routing between local gatekeepers.

VRC is a software product that runs on Sun servers and provides a GUI client running within a web browser on PCs running the Windows operating system.

You can deploy VRC to discover the dial plan of an existing network. You can also use it to design new dial plans incorporating Cisco routers running as gateways, gatekeepers, and directory gatekeepers.

The VRC is designed to administer a VoIP network at two levels:

- Administrative Domain (AD)—The highest level of administration which encompasses the entire dial plan. The AD includes all elements that participate in the VoIP call routing.
- Regions—A region partitions the AD. It may contain one or more zones, gatekeeper groups, and directory gatekeepers.

VRC Version 1.2.1 uses CNS security services for user administration and authorization.

The VRC application is a tool for dial plan provisioning including:

- Discovering existing dial plan configurations
- Designing new dial plan configurations
- Validating new dial plan configurations
- Previewing new configurations
- Distributing new configurations to network elements
- Archiving existing dial plans with the ability of restoring an earlier configuration

The VRC application consists of a centralized dial plan management server and web-based clients distributed across an IP network. The server uses a database for storing configuration information and is responsible for all direct interaction with each managed network element. These communications occur using the Cisco IE2100 or over Telnet and HTTP protocols.

When you use VRC integrated with PTC:

- VRC is launched from the PTC user interface.
- Network operations are managed through the PTC Topology Manager. These include adding and deleting regions and network elements from the topology. The VRC Topology view is not accessible from the VRC client.
- When you make changes to a dial plan and commit the design, any topology update, such as adding a gateway to a zone, is automatically reflected in the PTC Topology Manager.
- When you change network elements through PTC, these changes are sent to VRC as events and the elements affected by the change are flagged in the VRC Baseline View and Design View.

Note A dial plan is a numbering plan for voice-enabled networks. Blocks of numbers are assigned to physical lines or circuits and that information is propagated across the network so that a call can be routed from one telephone to another.

Features

Cisco VRC Version 1.2.1 provides support for the following:

- Dial Plan management for H.323 VoIP networks
- Destination number or tech prefix based routing
- Carrier and trunk group label based routing
- Dial peer voice configuration
- Zone configuration
- Directory gatekeeper redundancy mechanisms (alternate, cluster, hsrp)
- Gatekeeper redundancy mechanisms (alternate, cluster, hsrp)
- Arbitrary number of directory gatekeepers, but only single level hierarchy of directory gatekeepers
- Gatekeeper Transaction Message Protocol (GKTMP) triggers configuration on gatekeeper
- Call control security configuration
- Translation rules, number expansions, and call blocking configuration
- Source IP group configuration
- Hairpinning calls to PSTN
- Call path verification
- Network and regional administrators
- User administration through the CNS security module
- Integration with the Packet Telephony Center (PTC)
- Configuration distribution using the Cisco IE2100 or Telnet (speeds up and simplifies dial plan management for a large number of network elements)
- Fifty concurrent users
- Efficient dial plan administration and configuration functions for service provider VoIP networks

Architecture

The VRC is a web-based client/server architecture. The server resides on a Sun platform. It uses MySQL for its database needs and Tomcat for a servlet engine. For user management it uses the Cisco CNS Security module which has an embedded LDAP directory from DCL. The VRC code is implemented in Java and uses the Java 1.3 run-time environment. The client is a Java applet that runs within a standard Internet Explorer Version 5.0 or Version 5.5 web browser.

Note When VRC is integrated with PTC, PTC manages VRC installation, CNS security installation, and topology operations.

VRC provides basic provisioning of dial plans and configuration of the elements in a network and with the VRC. You can also archive and restore dial plans and validate the configuration before downloading it to the elements. The VRC can be deployed in a network with an existing dial plan or it can be used to create new dial plans.

Server Architecture

The VRC server runs on a Sun SPARC platform and requires:

- Sun Solaris 2.7 or 2.8 operating system
- 300 MB disk space

Client Architecture

The VRC client runs within a browser on a Windows PC and requires:

- At least Intel Pentium III
- Microsoft Windows NT4 or Windows 2000 operating system
- Microsoft Internet Explorer 5.0 and 5.5 web browser
- Netscape 7.0 web browser with a PC or Sun client

VRC Feature Sets

VRC uses the Cisco IOS version to determine what command line interface (CLI) it needs to generate to configure a network element. VRC applies the term “feature set” to capture the dial plan capabilities of a Cisco IOS version.

A VRC feature set is made up of a set of Cisco IOS features and a set of rules about how to apply the Cisco IOS features to the network elements to perform dial plan provisioning for the network.

The VRC Version 1.2.1 model supports the following feature sets:

- dp1.0—Supports prefix routing.
- dp1.1—Supports both prefix routing and carrier-sensitive routing. Devices that support dp1.1 support gateway and gatekeeper trunk and carrier-based routing enhancements.
- dp1.2—Supports all dp1.0 and dp1.1 features plus hierarchical directory gatekeepers, data migration, and gateway voice applications.

The feature set for the device depends on the Cisco IOS version running on the device.

Cisco IOS Support

Cisco VRC supports the Cisco IOS versions for gateways (GWs), gatekeepers (GKs), and directory gatekeepers (DGKs) and their corresponding feature sets shown in Table 1-1.

Table 1-1 Supported Cisco IOS Software Versions and Feature Sets

Device Type	VRC Feature Set	Supported Cisco IOS Version
GW	dp1.0	Release 12.2(2)XB*
GW	dp1.0	Release 12.2(2)XA*
GW	dp1.0 and dp1.1	Release 12.2(2)XU*
GW	dp1.0	Release 12.2.7*
GW	dp1.2	Release 12.2(13)T*
GK and DGK	dp1.0	Release 12.2(2)T*
GK and DGK	dp1.0	Release 12.2(2)XA*
GK and DGK	dp1.0 and dp1.1	Release 12.2(2)XU*
GK and DGK	dp1.0 and dp1.1	Release 12.2(11)T*
GK and DGK	dp1.2	Release 12.2(13)T

Denotes all releases of this Cisco IOS version. For example, Release 12.2(2)XB means that the network element supports the following Cisco IOS versions: Release 12.2(2)XB1, Release 12.2(2)XB2, Release 12.2(2)XB3, Release 12.2(2)XB4, and all releases following.

Note If the Cisco IOS version of your device does not match this list, VRC assigns the default feature set of dp1.0 to the network element.

Concurrent Operations

Most VRC operations can occur simultaneously by different users within the VRC server. However, there are certain operations that cannot run concurrently.

VRC concurrent operations constraints include:

- A single user can execute only one operation at a time.
- There can only be one design session open at a time for a given scope.

- Design sessions that originate with the Discovery operation are opened at the Administrative Domain (AD) level.
- No two operations of the same type can be executed simultaneously (exceptions: Design Export and Save Design)

Table 1-2 lists the VRC operations that cannot occur simultaneously.

Table 1-2 VRC Operation Limitations

Operation being executed	Cannot execute simultaneously
Distribution	Check network element
Distribution	Persist element configuration
Commit	Distribution within the same scope
Discovery	Import Topology
Discovery	Element activation or reactivation
Discovery	Design Export
Discovery	Commit
Discovery	Save Design
Design Preview	View generated CLI (both baseline and design views)
Import Topology	Element activation or reactivation
Check network element	Persist element configuration
View generated CLI (baseline view)	Export baseline dial plan

Because the following operations require serialized access to staging tables, they are semi-concurrent with the Commit operation:

- Design Preview
- View the generated CLI (both the Baseline View and Design View)

If you receive an error message that an operation cannot be executed because it cannot be initialized, wait a few moments and try again. VRC might be waiting for an operation to complete, or that operation must be in the initialized state before you can execute another operation.

If you are executing an operation for a scope that overlaps with another user, your operation request fails. If there is no scope overlap, your operation request is queued and executed when server resources become available.

Note If you are using a Cisco IE2100 device for automating the deployment and management of network devices, your concurrent operation issues might be different.

VRC Terminology

Table 1-3 lists common VRC terminology.

Table 1-3 VRC Terminology

Term	Definition
Administrative Domain	The entire scope of the VRC-managed dial plan.
Address resolution authority (ARA)	The network element assigned to a zone to provide address resolution service to all the elements of the zone. For example, an ARA could be a gatekeeper group or OSP server.
Baseline dial plan	VRC's assessment of what is currently configured on the network.
Baseline View	The view that shows the currently configured dial plan. Use the baseline view to
CLI	Cisco IOS command-line interface.
Design View	The view that allows you to make changes to the currently configured dial plan.
Dial plan	A system that allows one telephone or Cisco IP device to connect to another telephone or Cisco IP device by using dialed digits.
Directory Gatekeeper (DGK)	An H.323 gatekeeper that provides address translation support only for other gatekeepers and not for gateways.
Directory Gatekeeper Group (DGKGrp)	A set of one or more directory gatekeepers configured for redundancy.
Discovery	The operation by which VRC queries network elements for current dial plan related configuration and updates the baseline dial plan to match.
Distribution	The process by which VRC distributes the dial plan to network elements such that their configuration matches the baseline dial plan.
Element	A router with physical counterparts that is used in a VRC dial plan. For example, gateways, gatekeepers, and directory gatekeepers.
Egress Route	An internal zone behavior for a call that is received from the IP network.
Foreign Region	A special kind of region representing adjacent, but unmanaged segment of the VoIP network
Gatekeeper (GK)	An H.323 entity on a LAN that provides address translation and control access for H.323 terminals and gateways.
Gatekeeper Group (GKGrp)	A set of one or more gatekeepers configured for redundancy.
Gateway	A network access server (NAS) that acts as an interface between a circuit-switched Public Switched Telephone Network (PSTN) and a packet H.323 VoIP network.
Hierarchical DGKs	An H.323 configuration where multiple levels of GKs and DGKs are in the LRQ forwarding path.
Ingress Route	An internal zone behavior on the ingress side of the call, when the call is received from the PSTN.
LRQ Transit Region	A special type of managed region that contains only a single DGKGrp. LRQ transit regions are used to create a DGK hieracrchy.

Table 1-3 VRC Terminology (continued)

Term	Definition
Managed Zone	A subset of a managed region, logically corresponding to an H.323 zone.
Managed Region	A logical subset of zones that partitions the VRC managed VoIP netowrk.
Outgoing Region Connection	The assignment of another region as a potential destination for an outbound LRQs.
PTC	Packet Telephony Center
Routes	Calls that leave or enter a zone in a VoIP network.
Route Scope	A collection of call originating or terminating resources within a managed zone. Route scope are used to determine the scope of ingress or egress routes.
VoIP	Voice-over-IP

VRC Client

The VRC application runs on a Sun server and provides a GUI client running within a browser on PCs running the Windows operating system.

VRC software is used to provide basic dial plan provisioning and network configuration when integrated with Packet Telephony Center (PTC).

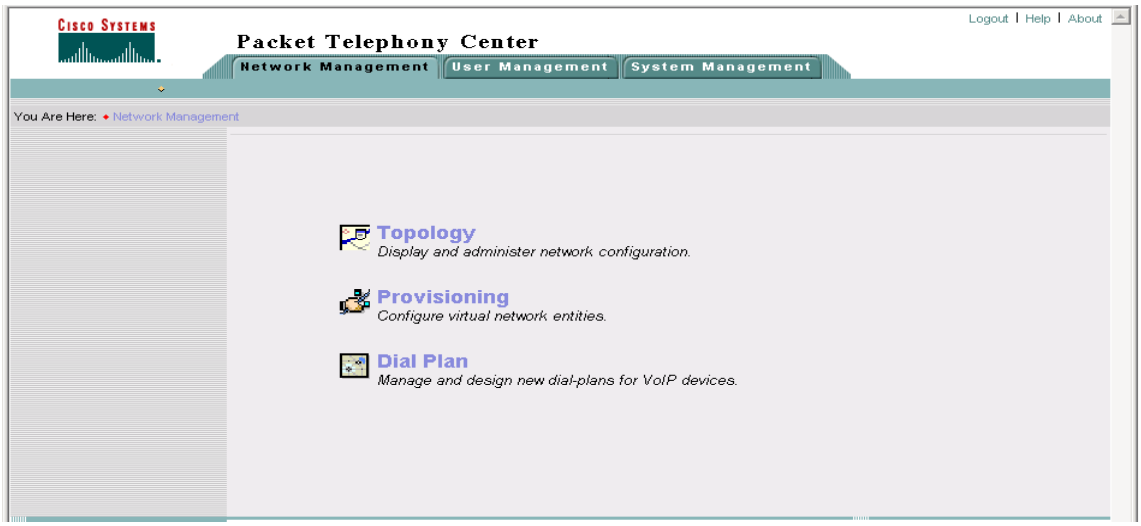
Accessing the VRC Client

The client is provided as web pages accessed with a web browser. Before you begin, read the following tips for troubleshooting client operations:

- Use the online help to help you execute specific tasks using the client.
- If the disk space for the client reaches 80 MB, you are prompted to refresh the memory. You must close all instances of Internet Explorer to refresh the memory.
- Certain operations take a long time to complete and cannot be canceled.

The VRC client is launched from the PTC application. The Dial Plan icon, which is used to launch VRC, is located on the main window of the PTC user interface. Figure 2-1 shows the main window that appears after a successful log in to PTC.

Figure 2-1 PTC User Interface Main Window

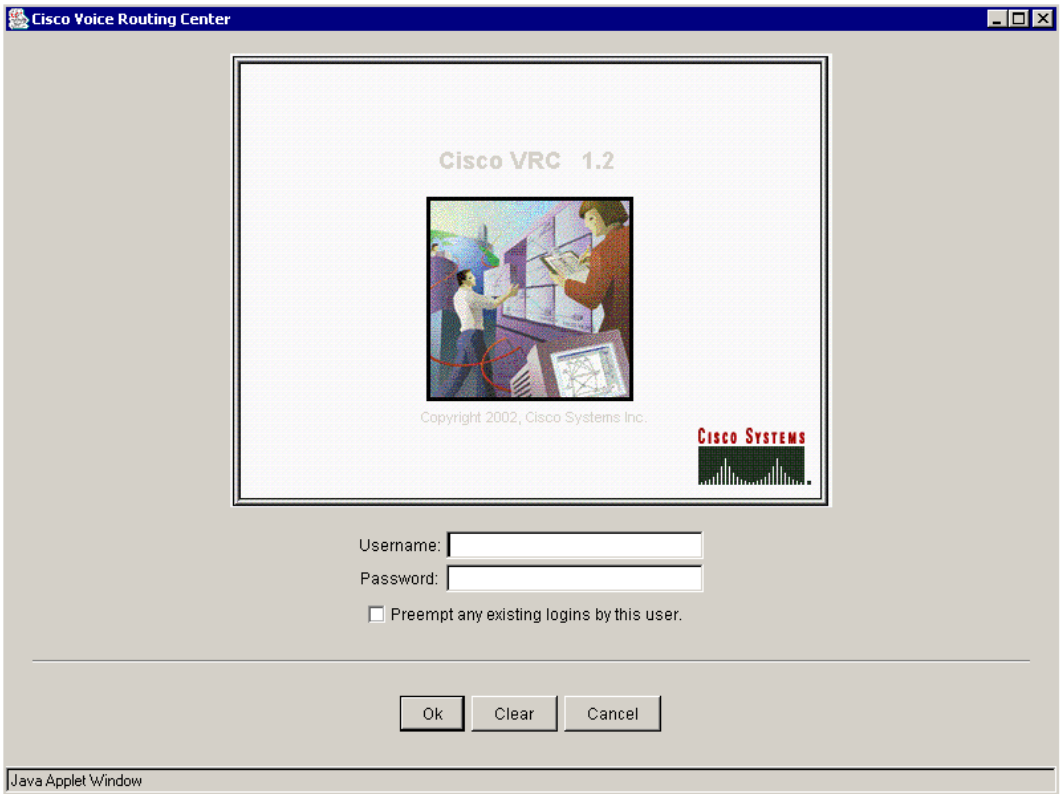


Logging In

To access VRC from the PTC user interface

Step 1 Click the Dial Plan icon on the PTC main window to access the VRC login window (Figure 2-2).

Figure 2-2 Cisco VRC Login Window

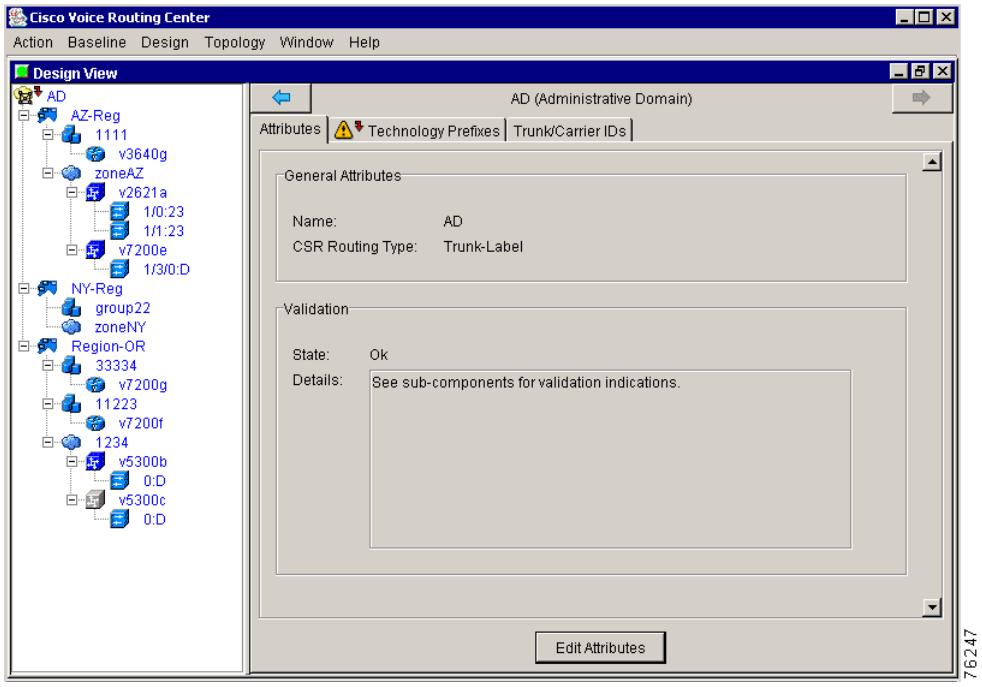


Step 2 Enter your **Username** and **Password** and click **OK**.

Step 3 Use the check box to preempt any previous logins.

Step 4 Click **OK**. The main Cisco Voice Routing Center window appears (Figure 2-3).

Figure 2-3 Cisco Voice Routing Center Window



Step 5 Choose your operation from the VRC menus.

- Baseline View —Represents the current dial plan. Ideally the baseline is consistent with the physical network but can differ if the dial plan changes are made outside of VRC.
- Design View—You make changes to an existing dial plan or start a new dial plan design session.

Logging Out

To log out of the VRC client:

Step 1 To exit from the VRC client, choose **Exit** from the Action menu and click **OK**.

Step 2 To exit from the browser window, restore your browser window, and choose **Close** from the File menu.

VRC Menus

Table 2-1 lists the options available from the VRC main menus.

Table 2-1 VRC Main Menus

Menu	Description
Action Menu	
Change Password	Opens the CNS Security Administration.
Show Privileges	Shows the privileges for each user account from the client.
Display User Log	Display the current user log.
Exit	Close VRC application.
Baseline Menu	Description
Open Baseline	Open the baseline dial plan.
Export Baseline	Export the baseline dial plan design to a browser window.
Find Gateways (Baseline)	identify and list the set of gateways which might terminate a given dial string from the Baseline View.
Design Menu	
Design From Baseline	Start a new dial plan design session
Open Saved Design	Open a previously saved design file.
Delete Saved Design	Delete a stored dial plan design.
Export This Design	Export the current dial plan design to a browser window.
Close This Design	Close the current dial plan design session.
Commit This Design	Commit a dial plan design to the network and establish a baseline dial plan.
Find Gateways (Design)	Identify and list the set of gateways which might terminate a given dial string from the Design View.
Preview (Normal or Forced)	Preview a new dial plan design before you commit it to the network elements.
Validate	Detect and prevent illegal or inconsistent data from being written to the dial plan.
Topology Menu	
Open Topology	Opens the Topology View. The Topology View is not available when VRC is integrated with PTC.
Import Topology	Import topology information from a batch file.
Windows Menu	Description
Display Baseline View	Bring the Baseline View forward.
Display Design View	Bring the Design View forward.
Display Topology View	Bring the Baseline View forward.
Refresh Display	Refresh the information displayed in any VRC view.

Table 2-1 VRC Main Menus

Menu	Description
Help Menu	
User's Guide	Open the VRC online help application.
About VRC	Display the current version of VRC.

VRC Quick Start

This section provides you with a quick overview of the Voice Routing Center and lists the first steps to take when you use the VRC to open an existing dial plan or to create a new dial plan.

The VRC is designed so that a user can make dial plan changes for the whole network (Administrative Domain, or AD), or only within a partition of the network (region). There can only be one design session open per region. The advantage of regional administration is that multiple users can concurrently be doing regional designs.

Only one user at a time can do AD level designs and that design session blocks all regional design sessions.

- **Administrative Domain (AD)**—The whole network. The highest level of administration which encompasses the entire dial plan. The AD includes all elements that participate in the VoIP call routing.
- **Regions**—A specific partition of the network. It may contain one or more zones, gatekeeper groups, and directory gatekeepers.

This section describes a quick start for:

- Creating a New Dial Plan from Scratch, page 2-5
- Creating a New Dial Plan by Discovery, page 2-6
- Starting a New Dial Plan Design, page 2-6
- Opening an Existing Dial Plan Design, page 2-7

Note The quick start is an overview of the required operations. For detailed information about each task, refer to the appropriate sections in this user guide.

Creating a New Dial Plan from Scratch

The following tasks provide a quick start for creating a new dial plan:

1. Add your elements to the topology by using batch import or by manually adding each element to the topology in the Topology View. If you are using VRC integrated with PTC, add the elements using the PTC Topology Manager. In either case, if an element is not present in the topology then it cannot participate in the dial plan.
2. Start a new design session.
3. Add your elements to the design session dial plan.
4. Configure regions, zones, routes, gatekeeper groups, and directory gatekeeper groups as desired.

5. Use the Validate operation to identify any inconsistencies and errors in the dial plan. See Appendix B, "Troubleshooting Cisco VRC" to help you correct any errors. Refer back to Step 4 to make corrections to your configurations.
6. Commit your design session to establish a baseline dial plan. After you commit a dial plan design, you are advised of the elements that receive a new configuration CLI. You can also preview the configuration CLI for those elements.

Creating a New Dial Plan by Discovery

The following tasks provide a quick start for creating a new dial plan by discovery:

1. Add your elements to the topology by using batch import or by manually adding each element to the topology in the Topology View. If you are using VRC integrated with PTC, add the elements using the PTC Topology Manager. An element must exist in the topology to participate in the dial plan.
2. Execute a discovery of the network at the Administrative Domain (AD) level. VRC uses this information to establish a baseline dial plan. If there are any problems with the dial plan from VRC's perspective, you receive error, warning, or informational messages. See Appendix B, "Troubleshooting Cisco VRC" to help you correct any errors.
3. Make the necessary corrections to your configurations. View the generated CLI for any element to determine if your corrections achieve the expected result.
4. Use the Validate operation to identify any inconsistencies and errors in the dial plan. Refer back to Step 3 to make corrections to your configurations.
5. Commit your design session to establish a baseline dial plan. After you commit a dial plan design, you are advised of the elements that receive a new configuration CLI. You can also preview the configuration CLI for those elements.

Starting a New Dial Plan Design

The following tasks provide a quick start for starting a new dial plan design:

1. Add your elements to the topology using batch import or by manually adding each element to the topology in the Topology View. If you are using VRC integrated with PTC, add the elements using the PTC Topology Manager. An element must exist in the topology to participate in the dial plan.
2. Start a new design. The baseline dial plan, which is the last committed dial plan design, is displayed. Start a new design from the baseline dial plan.
3. Configure regions, zones, routes, gatekeeper groups, and directory gatekeeper groups as desired.
4. Use the Validate operation to identify any inconsistencies and errors in the dial plan. See Appendix B, "Troubleshooting Cisco VRC," to help you correct any errors. Refer back to Step 3 to make corrections to your configurations. View the generated CLI for any element to determine if you achieved the expected result.
5. Commit your design session to establish a baseline dial plan. After you commit a dial plan design, you are advised of the elements that receive a new configuration CLI. You can also preview the configuration CLI for those elements.

Opening an Existing Dial Plan Design

The following tasks provide a quick start for opening an existing dial plan design:

1. Open an existing design. Choose a previously saved design file.
2. Configure regions, zones, routes, gatekeeper groups, and directory gatekeeper groups as desired. Any new element must be added in the topology before you can add it to the dial plan.
3. Use the Validate operation to identify any inconsistencies and errors in the dial plan. See Appendix B, "Troubleshooting Cisco VRC," to help you correct any errors. View the generated CLI for any element to determine if you achieved the expected result.
4. Commit your design session to establish a baseline dial plan. After you commit a dial plan design, you are advised of the elements that receive a new configuration CLI. You can also preview the configuration CLI for those elements.

Baseline View

This chapter describes the Baseline View in the Cisco Voice Routing Center (VRC) server application.

The VRC Baseline View provides the currently distributed dial plan and topology for the entire managed network. The baseline dial plan is the currently distributed dial plan.

From the Baseline View you can:

- Browse the baseline dial plan
- Export the baseline dial plan
- Distribute the baseline dial plan
- Execute the Discovery operation

You can execute the following in both the Baseline View and the Design View. See Chapter 4, "Design View" for more information on these operations.

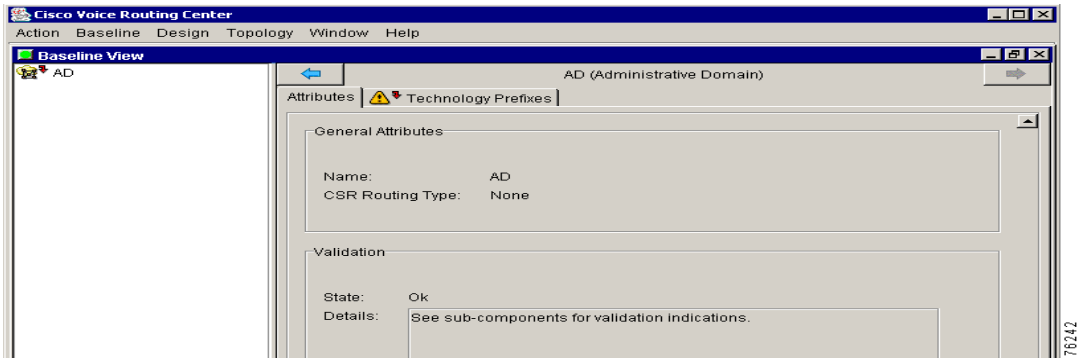
- View the VRC-generated command line interface (CLI)
- Open a telnet session or CLI console for a particular element
- Generate Reports
- Verify call paths
- Check element accessibility.
- Find Terminating Gateways

Opening the Baseline View

To open the Baseline View:

Step 1 Choose **Open Baseline** from the Baseline menu. The Baseline View window appears (Figure 3-1).

Figure 3-1 Cisco VRC Baseline View



The Baseline View window is divided into two panes.

- The left pane shows the dial plan tree for Administrative Domain (AD).
- The right pane shows the information related to the dial plan entity that is highlighted in the dial plan tree.

Exporting the Baseline Dial Plan

The Export process exports the baseline dial plan to a browser window to view or save. You can upload this saved file to the server using tftp, to the /tftpboot/clientinput directory and then reopen it in a future design session.

To export the baseline dial plan to your desktop, follow these steps:

Step 1 From the Baseline menu, choose **Export Baseline**.

A dialog box appears and prompts you to confirm your decision.

Step 2 Click **OK**. A processing window appears and a browser window opens.

A copy of the baseline dial plan appears in a browser window. For example, the browser window displays:

```
<?xml version="1.0" ?>
  <!DOCTYPE AD (View Source for full doctype...)>
- <AD routingType="prefix" exportType="AD" adId="AD0" exportId="AD0">
  <TechPrefix description="Voice Gateway" prefix="1#" adDefault="1"
techPrefixId="TekPf-1-393928" />
  </AD>
```

Distributing the Dial Plan

This section describes how to distribute the baseline dial plan to the elements in the specified scope. You can distribute the dial plan to a specified scope (the entire AD, a single managed region, or to a single network element).

Note Distribution occurs implicitly during the commit operation, or you can request a distribution explicitly by choosing Distribute from the right-click menu in the Baseline View.

To distribute a dial plan:

Step 1 Expand the AD to view all elements.

Step 2 Locate the scope that you want to perform a distribution on.

Step 3 Right-click and choose **Distribute** from the menu. A confirmation dialog box appears and asks you to confirm your decision. Click **OK**.

Before the distribution takes place, the VRC checks if all network elements receiving the updated dial plan configuration are connected. The distribution process starts at the lowest level in the AD hierarchy to minimize the impact on the AD if a failure occurs. VRC distributes the dial plan to the specified scope.

Step 4 An information dialog box appears when the operation is successful. Click **OK**.

Discovering a Dial Plan

VRC uses the Discovery operation to create a new design based on the current actual configuration of the network elements. The discovered dial plan design does not become part of the baseline until it is committed. When you execute a Discovery from the Baseline View, a Design View session opens with the discovered dial plan displayed.

Note You must execute your first Discovery at the AD level.

During the Discovery operation, VRC does the following:

- Queries each device for its dial plan and displays the results in the window
- Reports and flags all errors to help you resolve inconsistencies

Prerequisites

Read this information before you begin the Discovery operation.

- When you execute the Discovery operation from the Design View, the baseline dial plan is not automatically updated. You can view the discovered dial plan in a discovery design session and make changes without affecting the baseline dial plan. To change the baseline dial plan, you must **commit** the dial plan.
- When a network element is discovered by VRC, and its running configuration is not already in the directory /opt/cisco/vnm/gdpm/data/dialplan/origconfig, the element's running configuration is saved in that directory. If you need to restore an element's original configuration, you can manually retrieve it from this location.

- If you begin using VRC by discovering an existing operational network and you want to revert to the network as it was before the VRC Discover was executed, you can execute a Rollback operation from the VRC console. This operation installs all files found in the origconfig directory as the running config on the respective elements.

To discover a dial plan:

Step 1 Select the AD.

Step 2 Right-click the AD and choose **Discover** from the menu. The Open Discovery Design Session dialog box appears. You are prompted for the CSR route type.

Step 3 From the drop-down menu choose the CSR route type. Values are None (the default), Carrier, and Trunk-Label.

If you choose:

- None—VRC disables all CSR-related dial plan features in the AD.
- Carrier—VRC assumes that all CSR-related dial plan features utilized in the dial plan are carrier based.
- Trunk-Label—VRC assumes that all CSR-related dial plan features utilized in the dial plan are trunk-label based.

Step 4 Choose a normal or forced Discovery operation. Checking the box results in a forced Discovery.

- Normal Discovery—The VRC looks for the dial plan and if any of the following errors are encountered, the process stops and informs you of the errors:
  - If the element is unreachable.
  - If the running configuration for the element does not match the element defined in topology. Two examples of this are: The running configuration is for a gateway but the topology lists this element as a gatekeeper. There is an IP address mismatch where the running configuration does not contain the voice-enabled IP address that the element should have.
  - For gateways only—A gateway has no voice ports defined.
- Forced Discovery—The VRC looks for the dial plan and the process continues regardless of any errors. The errors are listed on the VRC server in a user log.

Step 5 Click **Discover**. The VRC reads the running configurations for the elements and the dial plan information for the AD. Or click **Cancel** to cancel the operation.

Step 6 Click **Continue** to display the dial plan in a discovery design session window.

Important Information about Discovery

During the Discovery operation:

- VRC might rename your route scope. To change the route scope name back after Discovery, you must manually edit this attribute in the Design View.
- VRC reads the running configurations for the elements and the dial plan information for the AD. Dial peers that are shut down are ignored.

- VRC constructs routes based on dial peers.
  - It creates an ingress route for every outbound-VoIP dial peer by associating an inbound-pots dial peer to it using a destination pattern. If there are dial peers that cannot be put into association because there is no destination pattern match, VRC creates ingress routes for each of those dial peers provided they have some parameters. In this case, VRC generates multiple routes.
  - Similarly, VRC creates an egress route for every outbound-pots dial peer by associating an inbound-VoIP dial peer to it using a destination pattern. If there are dial peers that cannot be put into association because there is no destination pattern match, VRC creates egress routes for each of those dial peers provided they have some parameters. In this case, VRC generates multiple routes.
- Even though VRC generates multiple routes and route scopes, the network configuration reflected in the client after Discovery is equivalent to the actual configuration of the discovered network. You can commit the dial plan design as it exists after Discovery or you can manually consolidate the routes in your design session before committing it.

From a discovery design session you can:

- Commit the Discovered dial plan. This overwrites the baseline dial plan. If VRC detects any errors during Discovery, you might be required to edit the dial plan before you can commit a design.
- Edit the Discovered dial plan and commit the modified dial plan to the baseline. This overwrites the baseline dial plan and distributes the modified dial plan to the network elements affected by the modifications.
- Exit the Discovery design session and discard any changes.

Note The running configuration for all discovered elements is stored in the origconfig directory, even if the Discovery is discarded.

Note The discovery process produces a design that is comparative, but not identical, to the configuration that is generated by VRC. If you want the configuration stored on the VRC server to exactly reflect the discovered dial plan, use the Distribution process. For more information on Distribution, see Distributing the Dial Plan, page 3-2.

Design View

This chapter describes the Design View in the Cisco Voice Routing Center (VRC) application.

The Design View is where you make administrative changes to a baseline dial plan or element list or create a new dial plan and apply those changes to the elements.

From the Design View you can:

- Browse and edit the dial plan for the active design session
- Delete a saved design from the server storage
- Export the current design to a browser
- Save your design for later use
- Commit your design for distribution to the network
- Validate your dial plan design
- Find terminating gateways
- Preview your design

Design View Basics

The design view reflects the active design session, whether it is a new dial plan design or a previously saved design. Use this view to introduce network elements with no previous dial plan configuration into a dial plan and modify the existing dial plan configuration in the network elements.

Use the following guidelines when manipulating a dial plan in the Design View:

- To view all the elements in your dial plan design, expand the dial plan tree for the Administrative Domain (AD).
- In the Design View you can view all elements in the dial plan. However, you can only modify dial plan components that are in your scope. These components appear highlighted in blue font.
- You can perform administrative tasks for the entire AD or a particular region. The scope is the piece of the network over which you have administrative privileges. Only one user can administer a particular scope at a given time.
- Administrative changes made in the Design View are not applied to the baseline dial plan or distributed to the network until the design is committed.
- Changes to a dial plan design can be saved and resumed at a later login session.

From the Design View right-click menu you can:

- View the VRC-generated command line interface (CLI)
- Open a Telnet session or CLI console for a particular element
- Generate Reports
- Export the dial plan for a region or the AD
- Verify call paths
- Add or delete elements in the dial plan, copy and paste element attributes
- Check element accessibility
- Reactivate elements

Use the Design View to open a new design or make changes to an existing design. When you open:

- An existing design—You are presented with the dial plan design that was previously saved either:
  - Explicitly from a design session
  - Explicitly when a baseline dial plan is exported
  - Implicitly when a design is successfully committed
- A new design—You are presented with a reflection of the baseline dial plan, which you can modify and commit to the network.

Opening a Saved Design

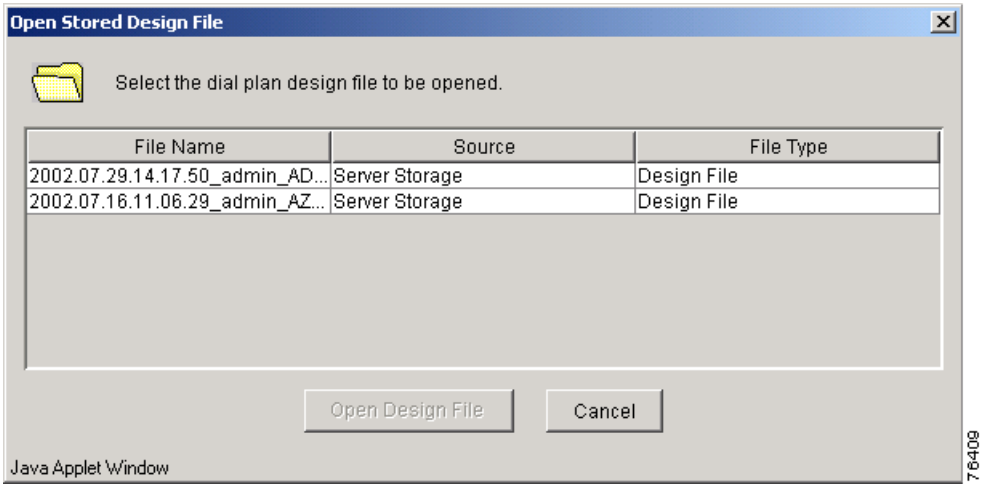
This section describes how to open a previously saved dial plan design. The list of previously saved design files can be any of the following file types:

- Archive files—Automatically created from the baseline dial plan, prior to each commit operation.
- Design Files—Produced when you close an active design session and choose to have the design saved for later recall.
- Import files—Found in the /tftpboot/gdpm/clientinput directory on the server. Use this file type to open a new design from a previously exported dial plan.

To open an existing dial plan design:

Step 1 Choose Open Saved Design from the Design menu. The Open Stored Design File window appears and displays a list of previously saved dial plans (Figure 4-1).

Figure 4-1 Open Stored Design File Window



Step 2 Select a saved dial plan to open and click **Open Design File**. A design session opens and the saved dial plan is displayed.

Step 3 Expand the dial plan tree to view the regions and elements within.

Step 4 Modify the dial plan design.

- Use the tabs in the right window pane to edit the attributes and add parameters to your dial plan entities.
- Use the right-click menu to add elements to the dial plan.

Step 5 You can close and save the design session again complete the dial plan later.

Starting a New Dial Plan Design

A new dial plan design allows you to add elements, make administrative changes to a new dial plan, and apply those changes to the elements.

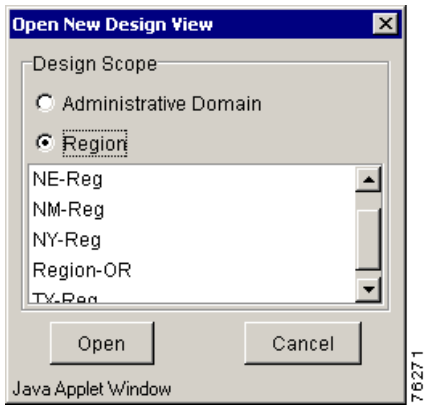
Before you begin, verify that all managed regions and elements affected by your new design are identified in the topology.

Note If an element is not identified in the topology, it cannot be added to a dial plan design.

To configure a new dial plan design:

Step 1 Choose **Design From Baseline** from the Design menu. The Open New Design View window appears (Figure 4-2).

Figure 4-2 Open New Design View Window



Step 2 Select a Design Scope. Choose the AD or a select a region from the list of regions in the topology.

Step 3 Click **Open**. A Design View session opens.

Note You can close and save the design session if you want to complete the dial plan design later.

Adding to a Dial Plan Design Using Copy and Paste

You can use the copy and paste command to add certain entities to the dial plan. For example, if you have one gatekeeper group in a region and want to add another gatekeeper group with the same attributes, use copy and paste.

The copy command creates a gatekeeper group with the same attribute information. The paste command adds this new gatekeeper group to the dial plan. After you paste the gatekeeper group, you must change the Name entry field. You cannot have two entities with the same name.

You can only use copy and paste to add like entities to the appropriate parent in the dial plan. For example, you cannot copy a server trigger and paste it into a region, you cannot copy a gatekeeper group and paste it into the AD, or you cannot copy a gatekeeper group and paste it in a region as a directory gatekeeper group.

The following dial plan entities can only be added by using the right-click menu:

- Gateways
- Gatekeepers
- Directory gatekeepers
- Managed regions
- Gateway parameters, such as voice ports, Ethernet ports, trunk groups, or access lists

Note You must be in the Design View to copy and paste entities into the dial plan.

To copy and paste dial plan entities:

Step 1 Expand the AD to view the entities in the dial plan.

Step 2 Select the dial plan entity that you want to duplicate.

Step 3 Right-click and choose **Copy** from the menu.

Step 4 Select the appropriate parent in the dial plan you want to add this duplicated entity to.

Step 5 Right-click and choose **Paste** from the menu.

Step 6 Click the **Attributes** tab.

Step 7 Right-click and choose **Edit** from the menu.

Step 8 Edit the attribute information. You must edit the Name attribute. You cannot have two dial plan entities with the same attribute information.

Step 9 Choose **Refresh Display** from the Window menu to update the design session display. The duplicated entity is added to the dial plan.

Deleting a Saved Dial Plan Design

This section describes how to delete a dial plan design from the server storage.

Note You can delete a design file in any view.

To delete a dial plan design:

Step 1 Choose **Delete Saved Design** from the Design menu. The Delete Stored Design File window appears.

Step 2 Click the desired dial plan from the list that you want to delete.

Step 3 Click the **Delete Saved Design File** button. You are asked to confirm the delete. Click **OK**.

Exporting a Dial Plan Design

You can export a dial plan for the entire AD or for a region.

Note You must be in the Design View to export a design and the design must be open.

Exporting a Dial Plan Design for an AD

To export a dial plan design for an AD:

Step 1 Select the AD in the dial plan tree.

Step 2 Right-click the AD and choose **Export**. Alternately, you can choose Export This Design from the Design menu.

The dial plan is exported to a browser window to view and save.

Exporting a Dial Plan Design for a Region

To export a dial plan design for a region:

Step 1 Expand the dial plan tree to view all elements.

Step 2 Select a region to export the dial plan from.

Step 3 Right-click the region and choose **Export**. A browser window opens showing the dial plan in a text format.

Committing a Dial Plan Design

This section describes how to commit a dial plan design to your network and establish a baseline dial plan. We recommend that you preview the design before you commit it to the network elements. See Previewing a Dial Plan Design, page 4-8 for more information

Note When you commit a design, VRC replaces the existing dial plan configuration for all elements in the design whose dial plan configuration has changed and updates the baseline dial plan. For example, changing a dial plan in one region might affect elements in other regions.

Note The dial plan design that you want to validate must be open.

To commit your dial plan to the network:

Step 1 With your design session open, choose **Commit This Design** from the Design menu.

Step 2 A Confirm dialog box appears. Click **OK** to confirm your commit or click **Cancel** to return to the Design View window.

During the dial plan commit process, the VRC validates the elements and then generates a baseline dial plan for the affected elements.

During the dial plan generation process, VRC:

- Determines which elements should be deleted, added, or need to be shut down so that the dial plan configuration can be modified.
- Enters a paused state so that you can view the generated CLI as the dial plan generation is taking place.
- Displays a list of elements added, deleted, or modified in the dial plan, or shut down during dial plan generation.

Note If you have one or more gateways with the Reactivate field set to **Yes**, you cannot commit a design. To reactivate a gateway, right-click the selected gateway and choose **Reactivate** from the menu.

An information message indicates that the operation has successfully completed.

Step 3 Click **OK**. The Design View window closes.

Finding Terminating Gateways

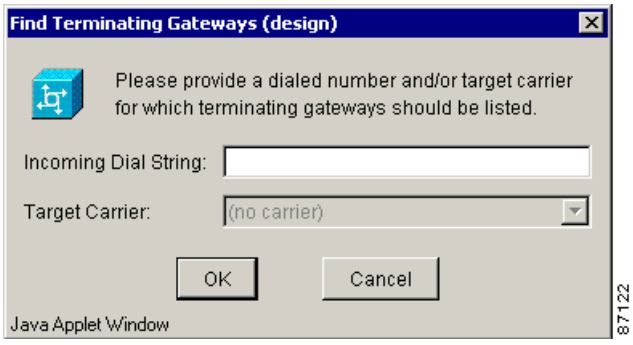
Use this option to find terminating gateways, for a given dial string. You can find terminating gateways for the baseline dial plan or for the dial plan in your active design session.

To find terminating gateways:

Step 1 Choose **Find Gateways** from the Baseline menu or the Design menu.

A dialog box appears (Figure 5-3).

Figure 4-3 Find Terminating Gateway Window



Step 2 Enter the incoming dialed string that you want to find the terminating gateway for. Use only digits in your dial string, leaving out dashes and dots. You can enter only a prefix for your string.

Step 3 If the CSR route type for the AD is set to carrier or trunk-label, select a target carrier. Choose a target carrier from the drop-down menu.

Step 4 Click **OK**. VRC displays the gateways used to terminate routed calls for this dial string.

Step 5 Click **Cancel** to return to the VRC window.

Previewing a Dial Plan Design

This section describes how to preview a new dial plan design before you commit the design to the elements.

Note You must be in the Design View to preview a design and the design must be open.

To preview a new dial plan design:

Step 1 Choose **Preview** from the Design menu and then choose either **Normal Preview** or **Forced Preview** .

- Normal Preview—Displays how your changes affect the elements and you are notified of errors that might occur.
- Forced Preview—Displays how your changes affect the elements despite any errors.

Step 2 The Creating design preview window appears. Wait until the system is finished loading the design. VRC creates a design preview. The location of the preview files on the VRC server is displayed.

Note You must Telnet to the VRC server to view the preview files.

Validating a Dial Plan Design

Validation is the mechanism by which VRC detects and prevents illegal or inconsistent data from being written to the dial plan or sent to the network elements. This action validates the entire design scope. VRC also validates the dial plan design during the Discovery and Commit operations.

Note The dial plan design that you want to validate must be open.

To validate a dial plan design:

Step 1 Choose **Validate** from the Design menu. An information dialog box appears, informing you that the design is being validated.

Note During the validation process, VRC does not check the state of an element in a foreign region.

- If the validation is successful, a confirmation message appears. Click **OK**.
- If the validation is unsuccessful, a warning message appears and tells you the source of the error. Click **OK**.

You are returned to the Design View to make any necessary changes.

Validation Issues

Validation is the mechanism by which VRC detects and prevents illegal or inconsistent data from being written to the dial plan or sent to the network elements. When errors are detected by validation, messages are produced and presented to the user through the client and through the server logs (system, audit, and internal).

Validation is executed implicitly as part of some design operations and explicitly when Validate is chosen from the Design menu. The appropriate recourse for troubleshooting validation errors and warnings depends on the type of operation being performed.

- Design Modification Operations—Include the addition, modification, or removal of any dial plan component from the Design View. When a design modification operation is executed, the validation process checks the affected object only, and determines if the modification being made is valid. If not, the modification is rejected and you are presented with an explanation.

  To correct validation errors produced by design modifications, retry the modification in a way that addresses the conditions described in the error message.

- Dial Plan Generation Operations—Dial plan generation operations include the commit, distribution, or preview of CLI generated from the Design or Baseline View. When a dial plan generation operation is executed, the validation process checks the full dial plan before generating the CLI. If the validation fails, the operation does not continue and you are presented with an explanation.

  – To correct validation errors produced by dial plan generation, review each error and manually correct the dial plan using the Design View for your modifications. The validation message should direct you to the components that require correcting, and which attributes are in violation.

Certain elements (gateways, gatekeepers, directory gatekeepers, managed regions, foreign regions, managed zones, ingress routes, and egress routes) have “status” attributes which indicate the severity (Fatal, Warning, Ok) of the most significant validation message produced for those components. Those in a “Fatal” or “Warning” state are flagged in the GUI dial plan tree as either red or yellow, respectively.

For network elements, you might only be able to correct certain errors by reactivating the element. For example, if a gateway has the “reactivate” attribute set as “yes”, or an element has a required read-only field such as “h323id” not set at all, then an error is produced during validation. In these examples, the failed element must be explicitly reactivated by the user to set these attributes to a state in which they can be committed.

- Dial Plan Discovery Operations— Include activation, reactivation, discovery, and import. For these operations, validation is performed implicitly as an audit of the modifications made to the dial plan. Error messages produced by implicit validation of dial plan discovery operations notify you that the design is no longer in a state that can be committed to the elements.

  – Validation errors produced by dial plan discovery operations do not need to corrected immediately, because the operations succeed despite any errors.

  – Address issues raised by dial plan discovery validation errors in the Design View before you commit the design to the elements.

  – You can also use the tips listed above for dial plan generation operation errors.

- Explicit Validation—Triggered when you choose “Validate” from the Design menu. This executes a validation of the entire design scope, the same as for dial plan discovery operations. An explicit validation provides an audit of what changes must be made before you commit the design to the network.

When you encounter validation error messages, use the console to set the debug of the Validation subsystem to On.

Validation Indicators

After a design validation, VRC uses color coded indicators to inform you that there is an error in the dial plan design. These indicators appear in the dial plan tree and on the tabs in the user interface.

VRC validation indicators are displayed:

- In the dial plan tree - Each entity in the dial plan is color coded to indicate the severity of any errors encountered during validation. A down arrow in the dial plan tree indicates that problems exist with sub-components of that dial plan entity.
- On the user interface Attributes tab - The tab displays a color coded symbol (red stop sign or yellow yield sign) to further point you to the source of the dial plan errors.
- In the table summary column - When you generate a route report, the validation status of the element is listed at the bottom of the report.
- In the Validation Status field - This is usually the last field on the Attributes tab. The validation status field indicates whether the Cisco VRC server can contact the element during the validation process.

Table 4-1 Validation Indicator Colors

Color	Meaning	Comments
Red	One or more FAILURES occurred during the validation process. The dial plan entity is put into a FATAL state.	You cannot commit a dial plan design that has red indicators.
Yellow	One or more WARNINGS occurred during the validation process.	You can commit a dial plan design that has yellow indicators. The design is valid, but the network might behave in an unpredictable manner.
Blue	The validation process has been executed and the validation status is OK	You can commit a dial plan design with blue indicators.
Gray	Validation has not taken place for this dial plan entity.	—

Generating a CLI Description

Before Cisco VRC can send a dial plan configuration to an element, the software must convert the dial plan model to a format that an element can understand, the command line interface (CLI).

During CLI generation of an element, VRC extracts all dial plan information that is relevant to that element and dynamically creates an XML file for that element. For example, during CLI generation for a particular gateway, VRC must extract all dial plan information that directly affects the configuration of that gateway. This information can include voice class codecs assigned to the region where the gateway resides, translation rules or profiles assigned to the managed zone in which the gateway resides, and voice ports on that gateway.

A static configuration file for each element type, which is located on the VRC server, defines how the information in the XML file is translated to CLI. VRC uses this static configuration file and the information in the XML file to generate the CLI configuration. The generated CLI configuration is used to distribute the dial plan to the running configuration for that element.

VRC distributes the configuration to the network elements in the following order:

1. Gatekeepers
2. Gateways
3. Directory gatekeepers

Each time you make a change to your dial plan, the CLI-generated configuration for the elements affected by the dial plan changes. To see how changes in your dial plan have affected the CLI-generated configuration, you must generate a new CLI to view.

Viewing the Generated CLI

This section describes how to view a generated CLI of an element. The generated file is displayed in text format. You can view a generated CLI for an element in the Baseline View or the Design View.

To view the VRC-generated CLI:

Step 1 Expand the Administrative Domain (AD) to view all elements.

Step 2 Locate the element that you want to view a CLI configuration for.

Step 3 Right-click the selected element.

Step 4 Choose **View Generated CLI**. A generated CLI for the selected element is displayed in a separate browser window.

Opening a CLI Session

This section describes how to open a Telnet session to execute CLI with a specific element.

Note You must be in the Design View to open a Telnet session or CLI console for an element.

To open a Telnet session:

Step 1 Expand the AD to view all elements.

Step 2 Locate the element that you want to open a CLI session for.

Step 3 Right-click the selected element.

Step 4 Choose **Open CLI Console** from the menu. A CLI console window opens and you are prompted for the password.

The Telnet application registered with your browser presents a standard Telnet session interface to allow you to perform direct administration on the selected network element.

The CLI console window closes.

Closing a Dial Plan Design

When you finish working on a dial plan design, you can either store the design or discard the design.

Note You must be in the Design View and have a design open to perform this procedure.

To close a dial plan design:

Step 1 Choose the **Close This Design** option from the Design menu.

The Closing Design dialog box appears.

Step 2 Choose one of the following closing methods:

- **Save**—The design is stored on the VRC server. The saved design is named according to the date and time it is closed. The next time you open a design, this saved design is one of your selections.

Note If your Design session originated using the Discovery operation, you cannot save the design.

- **Discard**—The design is discarded and the Design View window closes.
- **Cancel**—Returns you to the previously opened Design View.

A message appears to indicate that the operation was successful.

Step 3 Click **OK** to close the Design View window.

Managing Dial Plan Components

This chapter defines the components of a Voice Routing Center (VRC) dial plan, their attributes, and how to use the components.

VRC dial plan components described in this chapter include:

- Dial Plan Elements—A router with physical counterparts that are used in a VRC dial plan.
- The Administrative Domain—The whole network. The highest level of administration which encompasses the entire dial plan. The AD includes all elements that participate in the VoIP call routing.
- Regions - A specific partition of the network. It may contain one or more zones, gatekeeper groups, and directory gatekeepers.
- Directory gatekeeper groups, gatekeeper groups, and zones—Including the elements, attributes and parameters that can be configured for each of these dial plan components.

Elements

VRC recognizes the following as network elements:

- Gateways
- Gatekeepers
- Directory gatekeepers

The element states refer to their status in the VRC dial plan and the status of the running configuration in relation to the startup configuration.

This chapter decribes how to manage elements within a VRC dial plan. To add a specific element to the dial plan, refer to the following sections:

- To add a directory gatekeeper to the dial plan, refer to"Adding a Directory Gatekeeper to the Dial Plan" section on page 5-27.
- To add a gatekeeper to the dial plan, refer to"Adding a Gatekeeper to the Dial Plan" section on page 5-39.
- To add a gateway to the dial plan, refer to "Adding a Gateway to the Dial Plan" section on page 5-75.

Element States

In the VRC dial plan, the element states refer to their status in the VRC dial plan, availability to the Discovery operation, and the status of the running configuration in relation to the startup configuration.

There are two types of element states:

- **Dial plan state**—Indicates the element status in the VRC dial plan design. The values are:
  - Active—The element is currently used in the baseline dial plan.
  - Inactive—The element is not currently used in the baseline dial plan.
  - Active Pending—The element is not currently used in the baseline dial plan but is used in a design that is not yet committed.
  - Inactive Pending—The element is currently used in the baseline dial plan but has been removed from a design that has not been committed.
- **Configuration state**—Indicates the status of the running configuration in relation to the network device startup configuration. Values are:
  - Volatile—Current running configuration is different from the startup configuration on the device. Each time you make a change to the element in the Design View and commit the design, the configuration state remains volatile until you write the new configuration to startup.
  - Persisted—Current running configuration has been written to the startup configuration on the device.
  - Unknown—The relationship between the element running configuration and startup configuration is unknown.

During the Discovery operation, all elements in the topology which have an Assigned state are added to the discovery design session. If you want to perform a Discovery on a specific network element with an Assigned state, the element is put into the discovery design session. If the element is Unassigned, discovery cannot take place.

Checking Element Accessibility

You can check the accesibility of network elements within a selected scope.

To check on elements:

Step 1 In the Design View or Baseline View, expand the dial plan tree to show all elements.

Step 2 Select the elements that you want to check the accessibility for. You can check a group of elements within a particular scope.

Step 3 Right-click the selected element and choose **Check Elements** from the menu.

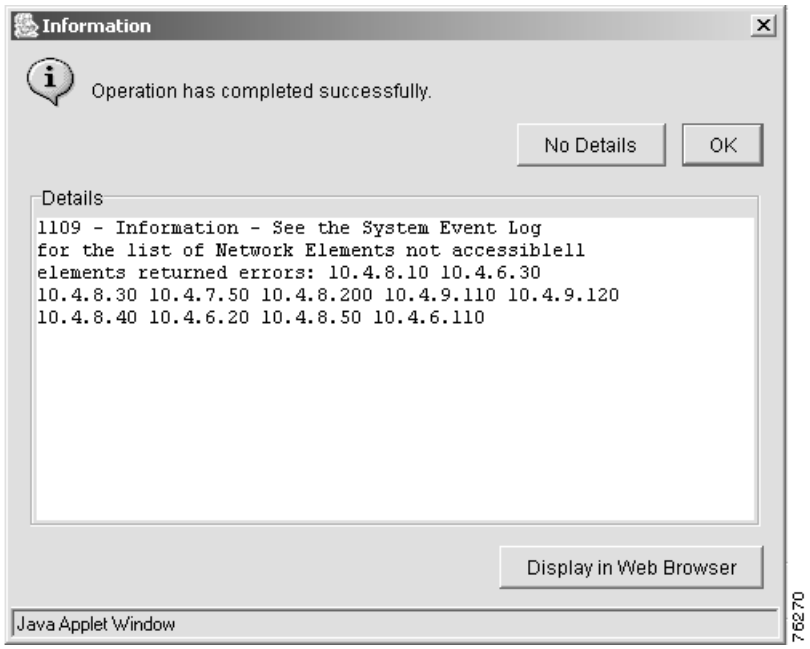
Step 4 Choose which elements that you want to check accessibility for. Select:

- Inactive—Check only elements that are in the Inactive state.
- Active—Check only elements that are in the Active state.
- All—Check all elements.

Step 5 You are asked to confirm your decision. Click **OK**.

A Checking Elements dialog box informs you that the operation is in progress. Once the checking has finished, an information dialog box (Figure 5-1) appears, telling you that the operation was successful.

Figure 5-1 Checking Elements Information Window



Step 6 Click **OK** to close the window, click **Details** to view detailed information, click **No Details** to hide the information, or click **Display Web Browser** to open a web browser window to view the information.

Reactivating an Element

When you add a network element to a dial plan design, that element is implicitly activated.

When you reactivate an element, VRC reads all dial plan configuration from a network element and updates the element topology information. This includes:

- Element information that VRC does not change, such as host name, IP address for that element
- Element configuration information that affects the dial plan, such as voice ports and trunk group configuration, and access lists

You can reactivate the element using the VRC client any time you suspect that there have been changes to element configuration information using the command line interface (CLI) directly.

To reactivate a gateway, gatekeeper, or directory gatekeeper:

Step 1 In the Design View, expand the dial plan tree to show all elements.

Step 2 Select the element for reactivation.

Step 3 Right-click the element and choose **Reactivate** from the menu.

VRC updates the dial plan configuration information for that element.

Administrative Domain

The Administrative Domain (AD) is the entire VoIP network whose dial plan is managed by VRC. The AD is made up of:

- Dial plan regions (managed or foreign)
- Technology prefixes
- Trunk or carrier IDs (if the carrier sensitive route (CSR) route type is set to trunk-label or carrier)

Note The AD must contain at least one managed region.

To view the general attributes of the AD in the Design or Baseline Views, select the AD in the dial plan tree and click the Attributes tab. AD attrtributes include:

- Name—AD.
- CSR Route Type—Defines how VRC manages carrier sensitive route (CSR) related dial plan features. Values are:
  - None—VRC disables all CSR-related dial plan features in the AD.
  - Carrier—VRC assumes that all CSR-related dial plan features utilized in the dial plan are carrier based.
  - Trunk-Label—VRC assumes that all CSR-related dial plan features utilized in the dial plan are trunk-label based.

AD Parameters

The following sections describes how to manage the AD parameters, including:

- Setting the CSR Route Type, page 5-4
- Adding Technology Prefixes, page 5-5
- Adding Trunk and Carrier IDs, page 5-6

Setting the CSR Route Type

The route type is used to define the CSR-related configuration of the dial plan design and sets the route type for the entire Administrative Domain (AD).

To set the route type for the AD:

Step 1 From the Design View, select the AD in the dial plan tree. The **Attributes** tab is forward.

Step 2 To change or set the route type, click **Edit Attributes**. The Attributes for AD dialog box appears.

Step 3 Select one of the following route types:

- Carrier—VRC assumes that all CSR-related dial plan features utilized in the dial plan are carrier-based.
- None—VRC disables all CSR related dial plan features in the AD.
- Trunk-Label—VRC assumes that all CSR-related dial plan features utilized in the dial plan are trunk-label based.

Step 4 Click **Apply** to select the CSR route type or **Cancel**.

Adding Technology Prefixes

A technology prefix is used for technology-related routing. For example, the characters 1# are used by convention to indicate voice gateways. A technology prefix allows the gatekeeper to select a gateway with specific capabilities. The specific capabilities for a technology prefix are defined at the AD level.

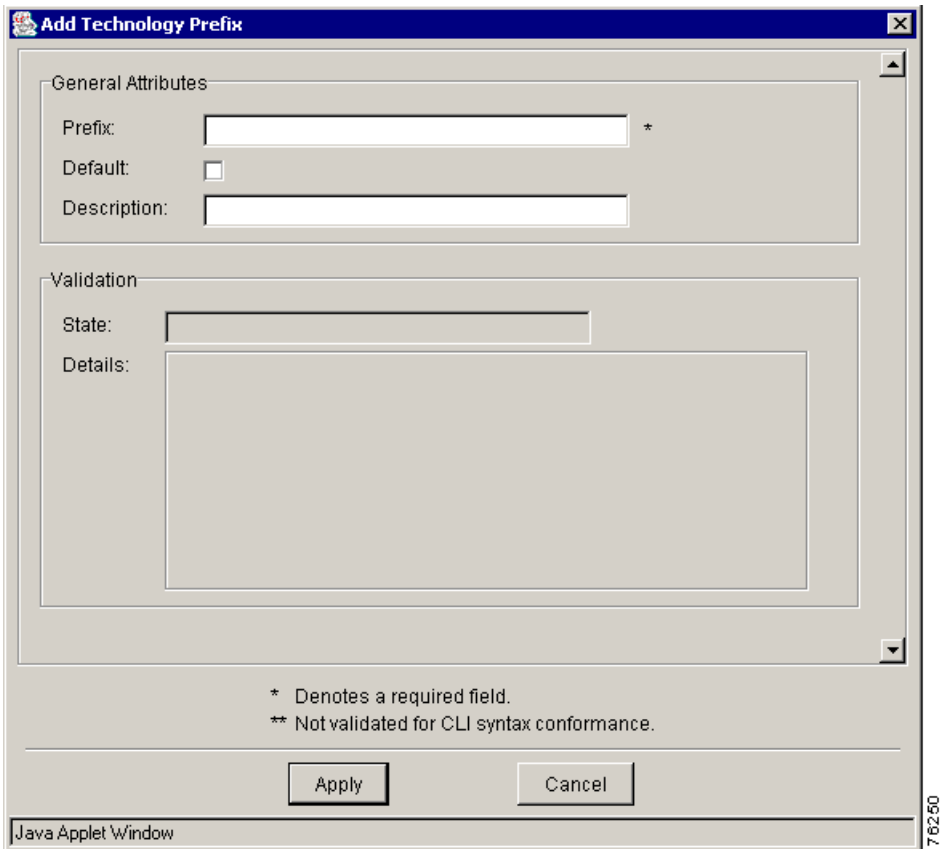
To add a technology prefix to the AD:

Step 1 From the Design View, click AD in the left pane.

Step 2 Click the **Technology Prefixes** tab in the right pane. The technology prefixes list is displayed.

Step 3 Right-click and choose **Add** from the menu. The Add Technology Prefix dialog box appears (Figure 5-2).

Figure 5-2 Add Technology Prefix Dialog Box



Step 4 Enter the technology prefix attribute information:

- Prefix—The technology prefix that you want to add.
- Check the **Default** checkbox if you want this to be your default technology prefix for a gateway.

- Description—Optional. A text description of the technology prefix. The maximum value is 255 characters.

Step 5 Click **Apply** to apply this prefix to the gateway or **Cancel**.

Deleting Technology Prefixes

You can delete a technology prefix from an existing design or a new design.

To delete a technology prefix from the AD:

Step 1 Select the AD and click the Technology Prefixes tab.

Step 2 Select the technology prefix you want to delete.

Step 3 Right-click and choose **Delete** from the menu. A confirmation dialog box appears asking you to confirm.

Step 4 Click **OK** to delete the technology prefix from the dial plan or **Cancel**.

Adding Trunk and Carrier IDs

Trunk and carrier IDs connect a carrier identifier with each inbound call by associating the call on an inbound trunk group, NFAS group, or voice port with a defined carrier.

In VRC, a trunk carrier represents a carrier ID or trunk group label supported by the AD.

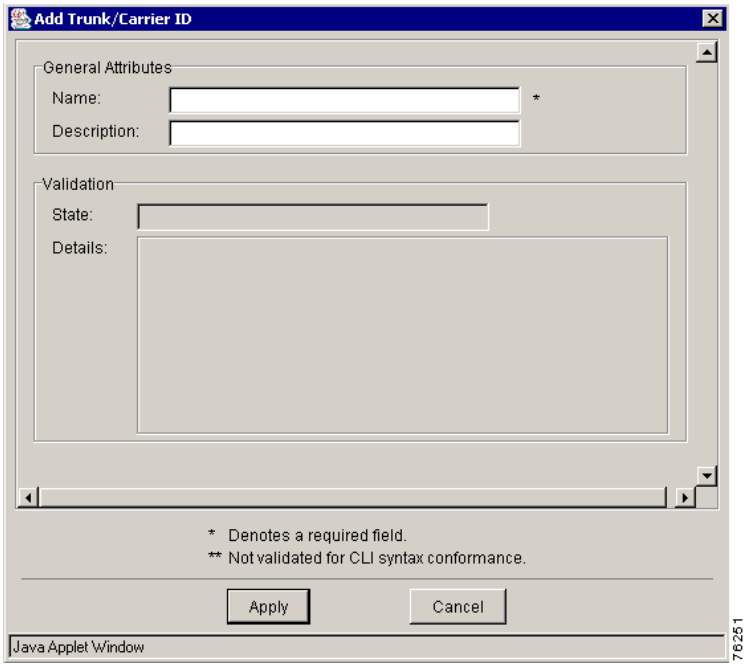
- The trunk ID is used to configure carrier sensitive route (CSR) functionality when the CSR route type for the AD is set to trunk-label.
- The carrier ID is used to configure CSR functionality when the CSR route type for the AD is set to carrier.

To add a trunk or carrier ID to the AD:

Step 1 Select the AD and click the **Trunk/Carrier IDs** tab. This tab is only available when the CSR route type is either carrier or trunk-label.

Step 2 Right-click and choose **Add** from the menu. The Add Trunk/Carrier ID dialog box appears (Figure 5-3).

Figure 5-3 Add Trunk/Carrier ID Dialog Box



Step 3 Enter the Trunk/Carrier attribute information.

- Name—The name of the trunk or carrier ID. The maximum value is 255 characters.
  - Enter a carrier ID if the CSR route type for this AD is set to Carrier.
  - Enter a trunk ID if the CSR route type for this AD is set to Trunk-Label.
- Description—The description value can be an alphanumeric string, maximum value 255 characters.

Step 4 Click **Apply** to add the carrier or trunk ID to the AD or **Cancel**.

Route Servers

A route server is external to the VRC managed dial plan. A VRC managed gatekeeper is configured to communicate with a route server (route servers are used across regions) through the use of server triggers which instruct the router to forward messages of a given route server type.

Note The AD must contain at least one route server.

To add a route server to the AD:

Step 1 From the Design View, select the AD in the dial plan tree.

Step 2 Right-click and choose **Add** and **Route Server** from the menus. The Add Route Server dialog box appears.

Step 3 Enter the attribute information:

- Name—Name of the route server. The maximum value is 64 characters.
- IP Address—IP address of the route server.
- Port—Number of the port. The value must be an integer between 1 and 65535.

Step 4 Click **Apply** to add the route server to the AD or **Cancel**.

Regions

A region is a logical division of the Administrative Domain (AD). Regions consist of network elements that are grouped for geographical or administrative reasons.

The VRC application supports:

- Managed region—A managed region is a subset of the VoIP network which is configured by VRC and is defined as a collection of zones, gatekeepers groups, and zero or one associated directory gatekeeper group.
- Foreign region—Exists as a peer to all other regions within the AD. It does not contain network elements that are managed by VRC, but it can contain routes that might be terminated on a region's directory gatekeeper group or gatekeeper group.
- LRQ Transit region—A special type of managed region which contains only one directory gatekeeper group. This type of region is used for networks with hierarchical DGKs.

A region is either meshed or hierarchical.

- Meshed—A region without a directory gatekeeper group is a meshed configuration. In a meshed configuration all gatekeepers in the region know about each other. Every gatekeeper contains its own database of all addresses and prefixes in the region.
- Hierarchical—A region containing a directory gatekeeper group has a hierarchical configuration. In a hierarchical configuration, the gatekeepers only know about the directory gatekeeper.

This section contains the following topics about a region:

- Adding a Region to the Dial Plan, page 5-10
- Deleting a Region from the Dial Plan, page 5-11
- Region Parameters, page 5-12

Managed Region

A managed region and the elements within the region are managed by the VRC. A managed region consists of network elements which are grouped for geographical or administrative reasons.

A managed region might contain:

- Directory gatekeeper groups (if it is a hierarchical region)
- Gatekeeper groups
- Managed zones
- Outgoing or incoming regional connections
- Open Settlement Protocol (OSP) servers

- Voice class codecs

Table 5-1 describes the attributes for a managed region.

Table 5-1 Managed Region Attributes

Entry Field	Description
Name	The name of the region. The maximum value is 64 characters.
Domain	The domain name. The maximum value is 255 characters.
Class	The class of the region. Choose **meshed** or **hierarchical**. The default is meshed. If you specify a meshed region, you cannot add directory gatekeeper groups to this region.
Role	The role for this region in the dial plan. • Regular - A managed region is a subset of the VoIP network which is configured by VRC and is defined as a collection of zones, gatekeepers groups, and zero or one associated directory gatekeeper group. • LRQ transit - A special type of managed region which contains only one directory gatekeeper group. This type of region is used for networks with hierarchical DGKs. **Note** An LRQ transit region cannot contain any managed zones or gatekeeper groups.
Default LRQ Password	The LRQ password used by all elements in this region to trap LRQs from unknown remote zones. Choose from a previously defined list of LRQ passwords. The maximum value is 1023 characters. **Note** A default regional LRQ password is required before any other security feature can be used. The default LRQ password creates a "catch all" clause for all regional gatekeepers and directory gatekeepers. **Note** If you set this parameter, you must have an incoming connection for every region that has an outgoing connection pointing to it.
Discovery Status	Determines whether a synchronization is required for this region based on VRC-generated LRQ passwords.
Discovery Details	Additional information regarding the Discovery status.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the region. The maximum value is 255 characters.

Foreign Region

A foreign region is outside the AD. A foreign region exists as a peer to all other regions within the AD. It does not contain network elements that are managed by the VRC, but it can contain routes that might be terminated on a region's directory gatekeeper group or gatekeeper group. A foreign region:

- Has a single point of contact

- Is made up of unmanaged zones

Table 5-2 describes the attributes that you must define for a foreign region.

Table 5-2 Foreign Region Attributes

Entry Field	Description
Name	The name of the region. The maximum value is 64 characters.
Domain	The domain name. The maximum value is 255 characters.
IP Address	The IP address of the gatekeeper, which is the point of contact for this foreign region.
RAS Port	The Registration, Admission, and Status signaling port. The range is 1 to 65535.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process
Details	An optional text string that gives more details about the status of the region. The maximum value is 255 characters.

Adding a Region to the Dial Plan

Note The region must exist in the topology before you can add it to the dial plan.

To add a managed region to a dial plan:

Step 1 Expand the dial plan tree to view all components.

Step 2 Right-click the AD and choose **Add** and **Managed Region** from the menus. The Add Managed Region to Dial Plan dialog box appears with a list of available regions.

Step 3 Select a region to add to the dial plan.

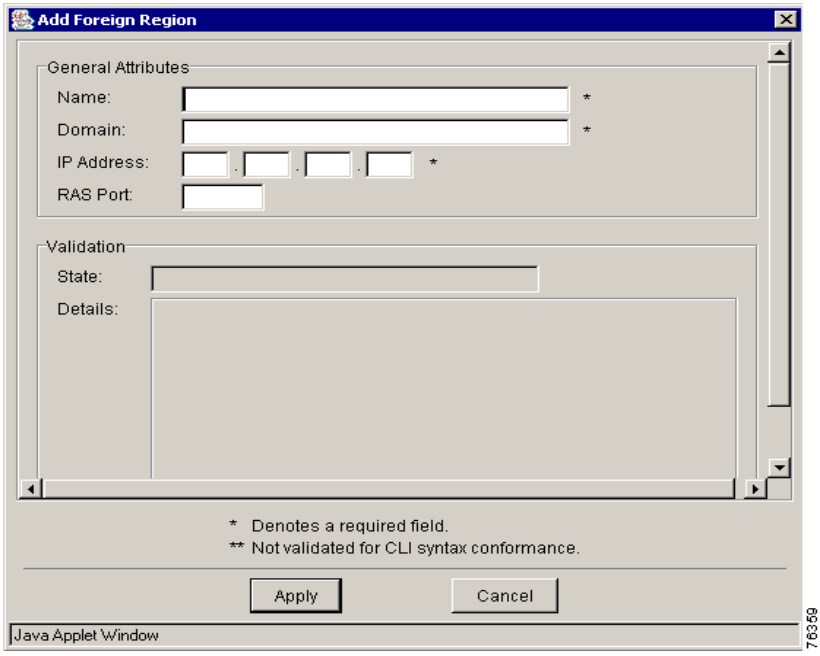
Step 4 Click **Apply** to add the region to the dial plan or **Cancel**.

To add a foreign region to a dial plan:

Step 1 Expand the dial plan tree to view all components.

Step 2 Right-click the AD and choose **Add** and **Foreign Region** from the menus. The Add Foreign Region dialog box appears (Figure 5-4).

Figure 5-4 Add Foreign Region Dialog Box



Step 3 Enter the foreign region attributes. The entry fields are described in Table 5-2.

Step 4 Click **Apply** to add the region to the dial plan or **Cancel**.

Deleting a Region from the Dial Plan

Note When you remove a region from the dial plan, you remove all elements contained in that region.

To remove a region from the dial plan:

Step 1 In the Design View, expand the dial plan tree to view all components.

Step 2 Select the region you want to delete.

Step 3 Right-click and choose **Delete** from the menu.

Step 4 Determine the status of the dial plan configuration. If you choose:

- Disable—VRC clears the dial plan configuration and removes the region from the dial plan database during the next commit process.
- Do not Disable—VRC leaves the current dial plan configuration and removes the region, and all elements that reside in the region, from the dial plan database during the next commit process.
- Cancel—Cancels this procedure.

Step 5 Confirm your decision.

Region Parameters

This section describes how to add or delete the following region parameters:

Outgoing Connections

Regions own their outgoing connections. You can choose the other regions to receive communication from them. These outgoing connections become the incoming connections of the receiving region. VRC allows you to add and delete outgoing connections to a region (managed or foreign).

Note If you set the Default LRQ password attribute for a given region, you must have an incoming connection for every region that has an outgoing connection pointing to it.

Adding Outgoing Connections

To add an outgoing connection for a region:

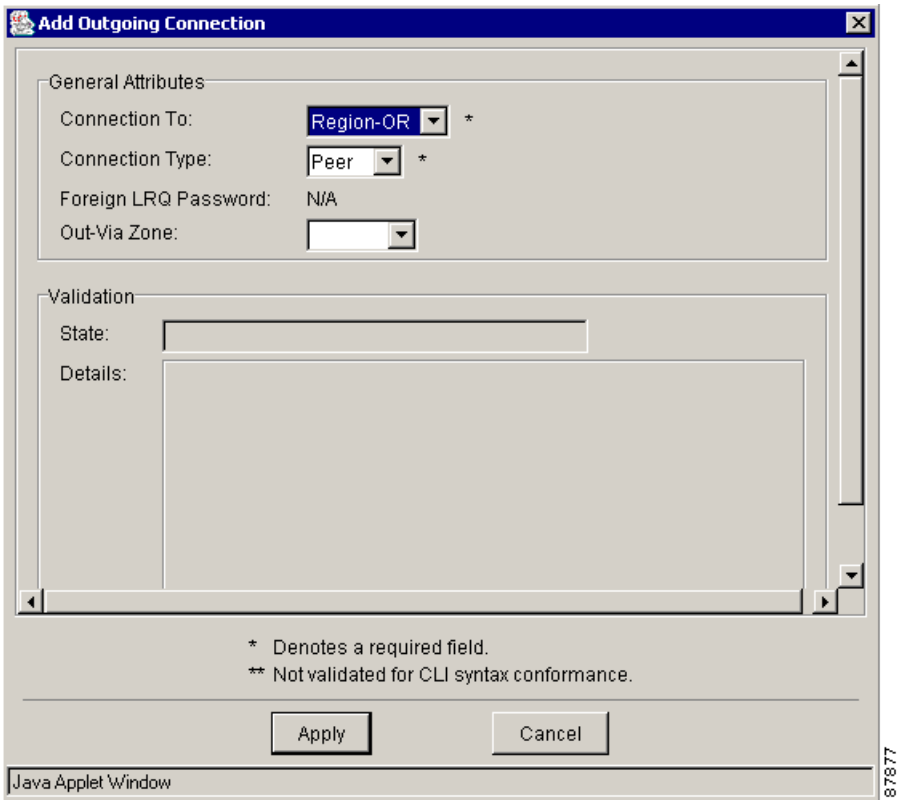
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the region you want to add an outgoing connection to.

Step 3 Click the **Outgoing Connections** tab. The right pane displays the outgoing connections associated with this region.

Step 4 Right-click choose **Add** from the menu. The Add Outgoing Connection dialog box appears (Figure 5-5).

Figure 5-5 Add Outgoing Connection Dialog Box



Step 5 Enter the outgoing region attributes.

- Connection To—The region to point to for this outgoing connection.
- Connection Type—The relationship between a region and its outgoing connection region that reflects the desired inter-region LRQ forwarding pattern.
  - Peer—There is no hierarchical relationship between this region and the region being pointed to for the outgoing connection.
  - Up—The region being pointed to for the outgoing connection is hierarchically above this region.
  - Down—The region being pointed to for the outgoing connection is hierarchically beneath this region.
- Foreign LRQ Password—If your 'connection to' region is a foreign region, set the LRQ password, if it is known and you want this security feature applied.
- Out Via-Zone—This parameter is not supported in VRC 1.2.

Step 6 Click **Apply** to apply the outgoing connection to the region or **Cancel**.

Deleting Outgoing Connections

To delete an outgoing connection from a managed region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a region you want to delete the outgoing connection from.

Step 3 Click the **Outgoing Connections** tab. The list of regions and associated outgoing connections displays.

Step 4 Select a 'Connection To' region to delete.

Step 5 Right-click and choose **Delete** from the menu. A Confirm dialog box appears.

Step 6 Click **OK** to confirm the delete or **Cancel**.

Voice Class Codecs

A voice class codec is the coding scheme used for outgoing calls. VRC allows the administrator to select a valid voice encoding or decoding scheme from its list. You can add or delete voice class codecs from a managed region. A codec is the voice coder rate of speech for a dial peer.

Adding Voice Class Codecs

To add voice class codecs to a managed region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the region you want to add the voice class codec to.

Step 3 Click the **Voice Class Codecs** tab. The list of voice class codecs associated with this region displays.

Step 4 Right-click and choose **Add** from the menu. The Add Voice Class Codecs dialog box appears.

Enter the voice class codec attributes:

- Tag—Unique ID for this voice class codec. The value can be any integer between 1 and 10000.
- Description—Text description of this voice class codec. The maximum value is 255 characters.

Step 5 Click **Apply** to add the voice class codec or **Cancel**.

Deleting Voice Class Codecs

To delete voice class codecs from a managed region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the region you want to delete the voice class codec from.

Step 3 Click the **Voice Class Codec** tab. The list of voice class codecs associated with this region displays.

Step 4 Right-click and choose **Delete** from the menu. A Confirm dialog box appears.

Step 5 Click **OK** to confirm the deletion or **Cancel**.

Adding a Codec

A codec is a software algorithm used to compress/decompress speech or audio signals in Voice-over-IP (VoIP) networks.

To add a codec option to a voice class codec in a region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the region which contains the voice class codec you want to add a codec to.

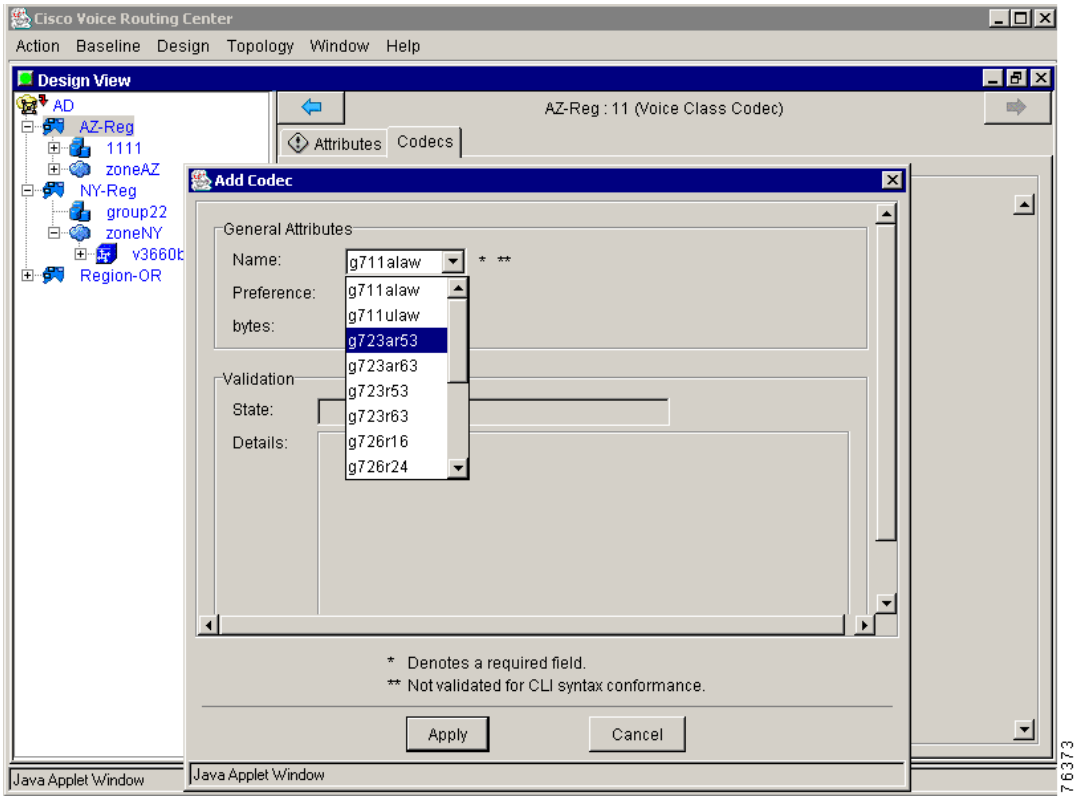
Step 3 Click the **Voice Class Codecs** tab.

Step 4 Double-click the voice class codec you want to add a codec to.

Step 5 Click the **Codecs** tab.

Step 6 Right-click and choose **Add** from the menu. The Add Codec dialog box appears (Figure 5-6).

Figure 5-6 Add Codec Dialog Box



Enter the codecattributes:

- Name—Sets the codec options that you can use when you execute this command. See Table 5-3 for a description of codec options.
- Preference—Specifies the order of preference for this codec. The range is 1 to 14, with 1 being the most preferred and 14 being the least preferred.
- Bytes—Specifies the number of bytes in the voice payload of each frame. The range is 10 to 240.

Note Not all codec options are available on all gateway platforms. Check the Cisco IOS version on your gateway to see which codecs are supported.

Table 5-3 Supported Codecs

Codec Option	Description
g711alaw	G.711 a-Law at 64,000 bits per second (bps)
g711ulaw	G.711 u-Law at 64,000 bps
g723ar53	G.723.1 Annex A at 5300 bps
g723ar63	G.723.1 Annex A at 6300 bps
g723r53	G.723.1 at 5300 bps
g723r63	G.723.1 at 6300 bps
g726r16	G.726 at 16,000 bps
g726r24	G.726 at 24,000 bps
g726r32	G.726 at 32,000 bps
g728	G.728 at 16,000 bps
g729br8	G.729 Annex A and B at 8000 bps
g729r8	G729 Annex A at 8000 bps
gsmcfr	12200 bps
gsmfr	13200 bps

Step 7 Click **Apply** to add the codec or **Cancel**.

LRQ Passwords

LRQ passwords represent CAT (Cisco Access Token) exchanged between two gatekeepers or directory gatekeepers, while forwarding an LRQ.

Note We recommend that you use Network Time Protocol (NTP) when you use LRQ passwords in VRC. Elements that exchange CAT must use NTP for authentication to succeed.

LRQ Passwords can be created by a regional administrator and are associated with all LRQ paths in the network. VRC ensures that passwords are correctly configured on both the sending and the receiving end.

LRQ passwords:

- Are used to validate any LRQs received from the specified remote zone.
- Represents the receiving password from each element to the parent region.
- Are used for incoming regional connections to the parent region and outgoing regional connections to foreign regions.

Note If you set the default LRQ password attribute for a given region, you must have an incoming connection for every region that has an outgoing connection pointing to it and you want this security feature applied.

Adding LRQ Passwords

To add an LRQ password to a region:

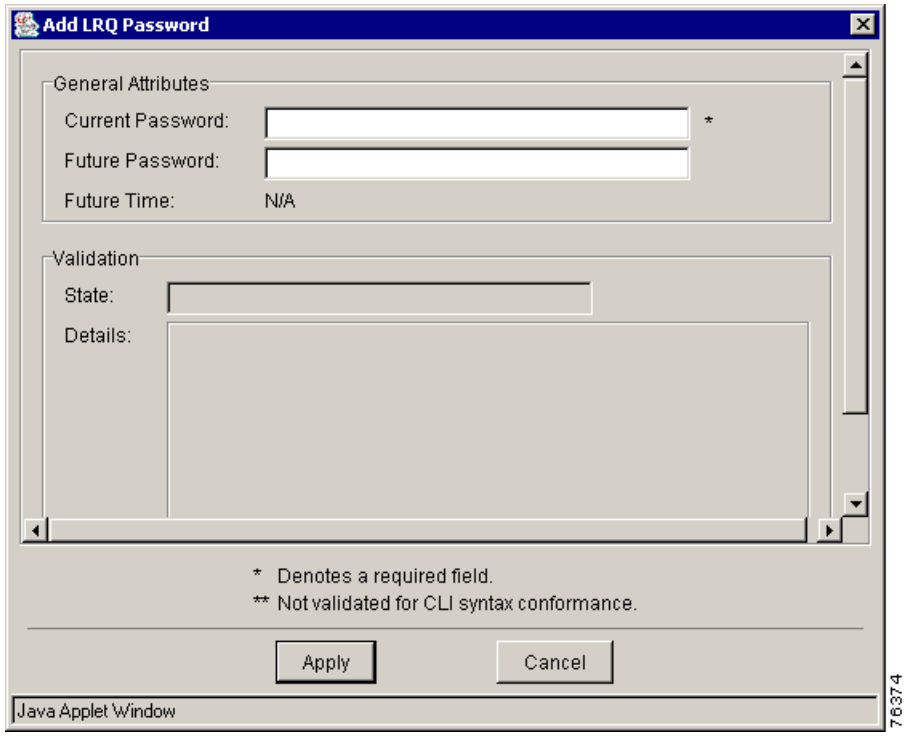
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the region you want to add an LRQ password to.

Step 3 Click the **LRQ Passwords** tab. The list of LRQ passwords associated with this region displays.

Step 4 Right-click and choose **Add** from the menu. The Add LRQ Password dialog box appears (Figure 5-7).

Figure 5-7 Add LRQ Password Dialog Box



Step 5 Enter the LRQ attribute information:

- Current Password—LRQ password used by all elements in this region to trap LRQs from unknown remote zones. Maximum value is 1023 characters.
- Future Password—LRQ password to use by all elements in this region to trap LRQs from unknown remote zones at the time specified in the Future Time parameter. Maximum value is 1023 characters.
- Future Time —This parameter can only be set if the Future Password parameter is set. Enter the hour, minute, month, day and year associated with the future password. The future time is Coordinated Universal Time (UTC), which is the time zone at zero degrees longitude, regardless of the time zone set on the router.

Step 6 Click **Apply** to add the LRQ password to the region or **Cancel**.

Deleting LRQ Passwords

Note You must delete all references to an LRQ password before you can delete it (for example, in incoming and outgoing connections).

To delete an LRQ password from a region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the region you want to delete an LRQ password from.

Step 3 Click the **LRQ Passwords** tab. The list of LRQ passwords associated with this region displays.

Step 4 Select the LRQ password to delete.

Step 5 Right-click and choose **Delete** from the menu. You are asked to confirm your decision.

Step 6 Click **OK** to delete the LRQ password from the region or **Cancel**.

Incoming Connections

An incoming region connection represents the unidirectional connection from one region to the owner region.

Note You must set up an LRQ password before you can add an incoming region connection to a region.

Note You must have an incoming connection for every region that has an outgoing connection pointing to it, if the default LRQ password attribute is set and you want this security feature applied.

Adding an Incoming Connection

To add an incoming region connection from one region to another:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the region you want to add an incoming connection to.

Step 3 Click the **Incoming Connections** tab. The list of incoming connections associated with this region displays.

Step 4 Right-click and choose **Add** from the menu.

Step 5 Enter the attribute information.

- Connection From—The region this incoming connection is from.
- LRQ Receive Password—The password used to validate any LRQs received from the specified remote zone.

- In-Via Zone—This parameter is not supported in VRC 1.2.

Step 6 Click **Apply** to add the incoming region connection to the owner region or **Cancel**.

Deleting Incoming Connections

To delete an incoming connection from a managed region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the region to delete an outgoing connection from.

Step 3 Click the **Outgoing Connections** tab. The list of outgoing connections associated with this region displays.

Step 4 Select the 'Connection To' region you want to delete.

Step 5 Right-click and choose **Delete** from the menu. You are asked to confirm your decision.

Step 6 Click **OK** to delete the outgoing connection from the region or **Cancel**.

Directory Gatekeeper Group

A directory gatekeeper group (DGKGrp) is a set of one to five directory gatekeepers (DGKs) depending on the group type, that you configure for redundancy. This configuration is based on primary, none, Hot Standby Router Protocol (HSRP), cluster, or overlap directory gatekeepers (see Table 5-4).

You can add server triggers and zone circuits to a directory gatekeeper group.

Note You can only add a zone circuit to a directory gatekeeper group if the CSR route type is set to trunk-label or carrier and the VRC feature set is dp1.1 or later.

Directory Gatekeeper Group Attributes

You can view the general attributes of a selected directory gatekeeper group (DGKGrp) from the Baseline View or the Design View:

- Expand the dial plan tree to view all components.
- Locate the directory gatekeeper group and select it to view the attributes.

Note Enhanced functionality attributes can only be viewed and edited if the VRC feature set for this directory gatekeeper group is set to dp1.1 or later.

Table 5-4 describes the attributes of a directory gatekeeper group.

Table 5-4 Directory Gatekeeper Group Attributes

General Attributes	Description
Name	The name of the directory gatekeeper group. The maximum value is 64 characters.
Cluster Name	The local cluster name assigned by this directory gatekeeper group, if it is configured as clustered. The maximum value is 64 characters.
RAS Port	The registration, admission, and status signaling port. The range is 1 to 65535. The default is 1719.
Type	The type of redundancy system used for this directory gatekeeper group. The default is none. • None—This directory gatekeeper group contains only one directory gatekeeper and it is the primary directory gatekeeper. • HSRP—Hot Standby Router Protocol. This directory gatekeeper group contains two directory gatekeepers; one is primary and one is backup. • Overlap—This directory gatekeeper group contains two directory gatekeepers; one is primary and one is overlap. • Both—Both HSRP and Overlap. This directory gatekeeper group contains three directory gatekeepers; one is primary, one is backup, and one is overlap. • Cluster —This directory gatekeeper group contains at least two directory gatekeepers; one is primary and the second (or all remaining directory gatekeepers) must be type cluster.
Feature Set	The VRC feature set supported by this directory gatekeeper group. The default is dp1.0.
Timeout	The timer server timeout (100-ms units). The default is none. The range is 1 to 50.
IRR Timer	Sets the IRR reporting interval which it sets on the gateway upon the gateway's registration. This value can only be set if the VRC feature set is dp1.1 or later. The range is 1 to 60.
Server Registration Port	Configures a port for the gatekeeper to communicate with a Gatekeeper Transaction Message Protocol (GKTMP) server. The range is 1 to 65535.
Server Flow Enabled	Check this box if you want to enable flow control from the VRC server to the network device. The server flow control monitors the average response time from the server to the GKTMP.
Server Flow High	Can only be set if server flow is enabled. The onset percentage of the timeout value used to mark the server as usable or unusable. The range is 1 to 100. The default is 80.
Server Flow Low	Can only be set if server flow is enabled. The abatement percentage of the timeout value used to mark the server as usable or unusable. The range is 1 to 100. The default is 50.

Table 5-4 Directory Gatekeeper Group Attributes (continued)

General Attributes	Description
Max. Queue Length	Can only be set if server flow is enabled. The threshold for the length of the outbound queue on the gatekeeper. The TCP socket between the gatekeeper and GKTMP server queues messages if it has too many to transmit. If the count of outbound queue length on the server reaches this value, the server is marked unusable. The range is 1 to 2000. The default is 50.
Enhanced Functionality	**Description**
Server Retry Timer	Specifies the interval (in seconds) to wait between the detection of a server failure and the next attempt to connect to the failed server. This value can only be set if the VRC feature set is dp1.1 or later. The range is 1 to 300.
Disable IRQ Global Request	Disables global request or call reference value (CRV) set to zero for newly registering end-points. This value can only be set if feature set is dp1.1 or later.
LRQ Reject Unknown Circuit	Enables directory gatekeeper rejection of LRQ messages that contain unknown destination carrier IDs descriptions. This value can only be set if the VRC feature set is dp1.1 or later and the CSR route type is carrier or trunk-label.
LRJ Immediate Advance	Disables the gatekeeper from immediately sending a sequential location request (LRQ) to the next zone after it receives a location reject (LRJ) from a gatekeeper in the current zone.
LRQ Reject Resource Low	If this parameter is set, the gatekeeper rejects the inter-zone call if all gateways in that zone are marked as almost-out-of-resources.
ICZT Password	Enables generation of the interzone ClearToken (ICZT) password. The range is 6 to 8 alphanumeric characters. You can only set this parameter if the VRC feature set is dp1.1 or later.
LRQ/ARQ Handling	**Description**
LRQ Reject Unknown	Rejects LRQ messages for unknown zone prefixes.
LRQ Forwarding	Forwards E.164 Location Request (LRQ) messages to remote gatekeepers managing that zone prefix. Values are: • Yes—The default, indicates that LRQ forwarding is enabled. • No—Indicates not enabled. **Note** VRC does not support simultaneous LRQs being sent on a gatekeeper for a specific zone prefix (LRQ blast), when multiple gatekeepers have the same prefix.
LRQ Delay	Time interval between successive LRQ messages (100-ms units). The range is 1 to 10.
LRQ Window	Defines the time window (in seconds) during which the gatekeeper collects responses to one or more outstanding LRQs. The range is 1 to 15.

Table 5-4 Directory Gatekeeper Group Attributes (continued)

General Attributes	Description
LRQ Receive Password	The LRQ password that the directory gatekeeper assigns to the zones. Set this password to specify an internal regional password for directory gatekeeper communication. If it is not set, the default regional password is used.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Adding a New Directory Gatekeeper Group

Use this procedure to add a new directory gatekeeper group (DGKGrp) to a managed region.

Note You can only add a directory gatekeeper group to a hierarchical region. You cannot add directory gatekeeper groups to meshed regions.

To add a directory gatekeeper group:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the managed region you want to add a directory gatekeeper group to.

Step 3 Right-click and choose **Add** and **Directory Gatekeeper Group** from the menus. The Add Directory Gatekeeper Group dialog box appears (Figure 5-8 and Figure 5-9).

Figure 5-8 Add Directory Gatekeeper Group Dialog Box(General Attributes)

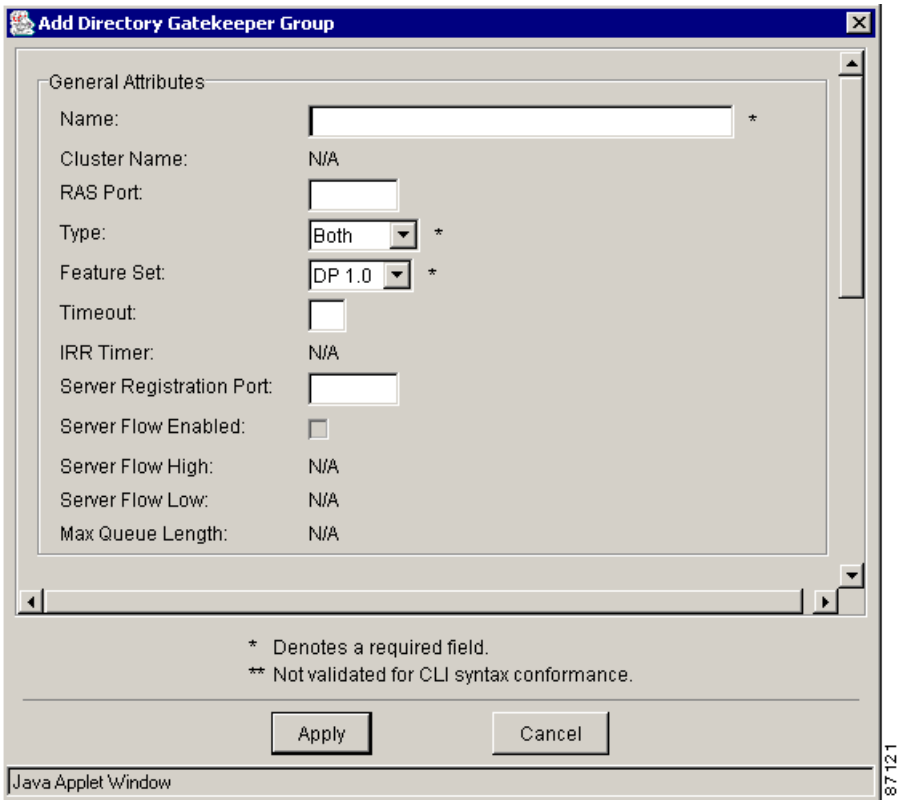
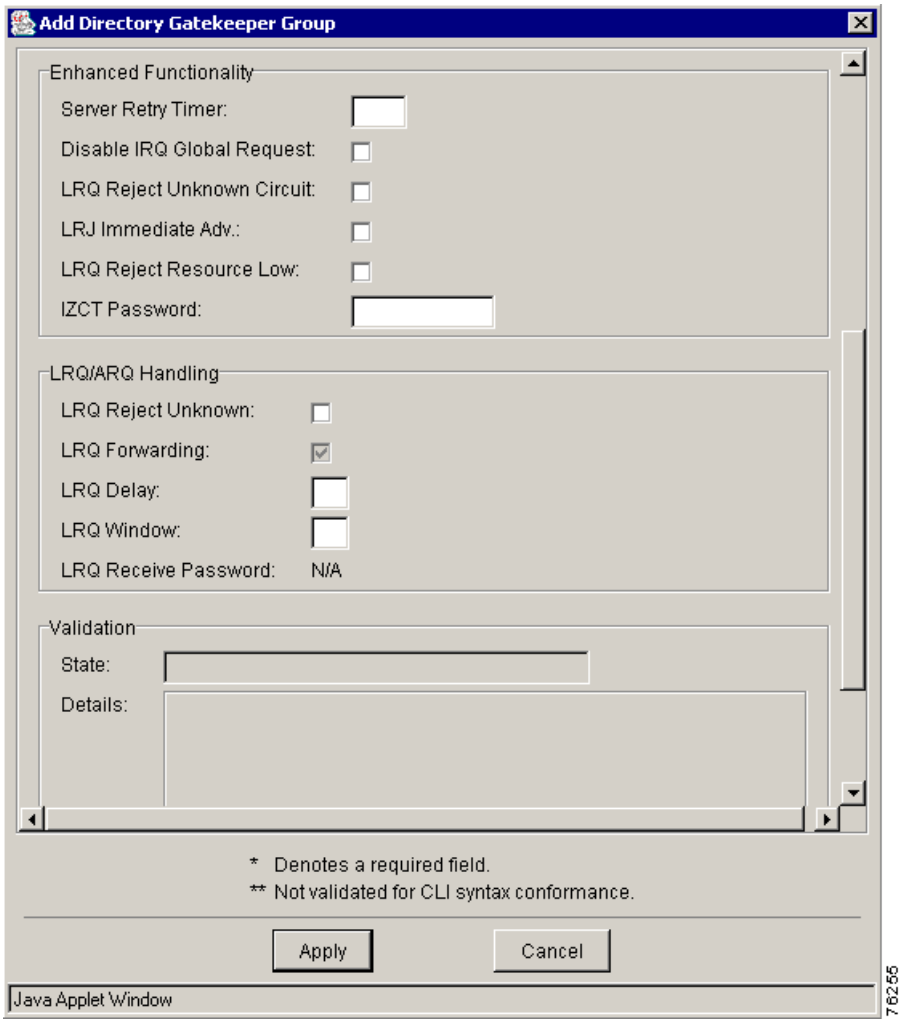


Figure 5-9 Add Directory Gatekeeper Group Dialog Box(Enhanced Functionality and LRQ/ARQ Handling)



Step 4 Enter the attribute information. Refer to Table 5-4 for a description of each entry field.

Step 5 Click **Apply** to add the new directory gatekeeper group or **Cancel**.

Deleting a Directory Gatekeeper Group

To delete a directory gatekeeper group from the dial plan:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the directory gatekeeper group you want to delete.

Step 3 Right-click and choose **Delete** from the menu.

Step 4 Determine the status of the dial plan configuration. If you choose:

- Disable—VRC clears the dial plan configuration and removes the directory gatekeeper group from the dial plan database during the next commit process.
- Do Not Disable—VRC leaves the current dial plan configuration and removes the directory gatekeeper group, and all elements that reside in the directory gatekeeper group, from the dial plan database during the next commit process.

The directory gatekeeper group is removed from the dial plan.

Directory Gatekeeper

A directory gatekeeper is an H.323 gatekeeper that provides address translation support only for other gatekeepers. With a directory gatekeeper, individual gatekeepers do not need to know about other gatekeepers. Instead, a gatekeeper consults its routing table, which provides a default route to a directory gatekeeper. This directory gatekeeper is more knowledgeable about the topology of the network and can forward messages over to the proper gatekeeper. A directory gatekeeper is a VRC element.

A directory gatekeeper:

- Has global dial plan responsibility
- Creates a hierarchical architecture of regional gatekeepers
- Eliminates the need for a fully meshed gatekeeper configuration
- Simplifies overall dial plan management

The directory gatekeeper routes calls outside the local zones by maintaining a list of zone prefix routing tables.

The following Cisco platforms are recognized as directory gatekeepers in VRC:

- Cisco 3640 Multiservice Platform
- Cisco 3660 Multiservice Platform
- Cisco 7200 Series Routers

Directory Gatekeeper Attributes

You can view the attributes of a directory gatekeeper (DGK) from the Design View or Baseline View:

- Expand the dial plan tree to view all components.
- Locate the directory gatekeeper and select it to display the Attributes tab.

Table 5-5 describes the attributes of a directory gatekeeper.

Table 5-5 Attributes of a Directory Gatekeeper

General Attributes	Description
Name	The name of the directory gatekeeper. The maximum value is 64 characters.
IP Address	IP address of the directory gatekeeper.
Standby IP	The IP address the directory gatekeeper uses to communicate with the directory gatekeeper group if the directory gatekeeper group is configured for HSRP.

Table 5-5 Attributes of a Directory Gatekeeper (continued)

General Attributes	Description
IOS version	The Cisco IOS version running on this directory gatekeeper.
Feature Set	The VRC feature set supported by this directory gatekeeper. This field is populated by VRC when the directory gatekeeper is added to the dial plan.
Local Zone Name	The name of the local zone that is associated with this DGK. Maximum value is 255 characters. The local zone name must be unique with respect to all unmanaged zone names, zone alias names, other DGK local zone names in the AD. **Note** Exception: If this DGK has the Type parameter set to primary or backup and another DGK in the same DGK group is also a primary or backup, the local zone names must be identical for those two directory gatekeepers.
Type	The type of directory gatekeeper. Choose from primary, overlap, cluster, or backup. The default is primary. You can have only one primary and only one overlap directory gatekeeper in a directory gatekeeper group (DGKGrp). If you choose: • Overlap, the directory gatekeeper group that this directory gatekeeper belongs to must be type overlap or both. • Backup, the directory gatekeeper group that this directory gatekeeper belongs to must be type backup or both. If you choose backup, you must set the Standby IP value to the IP address of the primary directory gatekeeper. • Cluster, the directory gatekeeper group that this directory gatekeeper belongs to must also be type cluster.
Discovery Status	Determines whether a synchronization is required for this region based on VRC-generated LRQ passwords.
Discovery Details	Additional information regarding the Discovery status.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Adding a Directory Gatekeeper to the Dial Plan

Use this procedure to add a directory gatekeeper to a directory gatekeeper group in the dial plan.

Note You can only add a directory gatekeeper to a directory gatekeeper group for a hierarchical region. There are no directory gatekeeper groups for meshed regions.

Note When you add an element (gateway, gatekeeper, directory gatekeeper) to the dial plan, any preexisting dial plan configuration for that element is overwritten when you commit the design.

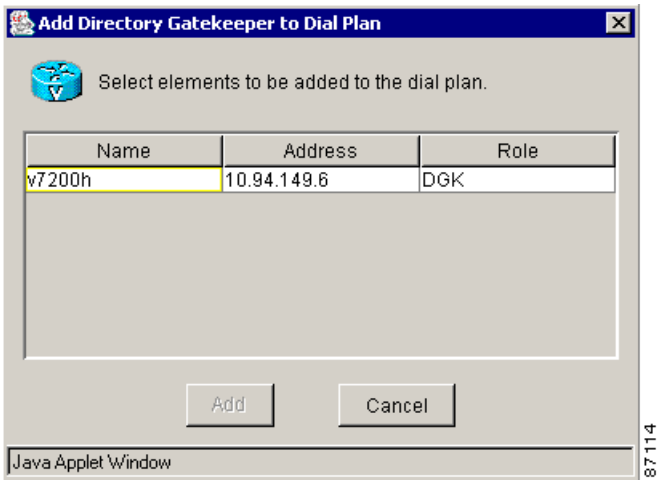
To add a new directory gatekeeper:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the directory gatekeeper group you want to add a directory gatekeeper to.

Step 3 Right-click and choose **Add** and **Directory Gatekeeper** from the menu. The Add New Directory Gatekeeper to Dial plan dialog box appears (Figure 5-10). This dialog box lists the IP addresses of available directory gatekeepers.

Figure 5-10 Add Directory Gatekeeper Dialog Box



Step 4 Select a directory gatekeeper and click **Add**. VRC checks for element accessibility and adds the directory gatekeeper to the dial plan.

If the operation is not successful, click the **Details** button on the error dialog box to view the log.

Gatekeeper Group

A gatekeeper group is a dial plan entity composed of one or more physical gatekeepers.

One gatekeeper in each gatekeeper group must be designated as the primary gatekeeper. If a gatekeeper group contains more than one gatekeeper, you must configure the gatekeepers in a redundant manner using one of the following supported techniques:

- Gatekeeper clusters
- Overlap (alternate) gatekeepers
- Hot Standby Router Protocol (HSRP)
- Both overlap and HSRP

Gatekeeper Group Attributes

You can view the general attributes of a selected directory gatekeeper group (GKGrp) in the Design View or the Baseline View:

- Expand the dial plan tree to view all components.
- Select the gatekeeper group to display the Attributes tab.

Note Enhanced functionality attributes can only be viewed and edited if the VRC feature set for this gatekeeper group is set to dp1.1 or later.

Table 5-6 describes the attributes of a gatekeeper group.

Table 5-6 Gatekeeper Group Attributes

General Attributes	Description
Name	The name of the gatekeeper group. The maximum value is 64 characters.
RAS Port (Registration, Admission, Status)	The port that performs registration, admission, and status signaling. The range is 1 to 65535. The default is 1719.
Type	The type of redundancy system used for this gatekeeper group. The default is none. Values are: • None—This gatekeeper group contains only one gatekeeper and it must be the primary gatekeeper. • HSRP—Hot Standby Router Protocol. This gatekeeper group contains two gatekeepers; one is primary and one is backup. • Cluster—This gatekeeper group contains two gatekeepers; one is primary and one is secondary. All other remaining gatekeepers must be type cluster. • Overlap—This gatekeeper group contains two gatekeepers; one is primary and one is overlap. • Both—Both HSRP and Overlap. This gatekeeper group contains three gatekeepers. One is primary; one is backup, and one is overlap.
Feature Set	The VRC feature set supported by this gatekeeper group. The default is dp1.0.
Timeout	The server timeout for Gatekeeper Transaction Message Protocol (GKTMP) messages. The range is 1 to 50.
Server Registration Port	Configures a port for the gatekeeper to communicate with a GKTMP server. The range is 1 to 65535.
Tech Prefix	Special characters to be included in the called number. Select from the list of predefined technology prefixes.
Server Flow Enabled	Check this box if you want to enable flow control from the VRC server to the network device. The server flow control monitors the average response time from the server to the GKTMP.
Server Flow High	Can only be set if server flow is enabled. The onset percentage of the timeout value used to mark the server as usable or unusable. The range is 1 to 100. The default is 80.
Server Flow Low	Can only be set if server flow is enabled. The abatement percentage of the timeout value used to mark the server as usable or unusable. The range is 1 to 100. The default is 50.
Max. Queue Length	Can only be set if server flow is enabled. The threshold for the length of the outbound queue on the gatekeeper. The TCP socket between the gatekeeper and GKTMP server queues messages if it has too many to transmit. If the count of outbound queue length on the server reaches this value, the server is marked unusable. The range is 1 to 2000. The default is 50.

Table 5-6 Gatekeeper Group Attributes (continued)

General Attributes	Description
Enhanced Functionality	**Description**
IRR Timer	Sets the IRR reporting interval which it sets on the gateway upon the gateway's registration. This value can only be set if the VRC feature set is dp1.1 or later. The range is 1 to 60.
Server Retry Timer	Specifies the interval (in seconds) to wait between the detection of a server failure and the next attempt to connect to the failed server. This value can only be set if the VRC feature set is dp1.1 or later. The range is 1 to 300.
Disable IRQ Global Request	Disables global requests or call reference values (CRVs) set to zero for newly registering end-points. This value can only be set if the VRC feature set is dp1.1 or later.
Enable Server Absent Reject RRQ	Configures the gatekeeper to reject new registration calls or calls when the connection to the Gatekeeper Transaction Message Protocol (GKTMP) server is down.
Enable Server Absent Reject ARQ	Configures the gatekeeper to reject admission requests when the connection to the GKTMP server is down.
LRQ Reject Unknown Circuit	Enables gatekeeper rejection of location request (LRQ) messages that contain unknown destination carrier IDs descriptions. This value can only be set if the VRC feature set is dp1.1 or later *and* the CSR route type is carrier or trunk-label.
LRJ Immediate Advance	Disables the gatekeeper from immediately sending a sequential LRQ to the next zone after it receives a location reject (LRJ) from a gatekeeper in the current zone.
LRQ Reject Resource Low	If this parameter is set, the gatekeeper rejects the inter-zone call if all gateways in that zone are marked as almost-out-of-resources.
High Resource Threshold	Sets high call volume thresholds in the gatekeeper for monitoring its gateway. The range is 1 to 99. This value can only be set if the VRC feature set is dp1.1 or later.
Low Resource Threshold	Sets low call volume thresholds in the gatekeeper for monitoring its gateway. The range is 1 to 99. This value can only be set if the VRC feature set is dp1.1 or later.
ICZT Password	Enables generation of the interzone ClearToken (ICZT) password. The range is 6 to 8 alphanumeric characters. You can only set this parameter if the VRC feature set is dp1.1 or later.
LRQ/ARQ Handling	
LRQ Reject Unknown	Rejects LRQ messages for unknown prefixes.
ARQ Reject Unknown	Rejects ARQ messages for unknown prefixes.

Table 5-6 Gatekeeper Group Attributes (continued)

General Attributes	Description
LRQ Forwarding	Forwards E.164 LRQ messages to remote gatekeepers managing that zone prefix. Values are: • Yes—The default, indicates that LRQ forwarding is enabled. • No—Indicates not enabled. **Note** VRC does not support simultaneous LRQs being sent on a gatekeeper for a specific zone prefix (LRQ blast), when multiple gatekeepers have the same prefix.
LRQ Delay	Time interval between successive LRQ messages (100-ms units). The range is 1 to 10.
LRQ Window	Defines the time window (in seconds) during which the gatekeeper collects responses to one or more outstanding LRQs. The range is 1 to 15.
LRQ Receive Password	The LRQ password that the gatekeeper assigns to the zones. Set this password to specify an internal regional password for gatekeeper communication. If it is not set, the default regional password is used.
LRQ Hop-Count	The hop-count configuration for LRQ forwarding on gatekeepers in this gatekeeper group. You can only set this parameter if the VRC feature set is dp1.1 or later. The range is 1-10.
Security	**Description**
Security Level	The security level. Choose from registration or all. The default is no security level.
Security Type	Enable authentication and authorization on a gatekeeper. Choose from any, h323id, or e164. The default is no security type.
Security Password	The default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The maximum value is 20 characters.
Separator	The character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. The character is null if H.323 is not used. The value must be one character.
Resource Management	**Description**
Load Balance	Specifies whether this gatekeeper group is configured for load sharing between the gatekeepers.
Max. Endpoints	Maximum number of endpoints. The range is 0 to 2147483647.
Max. Calls	Maximum number of calls. The range is 0 to 2147483647.
Max. CPU	Maximum percentage of CPU utilization. The range is 10 to 90.
Max. Memory	Maximum percentage of memory used. The range is 10 to 98.
Bandwidth Allocation	**Description**
Inter-Zone Bandwidth	Specifies the total amount of bandwidth for H.323 traffic from the zone to any other zone. The range is 1 to 10,000,000.

Table 5-6 Gatekeeper Group Attributes (continued)

General Attributes	Description
Total Bandwidth	Specifies the total amount of bandwidth for H.323 traffic allowed in the zone. The range is 1 to 10,000,000.
Remote Bandwidth	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper. The range is 1 to 10,000,000.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Adding a New Gatekeeper Group

You can add one or more gatekeeper groups to a region.

To add a gatekeeper group:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the region you want to add a gatekeeper group to.

Step 3 Right-click and choose **Add** and **Gatekeeper Group** from the menus. The Add Gatekeeper Group dialog box appears (Figure 5-11, Figure 5-12, and Figure 5-13).

Figure 5-11 Add Gatekeeper Group Dialog Box (General Attributes)

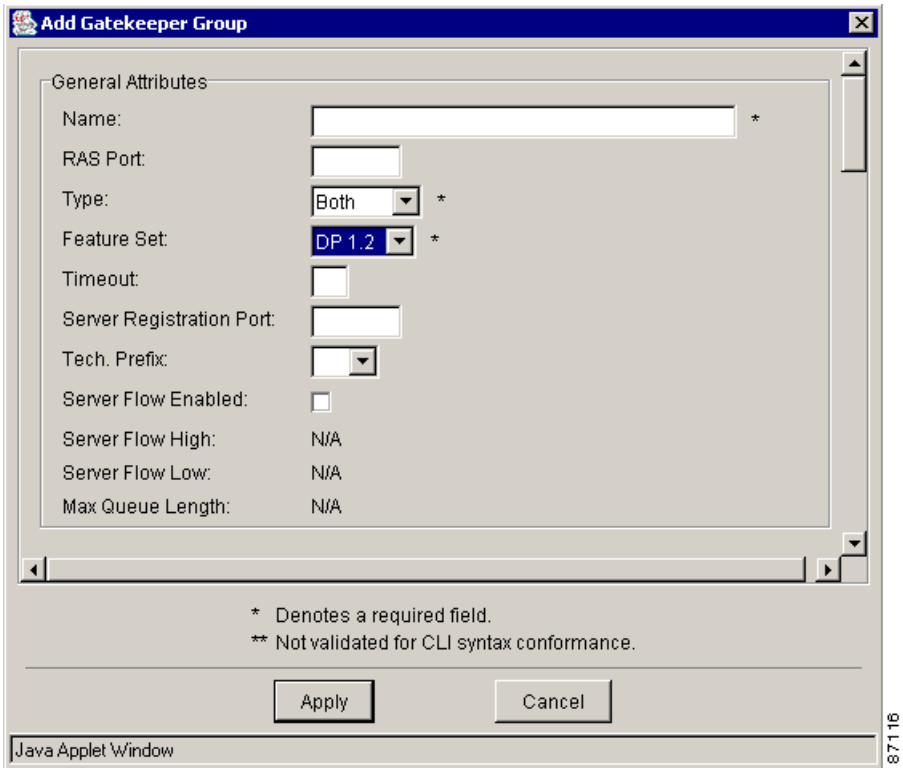


Figure 5-12 Add Gatekeeper Group Dialog Box (Enhanced Functionality and LRQ/ARQ Handling)

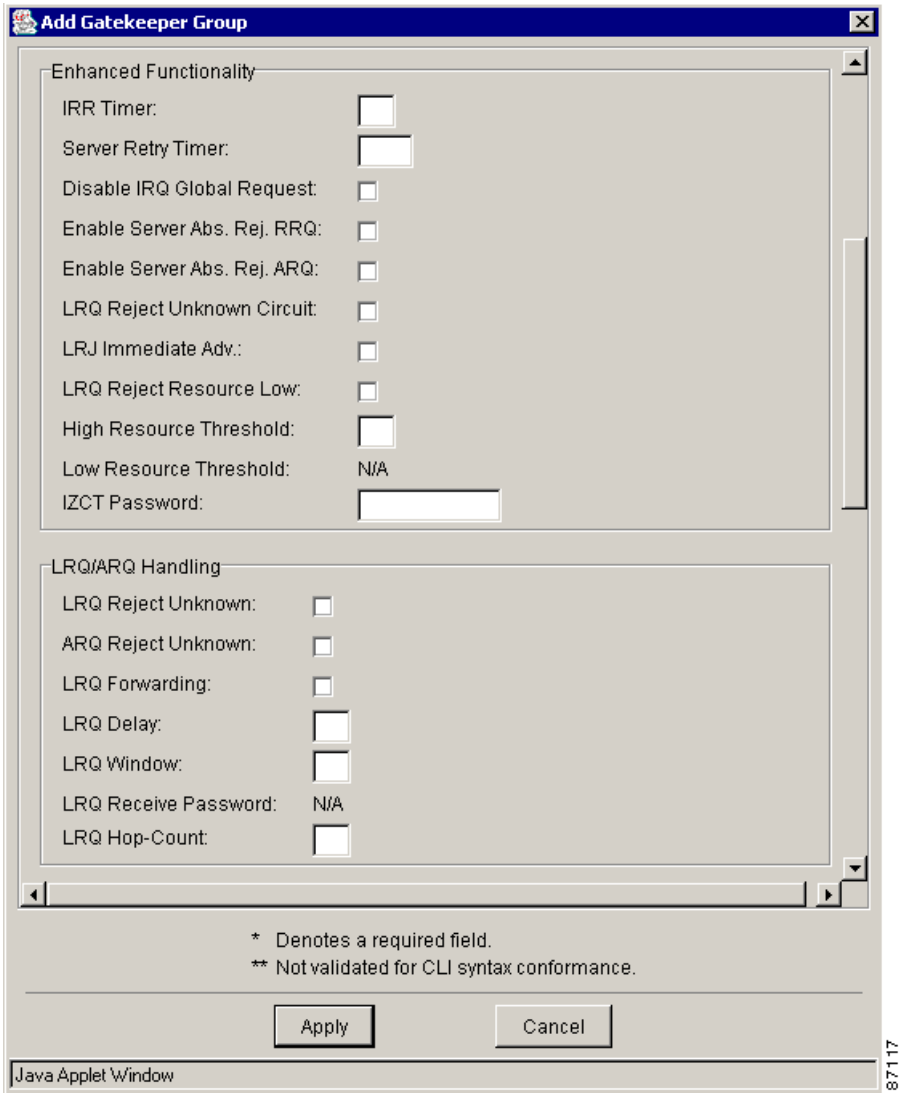
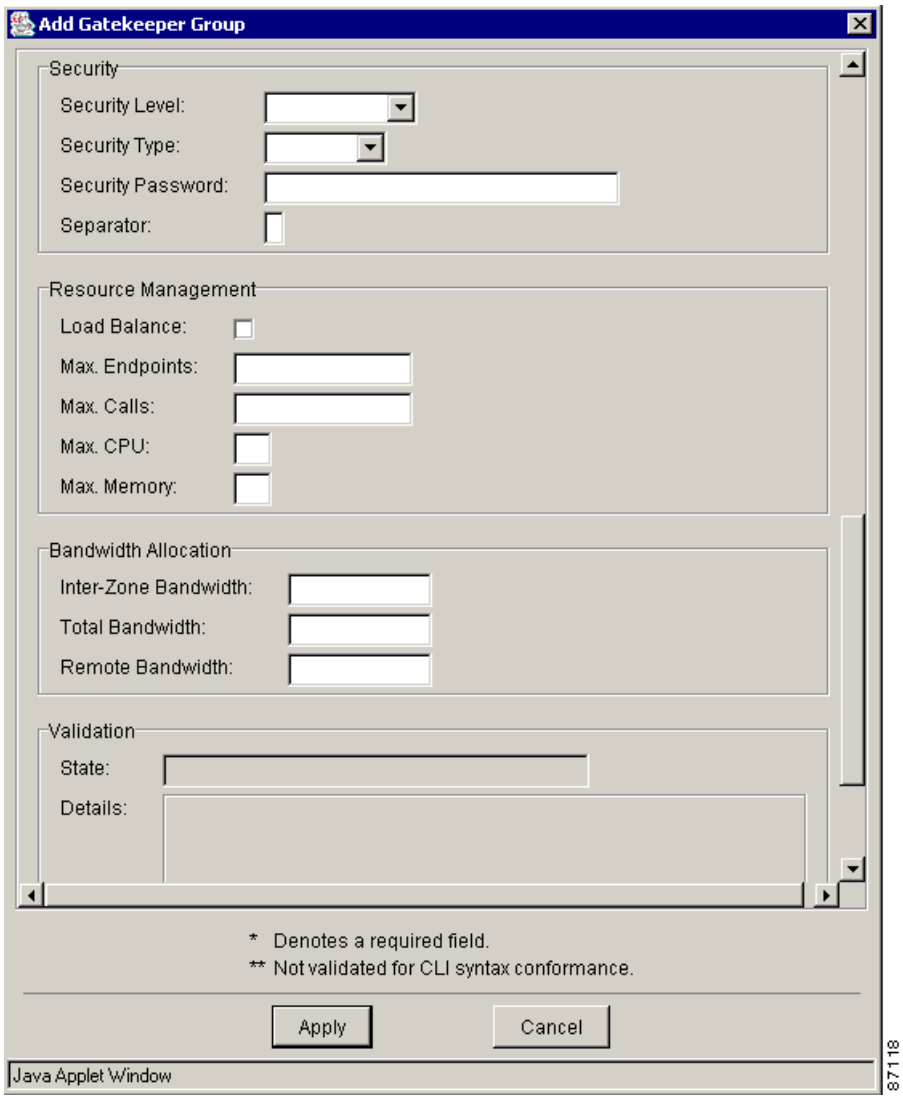


Figure 5-13 Add Gatekeeper Group Dialog Box (Security, Resource Management, and Bandwidth Allocation)



Step 4 Enter the gatekeeper group attribute information. See Table 5-6 for a description of the entry fields.

Step 5 Click **Apply** to add a new gatekeeper group or **Cancel**.

Deleting a Gatekeeper Group

To delete a gatekeeper group from the dial plan:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the gatekeeper group to delete.

Step 3 Right-click and choose **Delete** from the menu. A confirmation dialog box appears.

Step 4 Determine the status of the dial plan configuration. If you choose:

- Disable—VRC clears the dial plan configuration and removes the gatekeeper group from the dial plan database during the next commit process.
- Do Not Disable—VRC leaves the current dial plan configuration and removes the gatekeeper group, and all elements that reside in the gatekeeper group, from the dial plan database during the next commit process.

The gatekeeper group is removed from the dial plan.

Adding a Zone Circuit

A zone circuit is a zone foreign to VRC that is referred to in a "zone circuit-id" command on a gatekeeper or directory gatekeeper. A zone circuit assigns a trunk carrier (circuit-id) to a gateway.

You can add a zone circuit to a gatekeeper group (GKGrp) or directory gatekeeper group (DGKGrp).

Note You can only add a zone circuit to a gatekeeper group or directory gatekeeper group if the CSR route type of the AD is set to trunk-label or carrier and the VRC feature set of the gatekeeper group is dp1.1 or later.

To add a zone circuit:

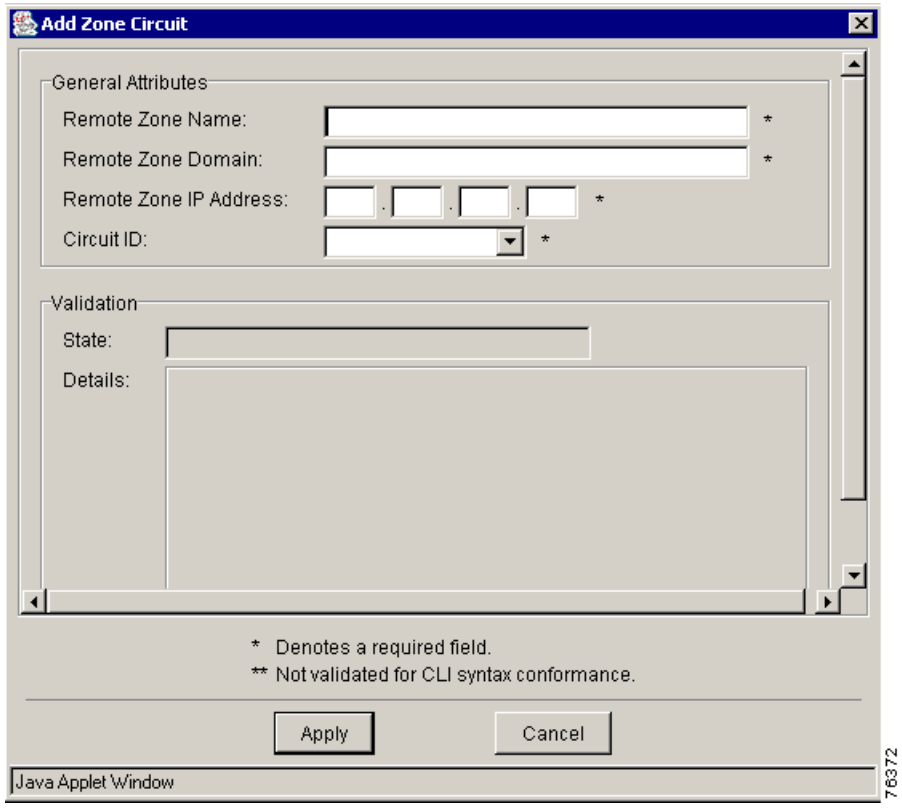
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the gatekeeper group or directory gatekeeper group you want to add a zone circuit to.

Step 3 Click the Zone Circuit tab.

Step 4 Right-click and select **Add** from the menu. The Add Zone Circuit dialog box appears (Figure 5-14).

Figure 5-14 Add Zone Circuit Dialog Box



Step 5 Enter the attribute information.

- Remote Zone Name—Name of the remote zone.
- Remote Zone Domain—Domain name of the remote zone. The maximum value is 255 characters.
- Remote Zone IP Address—IP address of the remote zone.
- Circuit ID—The trunk carrier ID associated with this remote zone.

Step 6 Click **Apply** to add the zone circuit or **Cancel**.

Gatekeeper

A gatekeeper (GK) is an H.323 component on a LAN that:

- Provides address translation and control access to the LAN for H.323 terminals and gateways.
- Provides other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.
- Maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper. A directory gatekeeper is a VRC element.

Gatekeepers perform the following tasks:

- **Resource Management**—Gatekeepers determine the health of H.323 gateways by monitoring registration and nonregistration messages and resource availability indicators.
- **Call Routing**—Gatekeepers provide call routing based on destination E.164 addresses. They can use their knowledge of local gateway health levels to make routing decisions in order to increase network availability of the gateways.
- **Security**—Gatekeepers in conjunction with an external server (for example, RADIUS) may be used for secure call admission.
- **CDR Generation**—Gatekeepers have limited abilities to generate call detail recording (CDR) records for calls either in addition to or instead of from the gateway.

The VRC network supports primary, alternate, overlap, and clustered gatekeepers.

- The Cisco VRC network supports the following Cisco products as H.323 gatekeepers:
  - Cisco 3640 Multiservice Platform
  - Cisco 3660 Multiservice Platform
  - Cisco 7200 Series Routers

Gatekeeper Attributes

View the general attributes of a selected gatekeeper from the Baseline View or Design View:

- Expand the dial plan tree to view all components.
- Locate the gatekeeper and select it to display the Attributes tab.

Table 5-7 describes the attributes of a gatekeeper.

Table 5-7 Attributes of a Gatekeeper

General Attributes	Description
Name	The VRC server contacts the host server to get the host name during discovery or distribution. The maximum value is 64 characters.
IP Address	The IP address of the element.
Standby IP	The IP address the gatekeeper uses to communicate with the gatekeeper group if the gatekeeper group is configured for HSRP.
IOS Version	The Cisco IOS version running on this gatekeeper.
Feature Set	The VRC feature set supported by this gatekeeper. This field is populated by VRC when the gatekeeper is added to the dial plan.

Table 5-7 Attributes of a Gatekeeper (continued)

General Attributes	Description
Type	The type of gatekeeper. Choose from secondary, cluster, overlap, or backup. The default is primary. There can be only one primary gatekeeper in a gatekeeper group. If you choose: • Secondary—Gatekeeper group that this gatekeeper belongs to must be cluster. There can only be one secondary gatekeeper in a gatekeeper group. • Cluster—Gatekeeper group that this gatekeeper belongs to must be type cluster. • Overlap—Gatekeeper group that this gatekeeper belongs to must be overlap or both. • Backup—Gatekeeper group that this gatekeeper belongs to must be type HSRP or both. There can only be one backup gatekeeper in a gatekeeper group. If you choose type backup, you must set the Standby IP value to the IP address of the primary gatekeeper.
Discovery Status	Determines whether a synchronization is required for this region based on VRC-generated LRQ passwords.
Discovery Details	Additional information regarding the Discovery status.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Adding a Gatekeeper to the Dial Plan

This section describes how to add a gatekeeper to a gatekeeper group in the dial plan.

Note When you add an element to the dial plan, any preexisting dial plan configuration for that element is overwritten when you commit the design.

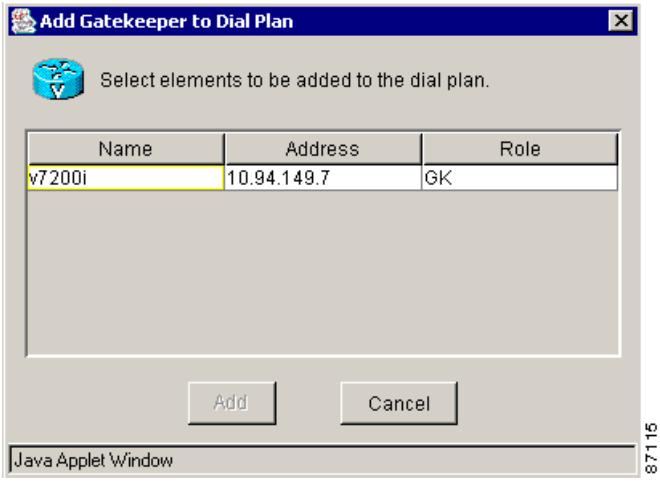
To add a gatekeeper to a gatekeeper group in the dial plan:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the gatekeeper group you want to add the gatekeeper to.

Step 3 Right-click and choose **Add** and **Gatekeeper** from the menus. The Add Gatekeeper to Dial Plan dialog box appears (Figure 5-15).The list of available gatekeepers displays.

Figure 5-15 Add Gatekeeper Dialog Box



Step 4 Select a gatekeeper and click **Add**. VRC checks for element accessibility and adds the gatekeeper to the dial plan.

If the operation is not successful, click the **Details** button on the error dialog box to view the log.

Zones

A zone is the collection of H.323 nodes such as gateways, terminals, and multipoint control units (MCUs) registered with the gatekeeper. There can only be one active gatekeeper per zone. These zones can overlay subnets and one gatekeeper can manage gateways in one or more of these subnets.

A zone is another component of the dial plan that contains address resolution authority (ARA), a set of prefixes that are managed by the zone, and routes that are associated with the zone. Zones partition regions by grouping together gateways with the same routing characteristics.

Zones must contain:

- At least one gateway
- One ingress or egress route
- Only one zone alias for each gatekeeper in the gatekeeper group associated with this zone

Zone types:

- **Managed**—Zone within a managed region and consists of gateways and a set of routes. The VRC feature set of a managed zone is set by VRC and is determined by the gateway with the lowest VRC feature set. The feature set of the zone is not established until a gateway is added to the zone.
- **Unmanaged**—Zone that is recognized by VRC but not managed by VRC. It is a zone in a foreign region.

A zone is local or remote in relation to the gatekeeper.

- Local zone—Zone in the same gatekeeper group as a gatekeeper
- Remote zone—Zone in the gatekeeper group of another gatekeeper

This section contains the following topics about zones in a dial plan:

Managed Zone Attributes

You can view the general attributes of a selected zone from the Design View or the Baseline View:

- Expand the dial plan tree to view all components.
- Locate the zone and select it to display the Attributes tab.

Table 5-8 describes the attributes of a managed zone.

Table 5-8 Managed Zone Attributes

General Attributes	Description
Name	The name of the zone. The maximum value is 64 characters.
Role	The role for the managed zone in the dial plan. This parameter is required. • Regular - A subset of a managed region corresponding to an H.323 zone. You can select this parameter if the region role is *regular*.
Feature Set	The VRC feature set for this managed zone. The feature set of a managed zone is set by VRC and is determined by the gateway with the lowest feature set. The feature set of the zone is not established until a gateway is added to the zone.
Protocol	H.323
Domain	The domain name of the zone (for example, cisco.com). The maximum value is 255 characters.
Cost	The cost associated with the zone. The range is 1 to 99.
Priority	The priority associated with the zone. The range is 1 to 99.
Gatekeeper Group	The gatekeeper group associated with this zone. The gatekeeper group must be in the same managed region as this managed zone.
Bandwidth Allocation	**Description**
Inter-zone bandwidth	The maximum aggregate bandwidth for H.323 traffic between one zone and another zone. The range is 1 to 10,000,000.
Total bandwidth	The maximum aggregate bandwidth for H.323 traffic within a zone and between zones (intrazone and interzone). The range is 1 to 10,000,000.

Table 5-8 Managed Zone Attributes (continued)

General Attributes	Description
Validation State	Indicates whether the Cisco VRC server can contact the elements during the Validation process. • OK—The last validation detected no warnings or errors. • Warning—The last validation detected one or more warnings that you might be required to correct before you commit the dial plan, depending on your intent of the dial plan design. • Fatal—The last validation detected one or more errors that you must correct before you commit the dial plan.
Details	Additional information regarding the validation state of the zone.

Adding a Managed Zone

A managed zone is a zone within a managed region and consists of gateways and a set of routes.

The VRC feature set of a managed zone is set by VRC and is determined by the gateway with the lowest VRC feature set. The feature set of the zone is not established until a gateway is added to the zone.

Note You must reference a gatekeeper group when you add a managed zone to a managed region. See Adding a New Gatekeeper Group, page 5-32.

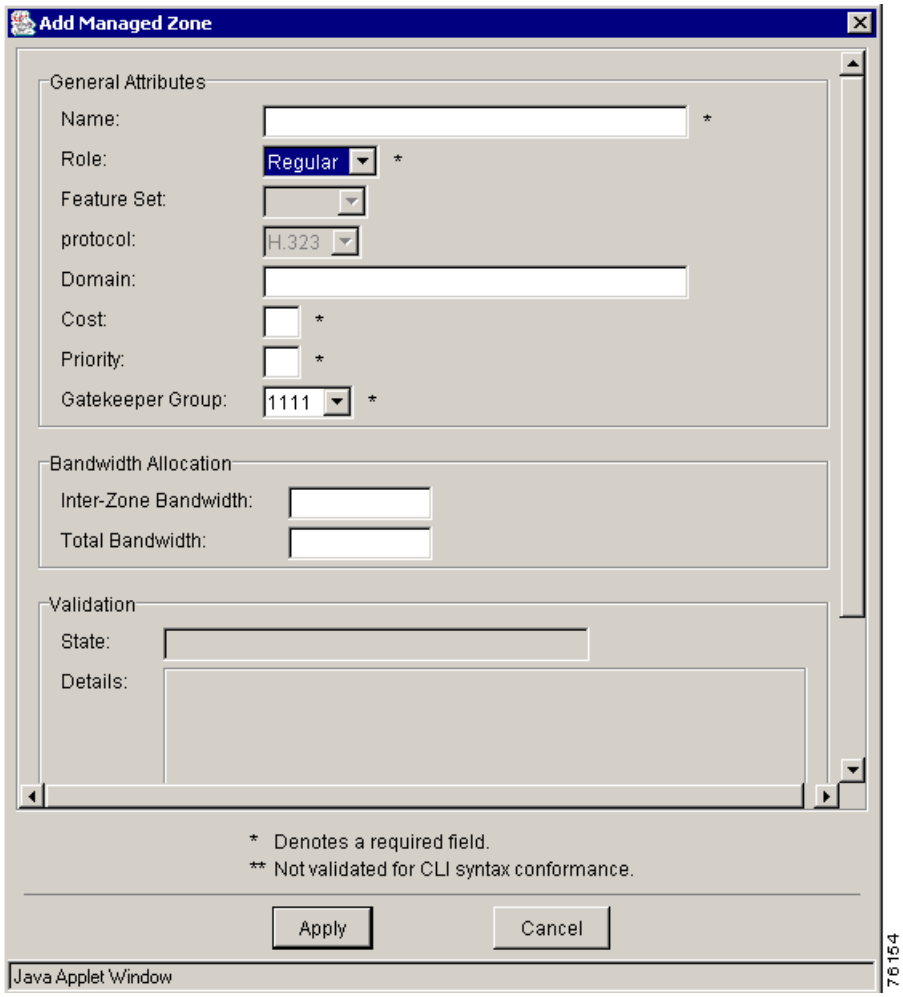
To add a managed zone to a region:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a region from the list you want to add a zone to.

Step 3 Right-click and choose **Add** and **Managed Zone** from the menus. The Add Managed Zone dialog box appears (Figure 5-16).

Figure 5-16 Add Managed Zone Dialog Box



Step 4 Enter the attribute information. See Table 5-8 for a description of each entry field.

Step 5 Click **Apply** to add the managed zone to the region or **Cancel**.

Note A managed zone must have a zone alias for each gatekeeper in the gatekeeper group. See the "Creating Zone Aliases" section on page 5-69.

Unmanaged Zones

An unmanaged zone is recognized by VRC but is not managed by VRC. It is a zone within a foreign region. A foreign region is outside the Administrative Domain (AD). You can add zone prefixes or hopoff technology prefixes to unmanaged zones.

Unmanaged Zone Attributes

Table 5-9 describes the attributes for unmanaged zones.

Table 5-9 Unmanaged Zone Attributes

General Attributes	Description
Name	The name of the zone. The maximum value is 64 characters.
Domain	The domain name of the zone (for example, cisco.com). The maximum value is 255 characters.
Cost	The cost associated with the zone. Values range from 1 to 99.
Priority	The piority associated with the zone. Values range from 1 to 99.
Foreign Domain	A read-only field that indicates whether this is a foreign domain.

Adding an Unmanaged Zone

To add an unmanaged zone to the dial plan:

Step 1 Expand the dial plan tree to view all components.

Step 2 Select the foreign region you want to add a unmanaged zone to.

Step 3 Right-click and choose **Add** and **Unmanaged Zone** from the menus. The Add Unmanaged Zone dialog box appears.

Step 4 Enter the unmanaged zone attribute information (see Table 5-9).

Step 5 Click **Apply** to add the unmanaged zone to the foreign region or **Cancel**.

Deleting a Zone

To delete a zone from the dial plan:

Step 1 Expand the dial plan tree to view all components.

Step 2 Select the zone that you want to remove.

Step 3 Right-click and choose **Delete**. Confirm your decision.

Note When you delete a managed zone, any remaining references to the zone might prevent a successful commit of the dial plan design. To locate residual references to the deleted zone, manually validate the design.

Step 4 Click **OK** to remove the zone or **Cancel**.

Modifying Local Zone Names

During the Discovery operation, VRC preserves local zone names when you generate a dial plan for:

- Alternate and cluster gatekeepers—The alternate and cluster gatekeeper's local zone names are associated with the managed zones in which the gatekeeper is the ARA.
- Primary and alternate directory gatekeepers—The local zone name is associated with the directory gatekeeper it came from.

During the Distribution and Commit operations, VRC configures associated gateways to use the zone alias. In certain dial plan configurations, you might be required to modify the local zone name for gatekeepers and directory gatekeepers.

- To modify the local zone name for a gatekeeper, you must create a zone alias for the zone where the gatekeeper resides.
- To modify the local zone name for a directory gatekeeper, you must modify its local zone name attribute.

This section describes how to modify a local zone name for a gatekeeper.

To modify a local zone name for a gatekeeper:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the managed zone which contains the gatekeeper whose local zone name you want to change.

Step 3 Create a zone alias for this zone.

a. Click the Zone Aliases tab.

b. Right-click and choose Add from the menu. The Add Zone Alias dialog box appears.

c. Enter the following values:

– Name - The local zone name for a zone for a particular gatekeeper. Maximum value is 64 characters. The name must be unique in the AD.

Note Note: If the gatekeeper referenced in this zone alias has the Type parameter set to primary or backup, and another gatekeeper in the same gatekeeper group is also a primary or backup, the zone alias in this zone must be identical for those two gatekeepers.

– Gatekeeper - The gatekeeper for which the local zone name is used. You can only choose from the gatekeepers in the gatekeeper group referenced by the zone associated with this alias.

d. Create a zone alias for the managed zone. The new local zone name (or zone alias) is applied to the gatekeepers in this zone.

This section describes how to modify a local zone name for a directory gatekeeper.

To modify the local zone name for a directory gatekeeper:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the directory gatekeeper that you want to modify the local zone name for.

Step 3 Click the **Attributes** tab.

Step 4 Click **Edit Attributes**.

Step 5 Modify the Local Zone Name entry field.

Step 6 Click **Apply**. The new local zone name (or zone alias) is applied to the directory gatekeeper.

Zone Parameters

This section describes the zone parameters that you must configure for your dial plan.

Zone Prefixes

A zone prefix is a dialed prefix that identifies the addresses to be serviced by a given gatekeeper. Zone prefixes are area codes and serve the same purpose as the domain names in the H.323-ID address space.

Adding a Zone Prefix

To add a zone prefix to a zone:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone to add a zone prefix to.

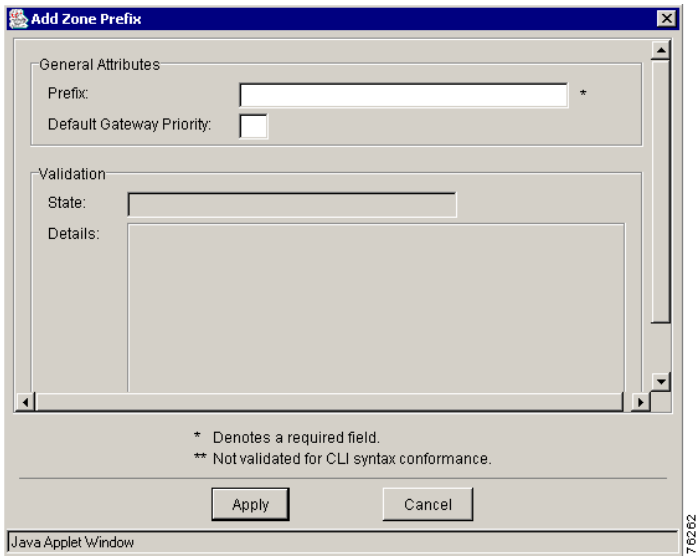
- For a managed zone, select a local zone.
- For a unmanaged zone, select a remote zone.

Step 3 Click the **Zone Prefixes** tab.

Step 4 Right-click and choose **Add** from the menu.

Step 5 The Add Zone Prefix dialog box appears (Figure 5-17).

Figure 5-17 Add Zone Prefix Dialog Box



Step 6 Enter the attribute information.

- Prefix—The zone prefix to support. The prefix field may be a string of up to 64 characters containing only digits, the asterisk (*) , or a period (.).

Note If the zone prefix is for a managed zone, it must be unique. Zone prefixes for a managed zone in the same gatekeeper group cannot be duplicated.

- Default gateway priority—The priority for this prefix in the managed zone. The range is 1 to 10. This cannot be set for an unmanaged zone. To add a gateway priority, see Adding a Gateway Priority for a Zone Prefix, page 5-48.

Step 7 Click **Apply** to add a zone prefix or **Cancel**.

Deleting a Zone Prefix

This section describes how to delete a zone prefix from a zone.

To delete a zone prefix:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone to delete.

Step 3 Right-click and choose **Delete** from the menu. The Delete Zone Prefix dialog box appears.

Step 4 Click **OK** to delete the zone prefix or **Cancel**.

Adding a Gateway Priority for a Zone Prefix

The gateway priority defines how the gatekeeper selects gateways in its local zone for calls to numbers beginning with the associated e164-prefix.

Note Do not use this option to set priority levels for a zone prefix assigned to a remote gatekeeper.

To assign a priority value for a zone prefix on a gateway:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone which contains the zone prefix you want to set a priority for.

Step 3 Click the **Zone Prefixes** tab.

Step 4 Double-click the zone prefix to set a gateway priority.

Step 5 Click the **Gateway Priorities** tab.

Step 6 Right-click and choose **Add** from the menu. Select a gateway you want to set a priority for. Repeat this procedure to assign a zone prefix priority for multiple gateways.

Step 7 Enter the priority value. The range is 1 to 10, with 1 being the highest priority. The default is 5.

Step 8 Click **Apply** to assign the zone prefix priority to the gateway or **Cancel**.

Zone Subnets

Zone subnets are used to configure a gatekeeper to accept discovery and registration messages sent by endpoints in designated subnets.

This section describes how to add a zone subnet to a gatekeeper and delete a zone subnet from a gatekeeper.

Adding a Zone Subnet

To add a zone subnet:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a zone to add a zone subnet to.

Step 3 Click the **Zone Subnets** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Zone Subnet dialog box appears.

Step 5 Enter the attribute information:

- Subnet—The IP address of the subnet. The default is blank. If this field is left blank, the local gatekeeper accepts discovery and registration requests from all subnets.
- Mask—The subnet mask. The default is zero. Values must be between 0 and 32.

Step 6 Click **Apply** to add a new zone subnet or **Cancel**.

Deleting a Zone Subnet

To delete a zone subnet from the dial plan:

Step 1 Expand the dial plan tree to view all components.

Step 2 Locate the zone which contains the zone subnet to delete.

Step 3 Right-click and choose **Delete** from the menu. The Delete Confirmation dialog box appears.

Step 4 Click **OK** to remove the zone subnet or **Cancel**.

Server Triggers

Server triggers allow you to configure your gatekeepers to:

- Connect to a specific back-end server
- Listen to any server that wants to connect to it

You can also set the triggers in the gatekeeper configuration so that they send only specified messages. Servers can also dynamically register their triggers with a gatekeeper.

Note Server triggers use the Gatekeeper Transaction Message Protocol (GKTMP) to communicate with servers other than Cisco IOS servers.

Adding a Server Trigger

To add server triggers to a zone:

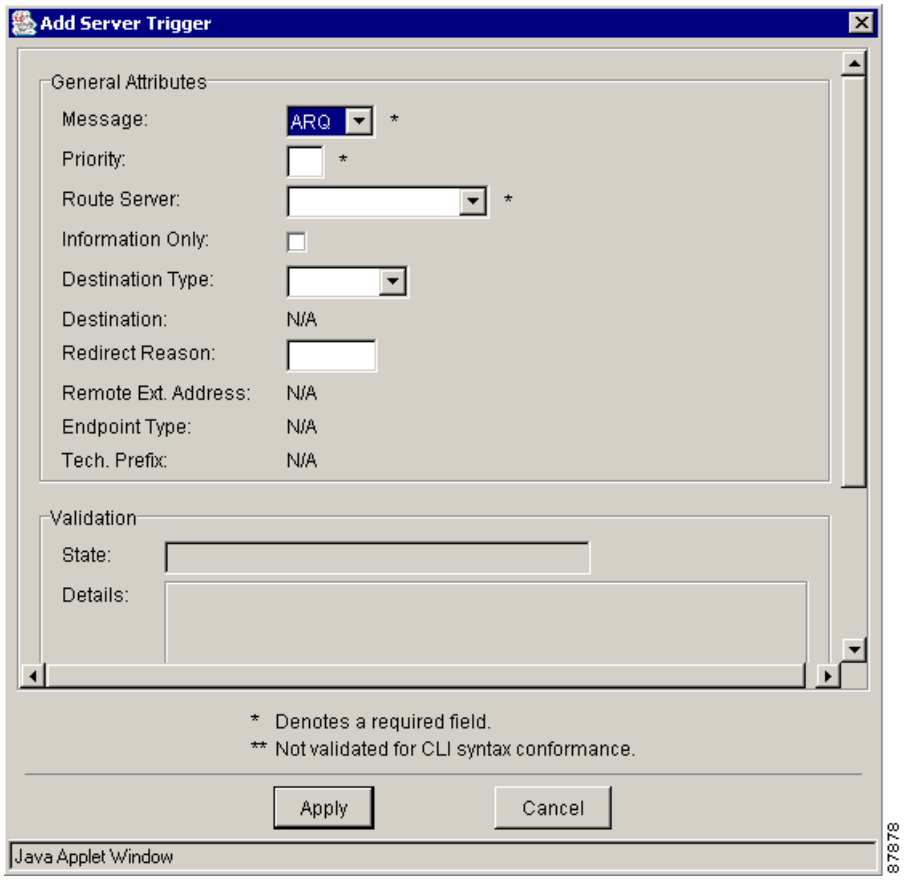
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate a zone or directory gatekeeper group to add a server trigger to.

Step 3 Click the **Server Triggers** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Server Trigger dialog box appears (Figure 5-18).

Figure 5-18 Add Server Trigger Dialog Box



Step 5 Enter the attribute information.

Table 5-10 describes the entry fields in the Server Trigger dialog box.

Table 5-10 Server Trigger Attributes

General Attributes	Description
Message	Configures triggering on RAS message types. Choose one message type from ARQ, DRQ, IRR, LCF, LRJ, LRQ, RAI, RRQ, or URQ. You can only choose IRR if one of the following conditions exists: • This server trigger is contained by a directory gatekeeper group with a VRC feature set of dp1.1 or later. • This server trigger is contained directly by a managed zone whose gatekeeper group attribute references a gatekeeper group with a VRC feature set of dp1.1 or later.
Priority	The priority for each trigger. The range is 1 to 20, with 1 being the highest priority.
Route Server	The route server associated with the gatekeeper for this server trigger.

Table 5-10 Server Trigger Attributes (continued)

General Attributes	Description
Information Only	Specifies whether this server trigger is for information only. There is no need to wait for acknowledgment.
Destination Type	Choose from e-mail, e164, or h323-id. You can only set this attribute if the message type is ARQ, LRQ, LCF, IRR, or LRJ. You must also specify destination information.
Destination	The value must be an address of the type specified by the destination type attribute.
Redirect Reason	Configure a redirect reason to trigger on if the message type is ARQ, IRR, or LRQ. The range is 0 to 65535. Reserved values are: 0–unknown, 1–call forwarding busy or called DTE busy, 2–call forwarded no reply, 4–call deflection, 9–called DTE out of order, 10–call forwarding by the call DTE, and 15–call forwarding unconditionally.
Remote Ext. Address	The remote extension address. The value can be any string up to 255 characters.
Endpoint Type	Choose from gatekeeper, h320-gateway, mcu, other gateway, proxy, terminal, voice-gateway.
Technology Prefix	The default technology prefix for this server trigger if the message type is RRQ or URQ.

Step 6 Click **Apply** to add a new server trigger or **Cancel**.

Deleting a Server Trigger

This section describes how to delete a server trigger.

To delete server triggers:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the zone that contains the server trigger to delete.

Step 3 Click the **Server Triggers** tab.

Step 4 Select the server trigger to delete.

Step 5 Right-click and choose **Delete** from the menu.

Step 6 Click **OK** to remove the server trigger from the dial plan or **Cancel**.

Creating Route Scopes

A route scope is a collection of voice ports grouped for routing purposes. The collection may be in the form of a single voice port, a trunk group, a hunt group, or an entire gateway.

Route scopes are assigned to routes to specify where the routes originate or terminate. For example, if a route scope of gateway is assigned to an ingress route, all voice ports on the gateway are configured to originate calls for that route. Similarly, if a route scope of type voice port is assigned to an egress route, only that voice port is configured to terminate the route.

Note You must create a route scope for a zone before you can set up ingress and egress routes.

To create a route scope for a zone:

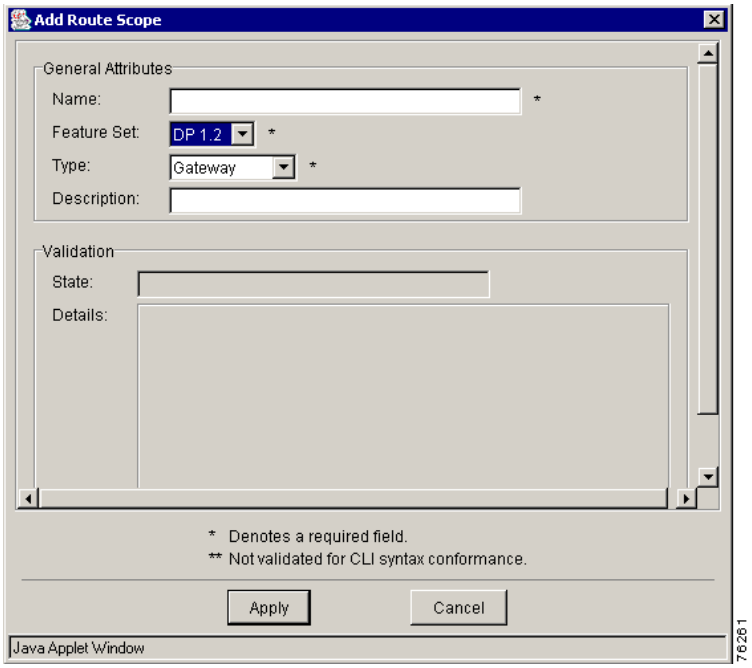
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone you want to create a route scope for.

Step 3 Click the **Route Scopes** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Route Scope dialog box appears (Figure 5-19).

Figure 5-19 Add Route Scope Dialog Box



Step 5 Enter the attribute information.

- Name—The name of the route scope. The maximum value is 64 characters.
- Feature Set—The VRC feature set supported by this route scope. The default is dp1.0.
- Type—Specifies where the routes in this route scope terminate. Choose from Gateway, Voice Port, Trunk Group, or Hunt Group. Trunk Group is not available if the feature set is dp1.0.
- Description—An optional text description of this route scope. The maximum value is 255 characters.

Step 6 Click **Apply** to create the route scope for the zone or **Cancel**.

Note During the Discovery operation, VRC might rename your route scope. To change the route scope name back after Discovery, you must manually edit this attribute in the Design View.

Deleting a Route Scope

When you delete a route scope, any remaining references to the route scope might prevent a successful commit of the dial plan design. To locate residual references to the deleted route scope, manually validate the design.

To delete a route scope from the dial plan:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the zone which contains the route scope that you want to delete.

Step 3 Click the **Route Scope** tab.

Step 4 Select the route scope to delete.

Step 5 Right-click and select **Delete** from the menu.

Step 6 Click **OK** to confirm the delete or **Cancel**.

Configuring Egress and Ingress Routes

This section describes egress and ingress routes, which represent the call routing paths entering or leaving a zone.

- An egress route defines an internal zone behavior for a call that is received from the IP network. An egress route specifies the subset of gateways that can terminate the call and the subset of interfaces on those gateways (for example, a set of voice ports), and also any required translations.
- An ingress route defines an internal zone behavior on the ingress side of the call, when the call is received from the PSTN. An ingress route specifies the address resolution authority (ARA) that is used to resolve the call destination (for example, the order might be: gatekeeper, OSP Server, and hairpinning back to the PSTN), and all required number translations.)

Note You must have a route scope defined for egress and ingress routes before you can add them to the dial plan.

Adding an Egress Route

An egress route represents the call path leaving the VoIP network to an egress gateway. You define egress routes at the zone level. An egress route:

- Defines an internal zone behavior for a call that is received from the IP network.
- Specifies the subset of gateways that can terminate the call and the subset of interfaces on those gateways (for example, a set of voice ports), and also any required translations.
- Encapsulates parameters necessary for both carrier-sensitive and prefix-based routing and other non-dial plan parameters such as codec or DTMF-relay.

To add an egress route:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a zone to add an egress route to.

Step 3 Click the **Egress Routes** tab. The Add Egress Route dialog box appears (Figure 5-20 and Figure 5-21).

Figure 5-20 Add Egress Routes Dialog Box (General Attributes)

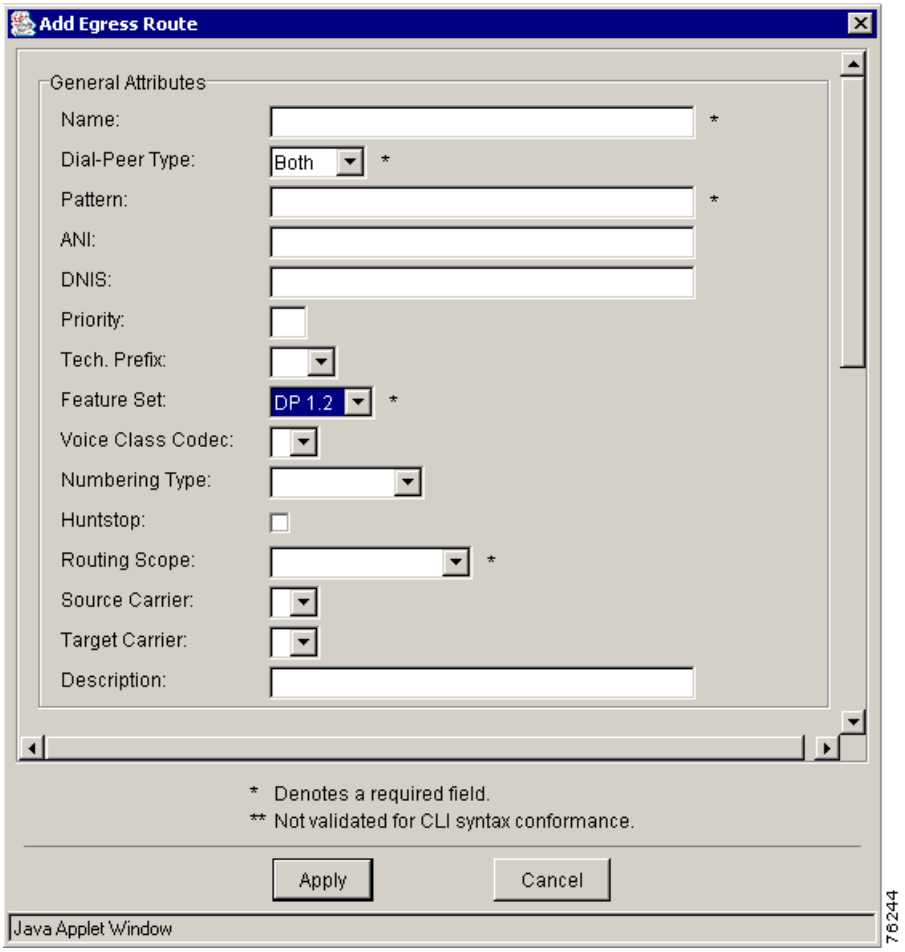
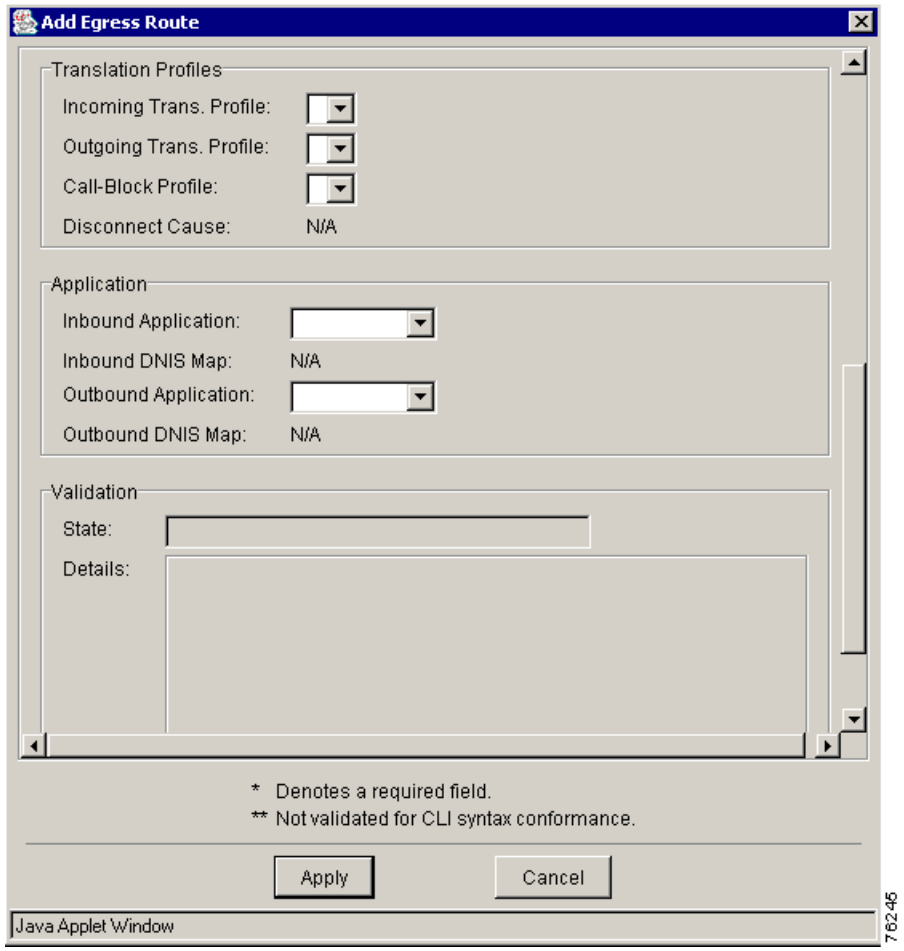


Figure 5-21 Add Egress Routes Dialog Box (Translation Profiles and Application)



Step 4 Enter the attribute information.

Table 5-11 describes the entry fields in the Add Egress Route dialog box.

Table 5-11 Add Egress Route Attributes

General Attributes	Description
Name	The name of the egress route. This name must be unique among all ingress and egress route names in the managed zone. Maximum value 64 characters.
Dial-Peer Type	Determines the dial peers created in the VRC-generated CLI. • Both - VRC configures an inbound POTS and an outbound VoIP dial peer for this route. • POTS - VRC configures a single POTS dial peer for this route. • VoIP - VRC configures a single VoIP dial peer for this route.

Table 5-11 Add Egress Route Attributes (continued)

General Attributes	Description
Pattern	The destination pattern, or dialed digit string supported by this route. Legal characters: ^[][0-9,ABCD#*.?+%()-^]*T?(\$)?$. The maximum value is 32 characters. This parameter is required if: • The dial peer type is POTS or both, AND the target carrier ID is not set, AND a tech prefix is not set. • The dial peer type is VoIP or both AND the DNIS is not set, AND the ANI is not set, AND the source carrier ID is not set.
ANI	The calling number for which this route is applicable. Legal characters: ^((\+)?([0-9,#*ABCD]+)\.*T?)$. The maximum value is 32 characters.
DNIS	The dialed number identification service (the called number). Legal characters: ^[][0-9,ABCD#*.?+%()-^]*T?(\$)?$. The maximum value is 32 characters.
Priority	The priority of this route. The range is 0 to 10, with 0 being the hightest priority. The default is 5.
Tech. Prefix	The technology prefix used for this route.
Feature Set	The VRC feature set supported by this egress route. The default is dp1.0.
Voice Class Codec	The Voice Class Codec used by the inbound VoIP dial peer.
Numbering Type	The numbering type. Choose from international, national, abbreviated, network, reserved, subscriber, and unknown. The default is blank.
Huntstop	Specifies whether to add a huntstop to the last dial peer in this route.
Routing Scope	The scope of this egress route. If you choose: • Managed zone—Zone must be the same zone to which this egress route belongs, and the VRC feature set of the zone must be the same as or better than the feature set of this egress route. • Route scope—VRC feature set of the route scope must be the same as or better than the feature set of this egress route.
Source Carrier	Specifies the carrier ID or trunk label for the inbound VoIP dial peer. This parameter can only be set if the VRC feature set is dp1.1 or later and the CSR route type of the AD is carrier or trunk-label.
Target Carrier	Specifies the carrier ID or trunk label for the outbound POTS dial peer. This parameter can only be set if the VRC feature set is dp1.1 or later and the CSR route type is carrier or trunk-label.
Description	An optional description of this egress route. The maximum value is 64 characters.
Translation Profiles	**Description**
Incoming Translation Profile	Associates a translation profile for the incoming side of gateway. If you set this optional parameter, the VRC feature set of this egress route must be dp1.1 or later. If you set this parameter, you must also reference a translation profile with a feature set of dp1.1 or later.

Table 5-11 Add Egress Route Attributes (continued)

General Attributes	Description
Outgoing Translation Profile	Associates a translation profile for the outgoing side of the gateway. If you set this optional parameter, the VRC feature set of the translation profile must match the VRC feature set of this egress route.
Call-Block Profile	Adds a call blocking profile to the inbound dial peer for this route. If you set this optional parameter, the VRC feature set of this egress route must be dp1.1 or later. You must also use a translation profile with a feature set of dp1.1 or later.
Disconnect Cause	You must set this if a call blocking profile is set. Choose from call-rejected, invalid-number, unassigned-number, or user-busy.
Application	**Description**
Inbound Application	An inbound voice application in this zone to be applied to this ingress route. You can only set this parameter if the dial peer type is set to VoIP or both.
Inbound DNIS Map	The DNIS map to apply to the inbound application. You can only set this parameter if the dial peer type is both or VoIP AND you have set an inbound application for this route.
Outbound Application	An outbound voice application in this zone to be applied to this ingress route. You can only set this parameter if the dial peer type is set to POTS or both.
Outbound DNIS Map	The DNIS map to apply to the outbound application. You can only set this parameter if the dial peer type is both or POTS AND you have set an outbound application for this route.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Step 5 Click **Apply** to add the egress route to the zone or **Cancel**.

Deleting an Egress Route

To delete an egress route:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone where the egress route resides.

Step 3 Click the **Egress Routes** tab.

Step 4 Select the egress route to delete.

Step 5 Right-click and choose Delete from the menu.

Step 6 Click **OK** to remove the egress route from the dial plan or **Cancel**.

Adding an Ingress Route

An ingress route represents the call path entering the VoIP network ingress gateways to their ARA. An ingress route:

- Defines an internal zone behavior on the ingress side of the call, when the call is received from PSTN.
- Specifies the ARA that is used to resolve the call destination (that is, it could be in the following order: gatekeeper, OSP Server, hairpinning back to PSTN), and all required number translations, such as preferred target carrier ID.
- Encapsulates non-dial plan parameters such as direct inward dial (DID), applications, and codec.

To add an ingress route:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a zone to add an ingress route to.

Step 3 Click the **Ingress Routes** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Ingress Route dialog box appears (Figure 5-22 and Figure 5-23).

Figure 5-22 Add Ingress Route Dialog Box (General Attributes)

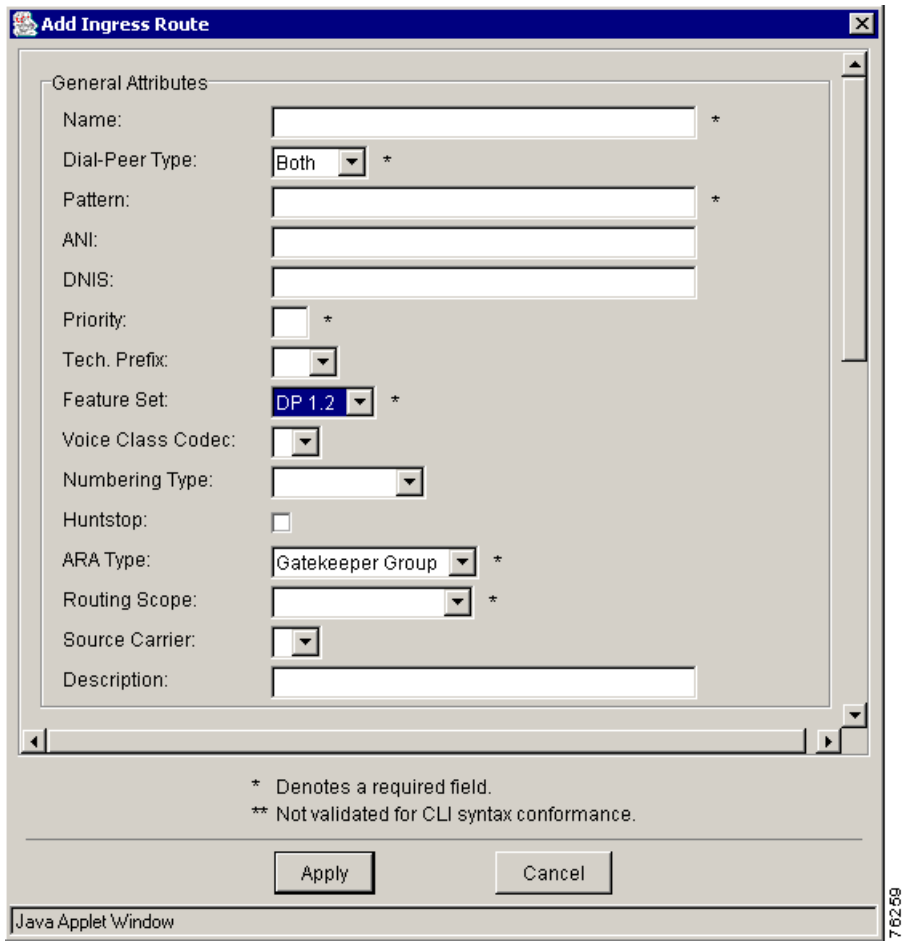
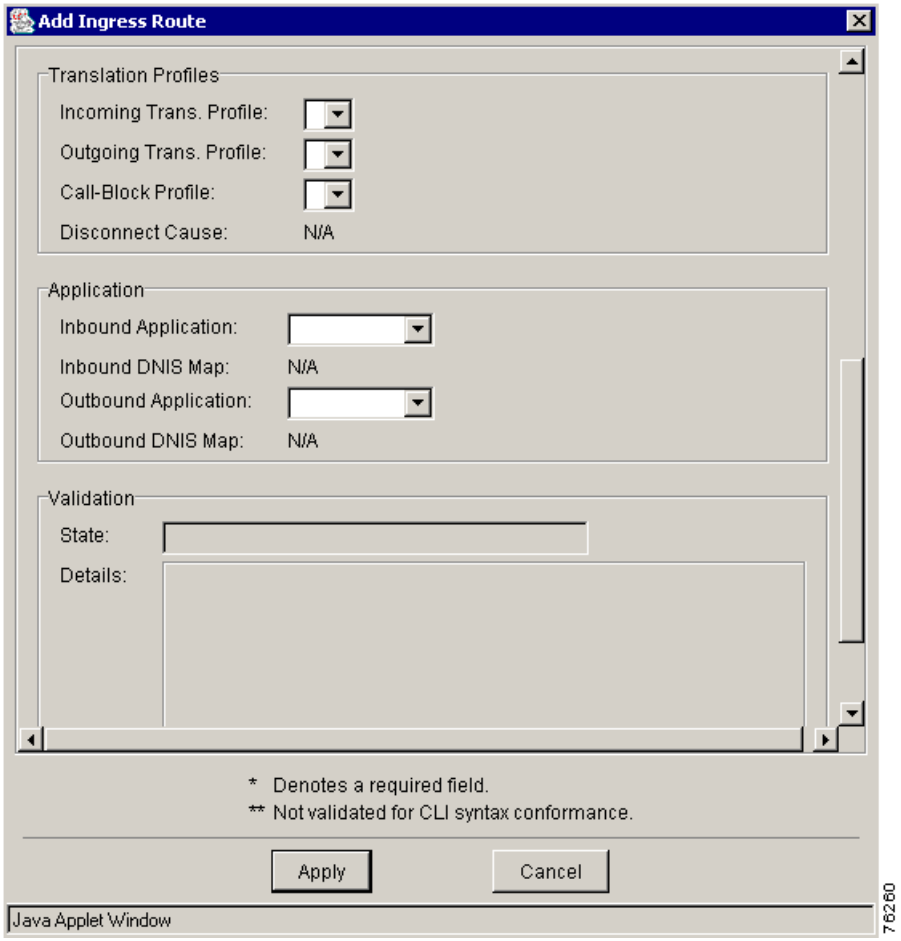


Figure 5-23 Add Ingress Route Dialog Box (Translations Profiles and Application)



Step 5 Enter the attribute information.

Table 5-12 describes the entry fields in the Add Ingress Route dialog box.

Table 5-12 Add Ingress Route Attributes

General Attributes	Description
Name	The name of the egress route. This name must be unique among all ingress and egress route names in the managed zone. Maximum value 64 characters.
Dial-Peer Type	Determines the dial peers created in the VRC-generated CLI. • Both - VRC configures an inbound POTS and an outbound VoIP dial peer for this route. • POTS - VRC configures a single POTS dial peer for this route. • VoIP - VRC configures a single VoIP dial peer for this route.

Table 5-12 Add Ingress Route Attributes (continued)

General Attributes	Description
Pattern	The destination pattern, or dialed digit string supported by this route. Legal characters: ^[][0-9,ABCD#*.?+%()-^]*T?(\$)?$. The maximum value is 32 characters. This parameter is required if: • The dial peer type is POTS or both, AND the target carrier ID is not set, AND a tech prefix is not set. • The dial peer type is VoIP or both AND the DNIS is not set, AND the ANI is not set, AND the source carrier ID is not set.
ANI	The calling number for which this route is applicable. Legal characters: ^((\+)?([0-9,#*ABCD]+)\.*T?)$. The maximum value is 32 characters.
DNIS	The dialed number identification service (the called number). Legal characters: ^[][0-9,ABCD#*.?+%()-^]*T?(\$)?$. The maximum value is 32 characters.
Priority	The priority of this route. The range is 0 to 10, with 0 being the hightest priority. The default is 5.
Tech. Prefix	The technology prefix used for this route.
Feature Set	The VRC feature set supported by this egress route. The default is dp1.0.
Voice Class Codec	The Voice Class Codec used by the inbound VoIP dial peer.
Numbering Type	The numbering type. Choose from international, national, abbreviated, network, reserved, subscriber, and unknown. The default is blank.
Huntstop	Specifies whether to add a huntstop to the last dial peer in this route.
ARA Type	The address resolution authority to use for this route. Choose from one of the following: • OSP Server—OSP server associated with the zone assigns the route to a gateway. • GKGrp—RAS assigns the route to a gateway. • ipv4—A route parameter assigns the route to a gateway.
Routing Scope	The scope of this egress route. If you choose: • Managed zone—Zone must be the same zone to which this egress route belongs, and the VRC feature set of the zone must be the same as or better than the feature set of this egress route. • Route scope—VRC feature set of the route scope must be the same as or better than the feature set of this egress route.
Source Carrier	Specifies the carrier ID or trunk label for the inbound VoIP dial peer. This parameter can only be set if the VRC feature set is dp1.1 or later and the CSR route type of the AD is carrier or trunk-label.
Target Carrier	Specifies the carrier ID or trunk label for the outbound POTS dial peer. This parameter can only be set if the VRC feature set is dp1.1 or later and the CSR route type is carrier or trunk-label.

Table 5-12 Add Ingress Route Attributes (continued)

General Attributes	Description
Description	An optional description of this egress route. The maximum value is 64 characters.
Translation Profiles	**Description**
Incoming Translation Profile	Associates a translation profile for the incoming side of gateway. If you set this optional parameter, the VRC feature set of this egress route must be dp1.1 or later. If you set this parameter, you must also reference a translation profile with a feature set of dp1.1 or later.
Outgoing Translation Profile	Associates a translation profile for the outgoing side of the gateway. If you set this optional parameter, the VRC feature set of the translation profile must match the VRC feature set of this egress route.
Call-Block Profile	Adds a call blocking profile to the inbound dial peer for this route. If you set this optional parameter, the VRC feature set of this egress route must be dp1.1 or later. You must also use a translation profile with a feature set of dp1.1 or later.
Disconnect Cause	You must set this if a call blocking profile is set. Choose from call-rejected, invalid-number, unassigned-number, or user-busy.
Application	**Description**
Inbound Application	An inbound voice application in this zone to be applied to this ingress route. You can only set this parameter if the dial peer type is set to VoIP or both.
Inbound DNIS Map	The DNIS map to apply to the inbound application. You can only set this parameter if the dial peer type is both or VoIP AND you have set an inbound application for this route.
Outbound Application	An outbound voice application in this zone to be applied to this ingress route. You can only set this parameter if the dial peer type is set to POTS or both.
Outbound DNIS Map	The DNIS map to apply to the outbound application. You can only set this parameter if the dial peer type is both or POTS AND you have set an outbound application for this route.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Step 6 Click **Apply** to a add a new ingress route or **Cancel**.

Deleting an Ingress Route

To delete an ingress route:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone where the ingress route resides.

Step 3 Click the **Ingress Routes** tab.

Step 4 Select the ingress route to delete.

Step 5 Right-click and choose **Delete** from the menu.

Step 6 Click **OK** to remove the ingress route from the dial plan or **Cancel**.

Rule Descriptions

Rule descriptions define sets of translation rules for a zone. The rules provide a mechanism to perform digit manipulation.

This section describes how to add and delete rule descriptions.

Adding a Rule Description

To add a rule description:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a zone to add a rule description to.

Step 3 Click the **Rule Descriptions** tab.

Step 4 Right-click and choose **Add** from the menu.

Step 5 Enter the attribute information.

- Tag—The tag number by which the rule set is referenced.
  - The range is 1 to 10 if the VRC feature set or the parent rule description is dp1.0.
  - The range is 1 to 15 if the VRC feature set of the parent rule description is dp1.1 or later.
- Feature Set—The VRC feature set supported by this rule description. The default is dp1.0.

Step 6 Click **Apply** to add the rule description or **Cancel**.

Deleting a Rule Description

To delete a rule description:

Step 1 Expand the dial plan tree to view all components.

Step 2 Select the zone where the rule description resides.

Step 3 Click the **Rule Descriptions** tab

Step 4 Select the rule description to delete.

Step 5 Right-click and choose **Delete** from the menu. The delete confirmation dialog box appears.

Step 6 Click **OK** to remove the rule description from the dial plan or **Cancel**.

Adding a Translation Rule

Translation rules apply a set of rules to a calling party number (Automatic Number Identification [ANI]) or a called party number (Dial Number Information Service [DNIS]) for both incoming and outgoing calls within Cisco H.323 voice-enabled gateways.

To add a translation rule:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select the zone which contains the rule description that you want to add a translation rule to.

Step 3 Click the **Rule Descriptions** tab. The list of rule descriptions for this zone is displayed.

Step 4 Double-click the rule description that you want to add a translation rule to.

Step 5 Click the **Rules** tab.

Step 6 Right-click and choose **Add** from the menu.

Step 7 Enter the rule description attributes.

Table 5-13 describes the entry fields in the Add Rule dialog box.

Table 5-13 Attributes of the Add Rule Dialog Box

General Attributes	Description
Number	The number assigned to this translation rule. The range is: • 1 to 10 if the VRC feature set for the parent rule description is dp1.0. • 1 to 15 if the feature set of the parent rule description is dp1.1 or later.
Reject	This optional parameter can only be set if the parent translation rule has a feature set of dp1.1 or later.
Search Pattern	The maximum value is 32 characters.
Replacement Pattern	This parameter is required if the Reject parameter is not set. The maximum value is 32 characters.
Match Type	The match type for this translation rule. Choose from any, international, national, abbreviated, network, reserved, subscriber, and unknown. You must also set a replacement type.
Replacement Type	The replacement type for this translation rule. Choose from international, national, abbreviated, network, reserved, subscriber, and unknown. This parameter must be set if the Match Type parameter is set and the Reject parameter is not set.
Match Plan	Specifies the match plan for the Match Type parameter. Choose from any, data, ermes, isdn, national, private, reserved, telex, and unknown. This parameter can only be set if the parent rule description has a feature set of dp1.1 or later.
Replace Plan	Specifies the match plan for the Match Type parameter. This parameter must be set if the Match Type parameter is set and the Reject parameter is not set. Choose from data, ermes, isdn, national, private, reserved, telex, and unknown. This parameter can only be set if the parent rule description has a feature set of dp1.1 or later.

Table 5-13 Attributes of the Add Rule Dialog Box (continued)

General Attributes	Description
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Step 8 Click **Apply** to add this translation rule to the rule description or **Cancel**.

Translation Profiles

Translation profiles provide a way to group ANI and DNIS translation rules together to use on ingress or egress routes.

You must have your rule descriptions set up before you can add them to a translation profile.

Adding a Translation Profile

To add a translation profile to a dial plan:

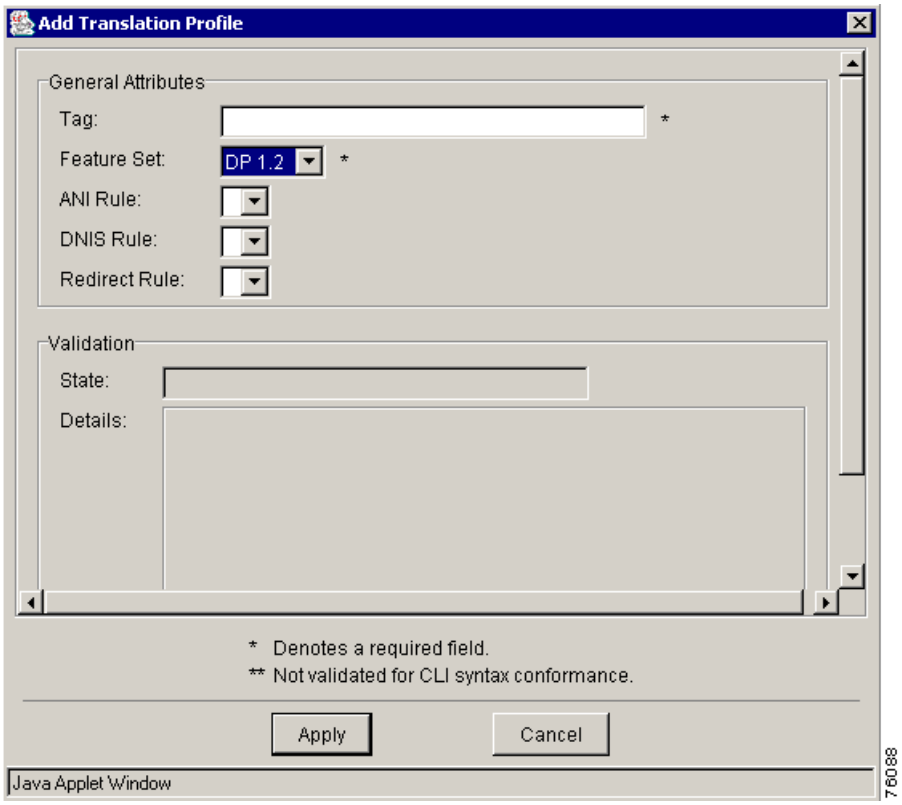
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a zone to add a translation profile to.

Step 3 Click the **Translation Profiles** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Translation Profile dialog box appears (Figure 5-24).

Figure 5-24 Add Translation Profile Dialog Box



Step 5 Enter the attribute information.

Table 5-14 describes the fields in the Add Translation Profile dialog box.

Table 5-14 Translation Profile Attributes

General Attributes	Description
Tag	A unique ID for this rule description. The maximum value is 31 characters.
Feature Set	The VRC feature set for this translation profile. The default is dp1.0.
ANI Rule	The ID of the rule description meant for ANI. Choose from the available ANI rules in the drop-down list. You must reference a rule description with the same feature set as this translation profile.
DNIS Rule	The ID of the rule description meant for DNIS. You must reference a rule description with the same feature set as this translation profile.
Redirect Rule	You can set this optional parameter if the feature set of this translation profile is dp1.1 or later. You must reference a rule description with a feature set of dp1.1 or later.
Validation State	Indicates whether the Cisco VRC server can contact the element during the Validation process.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.

Step 6 Click **Apply** to add a new translation profile or **Cancel**.

Deleting a Translation Profile

Note When you delete a translation profile, any remaining references to the translation profile might prevent a successful commit of the dial plan design. To locate residual references to the deleted translation profile, manually validate the design.

To delete a translation profile from a dial plan:

Step 1 Locate the zone that contains the translation profile.

Step 2 Click the **Translation Profiles** tab.

Step 3 Select the translation profile to delete.

Step 4 Right-click and choose **Delete** from the menu. The translation profile is deleted.

Managing Number Expansion Sets

In most corporate environments, the telephone network is configured so that you can reach a destination by dialing only a portion of the full telephone number. You can define an extension number as the destination pattern for a dial peer.

Adding a number expansion set enables you to define a set of digits for the router to add to the beginning of a dialed string before passing it to the remote telephony device. This reduces the number of digits that a user must dial to reach a remote location.

Adding a Number Expansion Set

Note You must specify number expansion rules for all number expansion sets added to the dial plan.

To add a number expansion set:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Select a zone to add a number expansion set to.

Step 3 Click the **Number Expansion Sets** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Number Expansion Set dialog box appears.

Step 5 Enter the name of a number expansion set. The maximum value is 64 characters.

Step 6 Click **Apply** to add the number expansion set or **Cancel**.

Deleting a Number Expansion Set

To delete a number expansion set from a zone:

Step 1 Locate the zone which contains the number expansion set you want to delete.

Step 2 Click the **Number Expansion Sets** tab.

Step 3 Right-click and choose **Delete** from the menu. The number expansion set is deleted.

Adding Number Expansion Rules

To add a number expansion rule for a number expansion set:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the zone which contains the number expansion set you want to add a number expansion rule for.

Step 3 Click the **Number Expansion Sets** tab. The list of number expansion sets for this zone is displayed.

Step 4 Double-click the number expansion set you want to add a number expansion rule to.

Step 5 Click the **Rules** tab.

Step 6 Click **Add Rule**.

Enter the number expansion rule attribute information.

- Number—Must be an integer between 0 and 2147483647.
- Search Pattern—Value can be a string up to 32 characters.
- Replacement Pattern—Value can be a string up to 32 characters.

Step 7 Click **Apply** to add the number expansion rule or **Cancel**.

Deleting Number Expansion Rules

Note When you delete a number expansion rule, any remaining references to the number expansion rule might prevent a successful commit of the dial plan design. To locate residual references to the deleted number expansion rule, manually validate the design.

To delete a number expansion rule:

Step 1 Select the zone which contains the number expansion set you want to delete the number expansion rule from.

Step 2 Click the **Number Expansion Sets** tab. The list of number expansion sets for this zone is displayed.

Step 3 Double-click the number expansion set which contains the number expansion rule you want to delete.

Step 4 Click the **Rules** tab. Select the number expansion rule you want to delete.

Step 5 Right-click and choose **Delete** from the menu. The rule is deleted from the number expansion set.

Creating Zone Aliases

A zone alias is the name a gatekeeper assigns to a local zone name. VRC creates a zone alias during the Discovery operation or you can enter a zone alias manually.

When a gateway registers with a gatekeeper, it uses the zone alias name. A managed zone must have one zone alias for every gatekeeper in the gatekeeper group.

To manually create a zone alias for a zone:

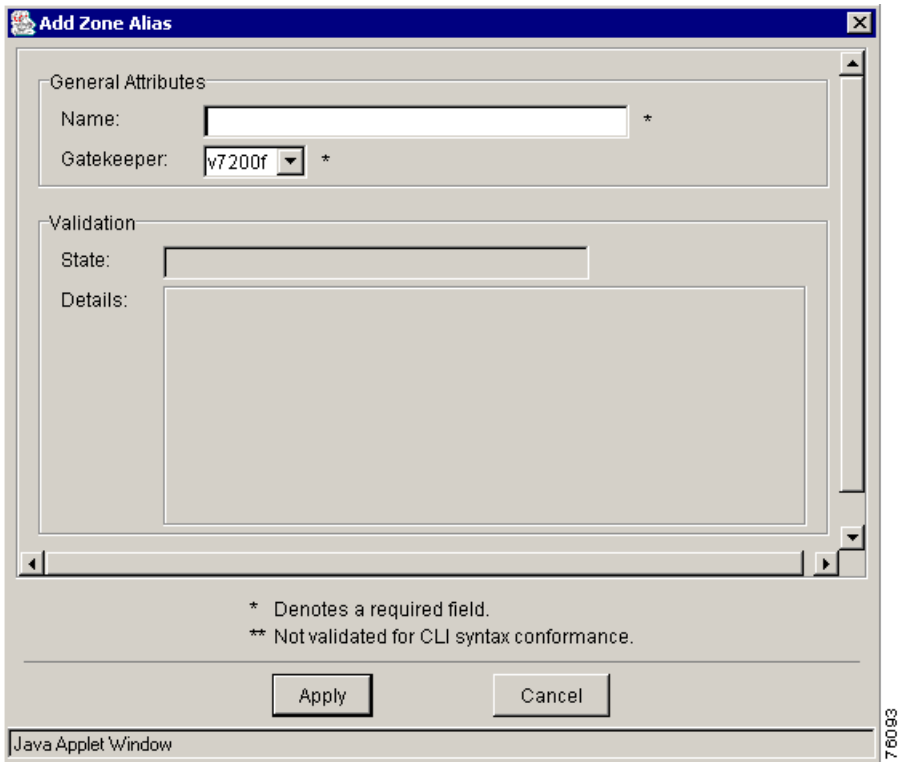
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the zone that you want to create a zone alias for.

Step 3 Click the **Zone Aliases** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Zone Alias dialog box appears (Figure 5-25).

Figure 5-25 Add Zone Alias Dialog Box



Step 5 Enter the attribute information.

- Name—Local zone name for a zone for a particular gatekeeper. The name must be unique among connected regions. The maximum value is 64 characters.

- Gatekeeper—Gatekeeper for which the local zone name is used. You can only choose from the gatekeepers in the gatekeeper group referenced by the zone associated with this alias.

Step 6 Click **Apply** to create the zone alias or **Cancel**.

Managing a Source Group

A source group is a template for setting individual voice source groups. A source group allows you to set the same parameters for all gateways in a zone. The parameters set in a zone's source group are used when you add a voice source group to the gateway.

To apply these parameters to a particular gateway in a zone, see Adding a Voice Source Group, page 5-83.

Creating a Source Group

To create a source group for a zone:

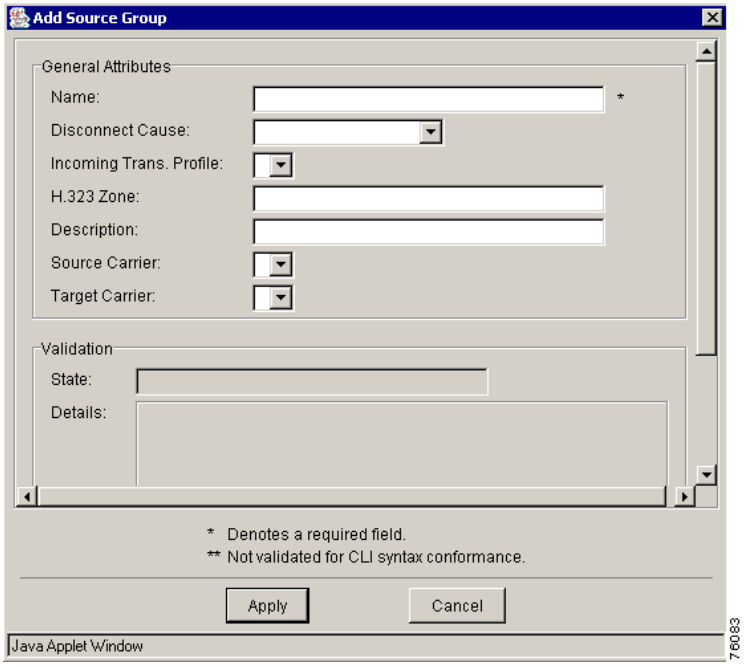
Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the zone to add a source group to.

Step 3 Click the **Source Group** tab.

Step 4 Right-click and select **Add** from the menu. The Add Source Group dialog box appears (Figure 5-26).

Figure 5-26 Add Source Group Dialog Box



Step 5 Enter the attribute information.

Table 5-15 describes the entry fields in the Add Source Group dialog box.

Table 5-15 Source Group Attributes

General Attributes	Description
Name	The name of the source group. The maximum value is 31 characters.
Disconnect Cause	Reason for disconnecting. Choose from call-rejected, invalid-number, unassigned-number, user-busy.
Incoming Translation Profile	Associates a translation profile for the incoming side of the gateway. The VRC feature set of the translation profile must be dp1.1 or later.
H.323 Zone	The maximum value is 127 characters.
Description	The maximum value is 63 characters.
Source Carrier	Specifies the inbound VoIP dial peer. Can only be set if the CSR route type of the AD is set to carrier or trunk-label.
Target Carrier	Specifies the outbound POTS dial peer. Can only be set if the CSR route type of the AD is set to carrier or trunk-label.

Step 6 Click **Apply** to add a source group or **Cancel**.

Deleting a Source Group

To delete a source group from a zone:

Step 1 Expand the dial plan tree to view all components.

Step 2 Locate the zone to delete the source group from.

Step 3 Click the **Source Group** tab.

Step 4 Locate the source group that you want to delete.

Step 5 Right-click and choose **Delete** from the menu.

Step 6 Click **OK** to delete the source group from a dial plan or **Cancel**.

Managing Hopoff Technology Prefixes

A hopoff zone is the point at which a call transitions from H.323 to a non-H.323 network. A hopoff technology prefix allows you to specify a technology prefix for a certain zone that you want to use as a hopoff zone. You can specify a hopoff technology prefix for a managed zone or an unmanaged zone.

Note You must already have a technology prefix added to the dial plan before you can specify it for a hopoff zone and you must be in the Design View.

To add a hopoff technology prefix to a zone:

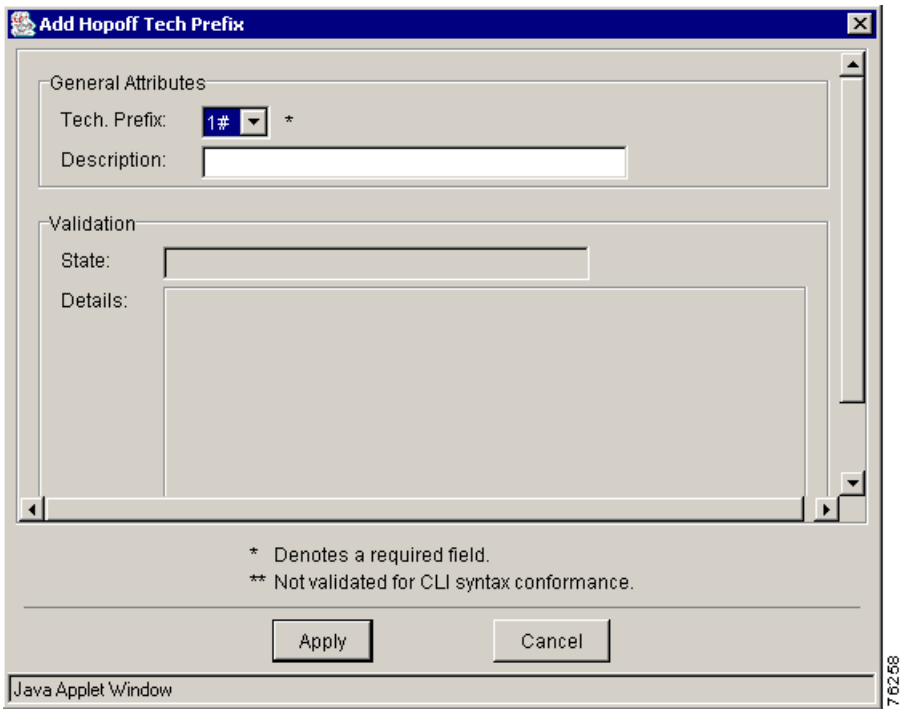
Step 1 Expand the dial plan tree to view all components.

Step 2 Select a zone to add a hopoff technology prefix to.

Step 3 Click the **Hopoff Tech Prefixes** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Hopoff Tech Prefix dialog box appears (Figure 5-27).

Figure 5-27 Add Hopoff Tech Prefix Dialog Box



Step 5 Enter the attribute information.

- Technology Prefix—Select one predefined technology prefix from the list.

Note If you are specifying a hopoff technology prefix for a managed zone, then the managed zone must contain at least one egress route that references this same technology prefix.

- Description—This optional field is a text description of this hopoff technology prefix. The maximum value is 255 characters.

Note A zone can have multiple hopoff technology prefixes.

Step 6 Click **Apply** to add the hopoff technology prefix or **Cancel** .

Gateways

This section contains the following topics about gateways:

Description

A gateway (GW) is a Network Access Server (NAS) which acts as an interface between a circuit-switched Public Switched Telephone Network (PSTN) and a packetized H.323 Voice-over-IP (VoIP) network. It is a network element in a dial plan that VRC manages.

A gateway is the point at which a circuit-switched fax or voice call is encoded (using a codec) and repackaged into IP packets, or vice versa. A gateway initiates a call setup with an H.323 gatekeeper through H.225 RAS. The originating gateway terminates the VoIP call to an appropriate destination gateway with the gatekeeper's assistance.

You can perform the following tasks when using VRC:

- Add hunt groups and voice source groups to a gateway
- Edit voice port and trunk group attributes

The VRC network supports the following Cisco platforms as H.323 gateways:

- Cisco 1750 Access Router
- Cisco Catalyst 2600 Series Routers
- Cisco 3600 Series Routers
- Cisco AS5300 Series Universal Access Server
- Cisco AS5350 Universal Gateway
- Cisco AS5400 Series Universal Gateways
- Cisco AS5800 Series Universal Access Servers
- Cisco AS5850 Universal Gateway
- Cisco 7200 Series Routers

Gateway Attributes

To view the attributes of a gateway, select the gateway in the dial plan tree. Table 5-16 describes the attributes of a gateway.

Table 5-16 Gateway Attributes

General Attributes	Description
Name	The gateway name. This corresponds to the name part of the full DNS host name.
H.323 ID	The H.323-ID for the gateway. This is usually the fully qualified e-mail ID, with the domain name being the same as this gateway's gatekeeper.
IP Address	The IP address of the gateway. This read-only field is populated by the VRC client.
Feature Set	The VRC feature set supported by this gateway. This field is populated by VRC when the gateway is added to the dial plan.
IOS Version	The Cisco IOS version running on this gateway.
Incoming VoIP Trans. Profile	Associates a translation profile for the incoming side of gateway. The translation profile must reside in the same managed zone as the gateway. The VRC feature set of the translation profile must match the feature set of the gateway.
Number Expansion Set	The number expansion set for this gateway.
OSP Enabled	Specifies if this gateway responds to OSP servers.
Circuit	Assigns a trunk label or carrier ID (circuit-ID) to a gateway. You can only set this parameter if the gateway's VRC feature set is dp1.1 or later, the managed zone's gatekeeper group is set to a gatekeeper group with a VRC feature set of dp1.1 or later *and* a CSR route type of carrier or trunk-label.
Max. Calls	Specifies the maximum number of voice or data calls allowed on the trunk group. You can only set this parameter if the circuit parameter is set. The range is 1 to 10000.
Needs Reactivation	This is a read-only field and indicates whether you need to reactivate the gateway because the configuration has been changed. The default is Yes. You cannot commit a dial plan design if one or more gateways have this attribute set to Yes.
RTCP	
Timer Receive RTCP	Enables the Real-Time Control Protocol (RTCP) timer and configures a multiplication factor for the RTCP timer interval. The range is 2 to 1000. This parameter can only be set if the VCR feature set for this gateway is dp1.1 or later.
IP RTCP Report Interval	Configures the average reporting interval between subsequent RTCP report transmission. The range is 1 to 65535. This parameter can only be set if the VCR feature set for this gateway is dp1.1 or later.

Table 5-16 Gateway Attributes (continued)

General Attributes	Description
Status	Indicates whether the Cisco VRC server can contact the elements during the Validation process. • OK—The last validation detected no warnings or errors. • Warning—The last validation detected one or more warnings that you might be required to correct before you commit the dial plan, depending on your intent of the dial plan design. • Fatal—The last validation detected one or more errors that you must correct before you commit the dial plan.
Details	An optional text string that gives more details about the status of the element. The maximum value is 255 characters.
Security	
Access Token	A password for registration. The maximum value is 20 characters. The default is blank.
Security Level	The security level of the gateway. You must set a security level if the access token is set. Choose from endpoint, per-call, or all.
Resource Management	
Resource Threshold All	Applies the high and low parameter settings to all monitored H.323 resources. This parameter can only be set if Resource Threshold High and Resource Threshold Low are set.
Resource Threshold High	A resource utilization level that triggers an RAI message that indicates that H.323 resource usage is high. The range is 1 to 100. The default is blank.
Resource Threshold Low	A resource utilization level that triggers an RAI message that indicates that H.323 resource usage has dropped below the high usage level. The range is 1 to 100. The default is blank.
Emulate H.323 Bandwidth	If checked, allows the gateway to terminate calls using H.323 bidirectional bandwidth. This parameter can only be set if the VCR feature set for this gateway is dp1.1 or later.

Adding a Gateway to the Dial Plan

A gateway must be defined in the topology before you can add it to the dial plan.

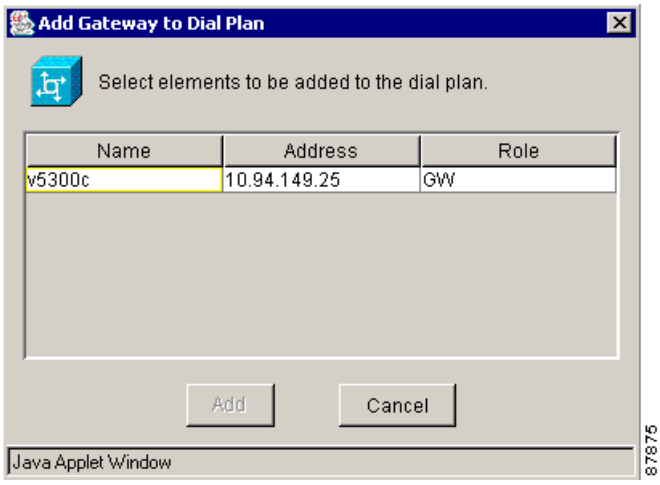
To add a gateway to the dial plan:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the managed zone to add a gateway to.

Step 3 Right-click and choose **Add** and **Gateway** from the menu. The Add Gateway to Dial Plan dialog box appears (). This dialog box lists the IP addresses of available gateways.

Figure 5-28 Add Gateway Dialog Box



Step 4 Select gateway and click the **Add** button. An information dialog box appears, asking you to confirm.

Step 5 Click **Add** to add the gateway or **Cancel** .

Step 6 To edit gateway attributes, click the **Edit Attributes** button.

Finding Terminating Gateways

You can identify and list the set of gateways which might terminate a given dial string. For more information, see Finding Terminating Gateways, page 4-7.

Call Path Verification

The call path verification feature in VRC is used to trace a call in a Voice-over-IP (VoIP) H.323 network. The call is traced from the originating gateway, through all gatekeepers used to resolve the destination address, and finally to the terminating gateway.

Note Routes identified with target ipv4.* or dns.* are reported but not traced or verified by VRC.

To trace the call path using VRC, you must enter the following information:

- **Call source**—Choose the ingress gateway, or the voice port or trunk group for the ingress gateway.

  The call source is the device from which the call is traced. It is always a gateway, but you can provide more details by selecting the trunk group or the voice port through which the call was received.

  Rules to follow when choosing the call source:

  - Select the interface for which translation rules are defined so that the translation rules can be applied to the called number.

  - Do not define the translations for both trunk groups and voice ports. With this configuration, the router executes the voice port rules and ignores the trunk group rules. VRC does not have enough information to tie voice port rules with trunk group rules and cannot determine which rules to apply.
  - If there are no translation rules defined on voice ports or trunk groups, and you are using carrier-based routing, then select the trunk group. The source carrier determined by the trunk group has a direct affect on the call routing.
- **DNIS**—The number received from the Public Switched Telephone Network (PSTN) by the originating gateway. It can contain the technology prefix, if it is present in the original number.
- **Target Carrier**—Select from the list of target carriers defined in the Administrative Domain (AD). This is not required if the CSR route type of the AD is set to None (for prefix routing only).

  Rules to follow when choosing the target carrier:

  - You cannot configure a target carrier on the originating gateway, but it can be added to the call path by the routing server if your system is configured to use one.
  - VRC cannot contact the route server to query for the target carrier information for the given entry parameters (source carrier, time of day, current traffic patterns).

    However, you can presume the target carrier that the routing server would select under the current conditions. VRC verifies that all devices in the path are correctly configured to route and terminate the call. If the routing server would return, as a result of a query, the terminating gateway (thus shortening the routing path and not requiring the correct gatekeeper configuration), the system configured by VRC should have all gatekeeper connectivity in place.

Note The target carrier setting is optional. If you leave this field blank, you test the behavior of the system with the routing server down or not used.

- **Translation Profiles**—The translation profiles applied during call path verification are determined bythe source of the call path verification request. You do not select them.
- **Translation Rules**—The following translation rules are executed to trace a call path:
  - Voice port translation rules (only if you select a voice port)
  - Trunk group translation rules (only if you select a trunk group)

    You receive a warning if there are voice port rules defined.
  - Ingress gateway number expansions
  - Ingress route inbound translation rules
  - Ingress route outbound translation rules
  - Egress gateway number expansions
  - Egress gateway VoIP translation rules

Note VRC call path verification does not recognize voice source groups, their translation rules, or ingress route call blocking.

- **Call Routing Process**—After applying all ingress translation rules, the resulting called number (without associated technology prefixes) is matched against the list of zone prefixes for all zones that are accessible from the ingress gatekeeper or directory gatekeeper.

If a technology prefix is part of the called number, either as part of the original DNIS or added by the gateway (this can be set in the ingress route), it is matched against the list of hopoff zones that are accessible from the ingress gatekeeper or directory gatekeeper.

The routing between gatekeepers must be strictly prefix or technology prefix based even in the carrier-based domain. This is why the routing server usually selects the terminating zone and the gateway. Gatekeepers do not exchange the correct information to enable carrier-based routing.

When the egress gatekeeper is selected, all provided data is used to select the gateway that meets the given criteria (the prefix, technology prefix and target carrier). Gatekeepers select the terminating gateway based on the static prefix priority list (by default every gateway registered in the zone can accept the call), dynamically registered technology prefix, and dynamically registered list of trunk groups and carriers.

Every gateway that meets the specified criteria is included in the call path verification, but only the gateways with at least one egress route that matches target carrier and/or destination pattern successfully terminates the call and only those paths are listed as confirmed successful paths. The other paths are reported with the error message that indicates the call setup is initiated by the originating gateway, but it fails because of an improper configuration on the terminating gateway.

Note VRC does not validate non-dial plan parameters such as codec or DTMF-relay between the call endpoints.

Verifying Call Paths

Use call path verification to trace the full route of a call from gateway to gateway.

Note You can verify a call path from the Baseline View or the Design View.

Note You must find the terminating gateways before you verify a call path.

Note If you trace a call path from a voice port or trunk group, select a voice port or trunk group that has a translation profile defined so that the translation rules can be applied to the called number. If there are no translation rules defined and you are using carrier-based routing, trace the call path from the trunk group.

To verify a call path:

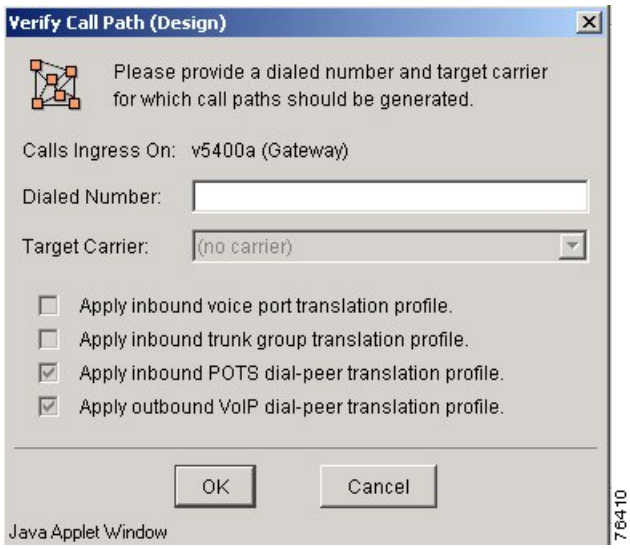
Step 1 Expand the dial plan tree to view all components.

Step 2 Locate the gateway to trace a call path from. You can also trace a call path from a voice port or trunk group on a gateway.

Step 3 Right-click the gateway (voice port or trunk group) and choose **Verify Call Path** from the menu.

The Verify Call Path dialog box appears (Figure 5-29).

Figure 5-29 Verify Call Path Dialog Box



Step 4 Enter the incoming dialed string that you want to find the call path for. Use only digits in your dial string, leaving out dashes and dots. You can enter only a prefix for your string.

Step 5 If the CSR route type for the AD is set to carrier or trunk-label, select a target carrier. If you leave the target carrier field blank, the call path is verified regardless of the routing server's status.

Step 6 Click **OK** to display the call paths from the incoming dial string or **Cancel**.

OSP Server

The Open Settlements Protocol (OSP) enables the call-routing infrastructure to choose the best place to terminate a phone call. During the Discovery operation, VRC checks to see if a gateway is configured for OSP.

Important Notes about OSP

- For managed zones, you can have one OSP server associated with a zone. This OSP server is the default for all gateways in the zone.
- For gateways, you can have one OSP server associated with a gateway. This OSP server overrides the default OSP server in the zone.
- For ingress routes with an ARA type of OSP Server, follow these rules:
  - If the route is assigned at the managed zone level, then use the OSP server associated with the zone.
  - If the route is assigned at the gateway, then use the OSP server associated with the zone.
- Ingress routes can terminate at OSP servers if the OSP Enabled attribute is configured on the gateway.
- OSP servers are not discovered by VRC.

Gateway Parameters

This section describes the parameters that can be configured for gateways in a VRC dial plan:

Assigning an Ethernet Port

When you execute the Discovery operation for a gateway, the Ethernet port associated with the IP address specified in the topology for a gateway is identified. The baseline dial plan shows this Ethernet port for each gateway.

Use the command line interface to add or delete an Ethernet port from the gateway.

View the Ethernet ports that are assigned to a gateway in the Design View or the Baseline View. Use this procedure to assign an Ethernet port on a gateway using the VRC client.

Note You must first create the Ethernet port using the command line interface (CLI).

To assign an Ethernet port on a gateway:

Step 1 From the Design View expand the dial plan tree to view all components.

Step 2 Locate the gateway to assign an Ethernet port to.

Step 3 Click the **Ethernet** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Ethernet Port dialog box appears.

Step 5 Enter the name of the Ethernet port to assign to the gateway.

Step 6 Click **Apply** to add the Ethernet port to the gateway or **Cancel**.

Editing a Trunk Group

A trunk group is a logical grouping of multiple DS1 interfaces with the same signaling characteristics that you can provision as an outbound dial peer target. You can perform the following functions:

- Configure multiple trunk groups per gateway.
- Edit the attributes of a trunk group using the VRC client, but you must use the command line interface to add or delete the trunk group from the gateway.
- View the trunk groups that are assigned to the gateway in the Design View or the Baseline View.

Note You can only use a VRC-discovered trunk group in your dial plan if the associated gateway has a VRC feature set of dp1.1 or later.

To edit the attributes for a trunk group on a gateway:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the gateway with the trunk group that you want to edit.

Step 3 Select the trunk group.

Step 4 Click the **Edit Attributes** button. The Edit Trunk Group dialog box appears.

Step 5 Enter the values that you want to change.

Table 7-22 describes the entry fields in the Edit Trunk Group dialog box.

Table 5-17 Trunk Group Attributes

General Attribute	Description
Name	The name of the trunk group. A read-only field.
Hunt Scheme	Specifies the way to select an interface from a trunk group for an outgoing call. Choose from least-idle, least-used, longest-idle, random, round-robin, sequential.
Hunt Order	Choose from both, even, or odd. Do not set this parameter if Hunt Scheme is set to random.
Hunt Direction	Choose from up or down. Set this parameter if Hunt Scheme is set to least-used, round-robin, or sequential.
Incoming Translation Profile	Associates a translation profile for the incoming side of the gateway. The VRC feature set of the translation profile must be dp1.1 or later.
Outgoing Translation Profile	Associates a translation profile for the outgoing side of the gateway. The feature set of the translation profile must be dp1.1 or later.
Description	The maximum value is 63 characters.
Carrier ID	The ID for the carrier that owns this trunk group. You can set this parameter only if the CSR route type is carrier.

Step 6 Click **Apply** to apply the values to the trunk group or **Cancel**.

Adding a Hunt Group

A hunt group is a series of dial peers, with the same destination pattern but different interfaces, organized to share the load. If the first interface is busy or unavailable, the next interface is “hunted” until an available interface is found, or the hunt process is stopped.

Note To use trunk groups in a hunt group, you must first create the trunk group using the CLI. (VRC creates hunt groups but cannot provision trunk groups.)

To add hunt groups to a gateway:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the gateway that you want to add a hunt group to.

Step 3 Click the **Hunt Groups** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Hunt Group dialog box appears.

Step 5 Enter the values in the entry fields.

- Name—The name for this hunt group. The maximum value is 64 characters.
- Choose either Trunk Group or Voice Port.
  - A trunk group is a group of similar trunks (shared electronic characteristics) that go between the same two geographical points. A trunk group performs the same function as a single trunk, but carries multiple conversations. You can only choose trunk group if the Cisco VRC feature set for the gateway is dp1.1 or later.
  - A voice port is a single voice port on a gateway.
- Description—Text description for this hunt group. The maximum value is 64 characters.

Step 6 Click **Apply** to add the hunt group or **Cancel**.

Adding a Voice Source Group

A voice source group allows you to assign a name to a set of source IP group characteristics. The terminating gateway uses these characteristics to identify and translate the incoming VoIP call.

Note You must set up a source group before you can add a voice source group. The voice source group receives parameter settings from the parent source group. You can only add a voice source group to a gateway if the VRC feature set of the gateway is dp1.1 or later.

To add a unique voice source group to a gateway:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the gateway to add a voice source group to.

Step 3 Click the **Voice Source Group** tab.

Step 4 Right-click and choose **Add** from the menu. The Add Voice Source Group dialog box appears.

Step 5 Enter attribute information.

Step 6 Table 7-23 describes the fields in the Add Voice Source Group dialog box.

Table 5-18 Voice Source Group Attributes

General Attributes	Description
Name	The name of the voice source group. The maximum value is 31 characters.
Source Group	The parent source group which contains the parameter settings to use for this voice source group.
Access List	The access list number for this voice source group to be used for call blocking. You must also set a disconnect cause for call blocking. This parameter allows the voice source group to block calls from the IP address specified in the access list.

Step 7 Click **Apply** to add the voice source group to the gateway or **Cancel**.

Editing a Voice Port

A voice port is an interface that connects the gateway to the PSTN network or the customer premise equipment (CPE). You can view the voice ports that are available on a gateway in the Design View or the Baseline View. You can edit voice port attributes using the VRC client; but you must first create the voice port using the command line interface (CLI).

To edit a voice port:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the gateway with the voice port that you want to edit.

Step 3 Select the voice port.

Step 4 Click the **Edit Attributes** button. The Attributes for Voice Port dialog box appears.

Step 5 Enter values that you want to change.

- Name—Read only field.
- Incoming Translation Profile—Associates a translation profile for the incoming side of gateway. You can only set this parameter if the gateway for this voice port has a VRC feature set of dp1.1 or later. The translation profile must already be defined and the feature set of the translation profile must also be dp1.1 or later.
- Outgoing Translation Profile—Associates a translation profile for the outgoing side of the gateway. You can only set this parameter if the gateway for this voice port has a feature set of dp1.1 or later. The translation profile must already be defined and the feature set of the translation profile must also be dp1.1 or later.

Step 6 Click **Apply** to add the translation profiles or **Cancel**.

Adding an Access List

An access list is kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

When you perform the Discovery operation on a gateway, all IP Standard (1-99) access lists for a gateway become part of the dial plan. VRC only discovers and displays access lists for gateways. VRC does not provision gateways.

The baseline and design dial plan show all access lists associated with a gateway on the gateway's Access Lists tab. The Access Lists tab is highlighted only if VRC discovers access lists provisioned on a gateway.

Use the CLI to add or delete an access list for a gateway.

Note You must first create the access list using the command line interface (CLI) before you can manually assign it to the gateway.

To add a predefined access list to a gateway:

Step 1 From the Design View, expand the dial plan tree to view all components.

Step 2 Locate the gateway that you want to assign an access list to.

Step 3 Click the **Access Lists** tab.

Step 4 Right-click and choose **Add** from the menu.

Step 5 Enter the access list number and an optional description.

Step 6 Click **Apply** to add the access list or **Cancel**.

CHAPTER 6

Opening the VRC Console

This chapter describes how to use the GUI console for the Cisco Voice Routing Center (VRC).

Certain server-based procedures are executed from the console instead of the VRC client. Because the console runs on the Sun server, you access it using the X protocol. We recommend that you use a Sun terminal, but you can also use a PC-based X package, such as Virtual Network Computing (VNC) server.

Note If you choose to use VNC viewer, you must install VNC server on the server where the VRC server resides.

Accessing the VRC Console

To open the Cisco VRC console from your X terminal:

Step 1 Open your Xclient application (or VNC server).

Your application might require you to enter a host name (IP address of the Xserver) and your password.

Step 2 If you must provide an IP address, then enter the IP address. Enter your password and click **OK**. A terminal work space session opens.

Step 3 From the workspace menu, right-click and choose **Terminal**, **Tools**, and then the **Terminal** option from the menus. A terminal session opens.

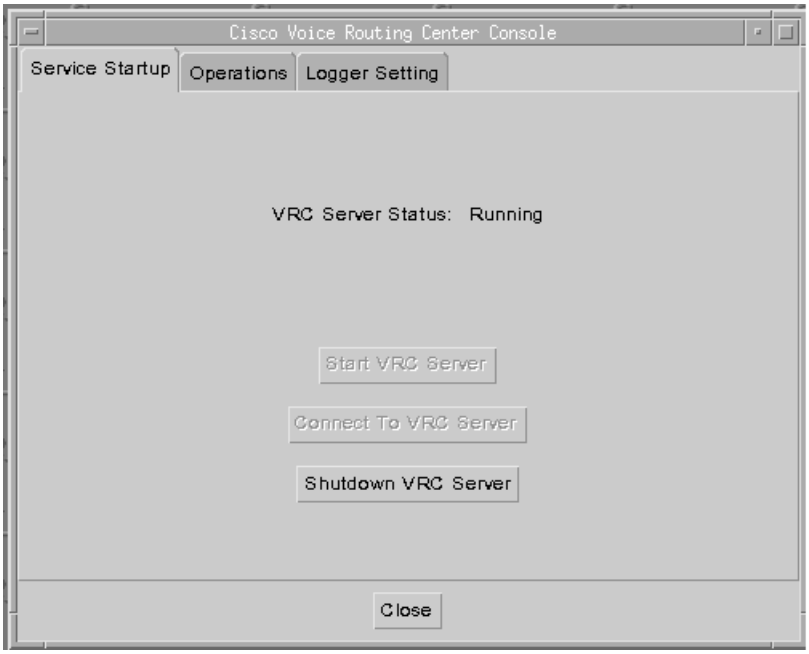
Step 4 Enter the following command:

```
start_console.sh
```

The VRC Console Login dialog box appears.

Step 5 Enter your name and password and press **OK**. The VRC Console window appears (Figure 6-1).

Figure 6-1 Voice Routing Center Console Window



The VRC Console window has the following tabs:

- **Service Startup** allows you to check the server status and contains the following action buttons:
  - Start VRC Server
  - Connect To VRC Server
  - Shutdown VRC Server
  - Close (the console session)
- **Operations** allows you to perform a batch import, set an emergency design session, back up the VRC system, restore the system, execute a rollback, and view the current logged-on list. The operations tab contains the following operation areas:
  - Topology
  - Dial Plan
  - System Admin
  - Security

Note **User Administration** appears under the Security area of operation; but it is managed through the CNS Security Services user interface.

- **Logger Setting** allows you to set up debugging for selected subsystems, activate, deactivate, or set all loggers to on or off.

Connecting to and Shutting Down the VRC Server

To establish a connection with the VRC server from the console:

Step 1 From the VRC console window, click the **Service Startup** tab.

Step 2 Click the **Connect to VRC Server** button.

Note If the VRC server status is running, you are already connected and you receive a message indicating that there is an existing session. Forced login can be caused by the same user login from the VRC client. Because only one active client session can be opened on the VRC server; if the user chooses a forced login, then another session from the VRC client will be closed.

Step 3 Enter your user name and password.

Step 4 Click **OK** to connect to the VRC server or click **Cancel** to cancel this procedure.

You can shut down the VRC server from the console or a UNIX shell.

Shutting Down the VRC Server from the Console

This procedure does not shut down any other processes that VRC might be using (for example, Tomcat or MySQL).

To shut down the VRC server from the console:

Step 1 From the VRC console window, click the **Service Startup** tab.

Step 2 Click the **Shutdown VRC Server** button. A Confirm dialog box appears.

Step 3 Click **OK** to confirm the shutdown or click **Cancel** to cancel the shutdown.

Shutting Down the VRC from the UNIX Shell

To shut down the VRC server software from the UNIX shell:

Step 1 Log in as the VRC system user.

Step 2 Run the script:

```
stop_gdpm.sh
stop_server.sh -u <username> -p <password>
```

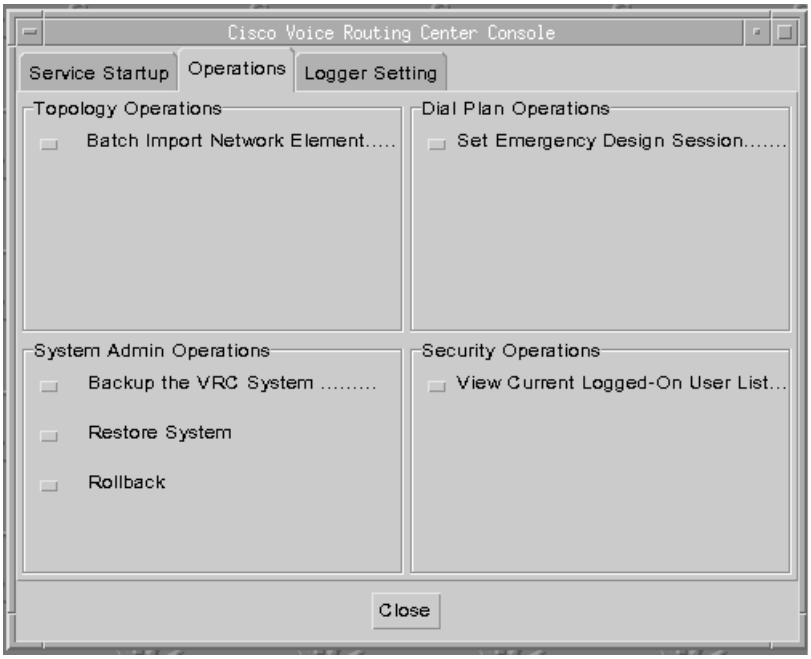
This script is located in $HOME/gdpm/scripts directory.

This stops the VRC server, Tomcat, and MySQL server processes. The MySQL process must be shut down after the VRC server process as the VRC server requires the MySQL database engine for its operation.

Using the Operation Functions

This section describes the operation functions from the Operations tab in the VRC Console window (Figure 6-2).

Figure 6-2 Operations Tab



Performing a Network Element Batch Import

The Topology Operations area in the Operations tab (Figure 6-1) displays the Batch Import Network Element button.

This section describes how to perform batch imports of network elements from the console. A network element must be added to the topology before it can be used in the dial plan.

Note You must check with your system administrator to see if you have user privileges.

To perform a batch import from the console:

Step 1 From the VRC Console window, click the **Operations** tab.

Step 2 Click the **Batch Import Network Element** button. The Choose Batch Import File dialog box appears (Figure 6-3). This dialog box lists available folders and files to import the network elements from. The path or folder name is the path to the VRC server.

Figure 6-3 Choose Batch Import File Dialog Box

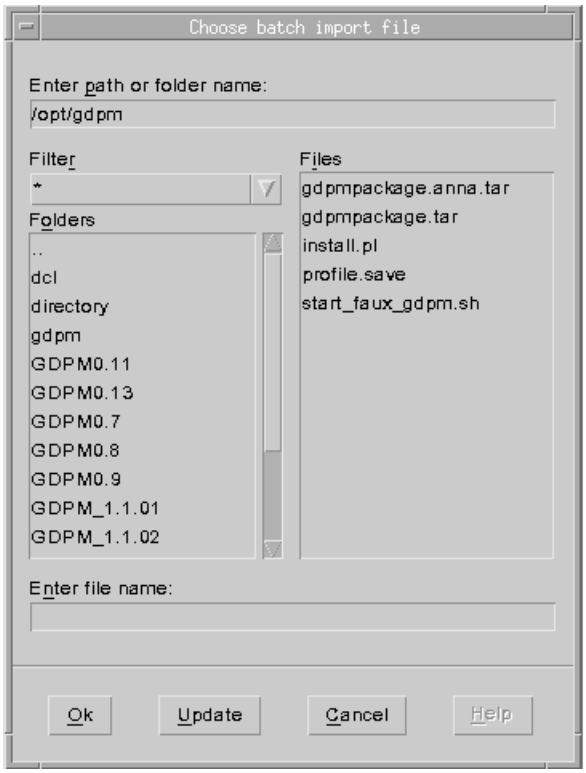


Figure 6-3 lists available folders and files to import the network elements from. Use this format to set up your network topology files.

Step 3 Enter the path or folder name which is the path to the VRC folder.

Step 4 Enter the folder and filename to import.

Step 5 Click **OK** to import the file.

Step 6 You are asked to confirm your selection. Click **OK**.

An Information dialog box appears and informs you if the import is successful. Click **OK** to confirm or click **Cancel** to cancel this operation.

Setting an Emergency Design Session

The Dial Plan Operations area in the Operations tab (Figure 6-2) displays the Set Emergency Design Session button.

VRC only allows one active design session per region. If a second user attempts to open a design session for the same region while the first user has a design session open, the access for the second user is denied.

If there is already an active design session and you need to make an urgent change to the dial plan, you can set an emergency design session through the VRC console from the Operations tab.

Note Any user who has the dp-admin privilege can perform an emergency design operation for a specific scope from the VRC console.

There are four possible reasons for using this option. A user has an active design session at the:

- Region level and the emergency occurs at the Administrative Domain (AD) level.
- Region level and the emergency occurs at the same region level.
- AD level and the emergency occurs at the AD level.
- AD level and the emergency occurs at the region level.

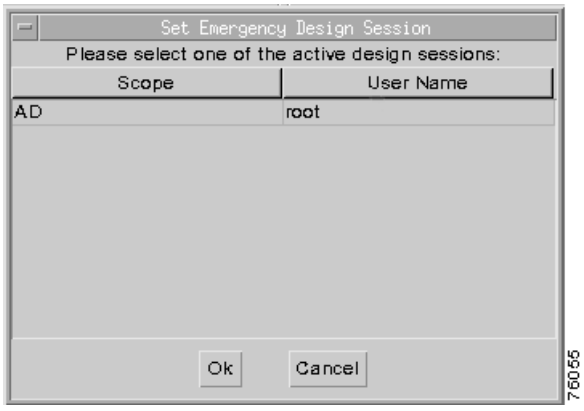
When the second user sets an emergency design session, the design session for the first user is closed. The user is notified that the session is closed and a design file is created. The design file name includes the time stamp, user name, scope, and file type. The first user is not logged out of the VRC server.

To set an emergency design session:

Step 1 From the VRC console window, click the **Operations** tab.

Step 2 Click the **Set Emergency Design Session** button under Dial Plan Operations area. The Set Emergency Design Session window appears with a list of active designs (Figure 6-4).

Figure 6-4 Set Emergency Design Session Window



Step 3 Select the scope you need to close. Choose a region or the AD.

Step 4 Click **OK**. A Confirm dialog box appears.

Step 5 Click **OK** to confirm your selection or click **Cancel** to cancel this procedure. An Information dialog box informs you if the operation is successful.

Step 6 Click **OK**.

System Administration Operations

The following sections describe the functions in the System Admin Operations area (see Figure 6-2) in the Operations tab:

- Backing Up the VRC System, page 6-7
- Restoring the VRC System, page 6-8
- Performing a Rollback, page 6-9

Backing Up the VRC System

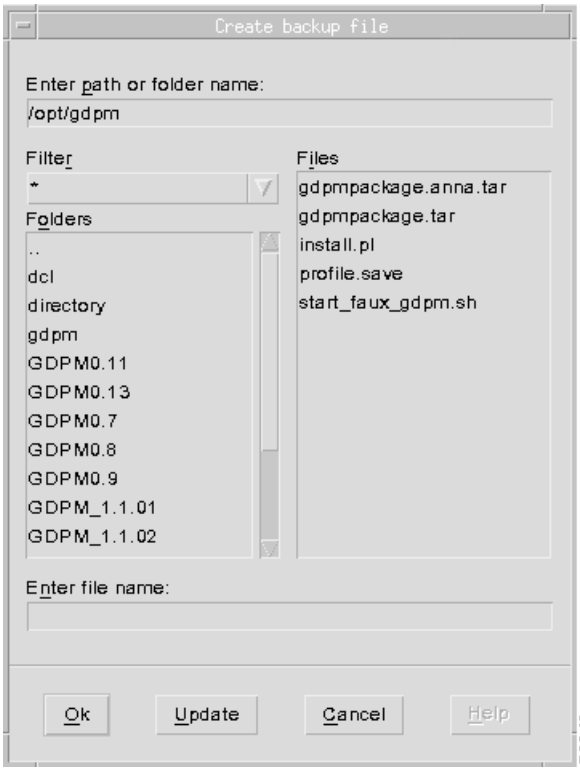
To back up the VRC database and directories from the console:

Step 1 From the VRC console window, click the **Operations** tab.

Step 2 Click the **Backup the VRC System** button from the System Admin Operations area.

The Create Backup File window appears (Figure 6-5).

Figure 6-5 Create Backup File Window



This window lists existing folders and files and the path or folder name which is the path to the VRC server.

Step 3 Enter the file name that you want to back up. You can select from existing files or enter a new file.

Step 4 Click **OK** to back up the file.

Step 5 Click **Update** to add this filename to the directory listing or click **Cancel** to cancel this procedure. A Confirmation dialog box appears.

Step 6 Click **OK** to confirm your selection.

An Information dialog box informs you if the import is successful. Click **OK**.

Restoring the VRC System

The Restore procedure overwrites the existing directory.

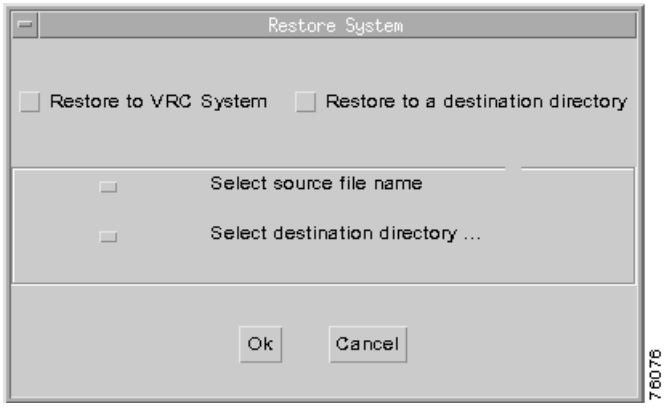
To restore the VRC system:

Step 1 From the VRC Console window, click the **Operations** tab.

Step 2 Click the **Restore System** button from the System Admin Operations area.

The Restore System window appears (Figure 6-6).

Figure 6-6 Restore System Window



The Restore System window displays two restore buttons:

- Restore to VRC System
- Restore to a Destination Directory

Choose where you want to restore the system to.

Step 3 If you choose Restore to VRC System, this restores the VRC system to a previously backed-up configuration.

a. Click the **Select source file name** button to open a window.

b. Enter a folder and file name.

c. Click **OK** in the Choose restore source directory browser window.

Step 4 If you choose Restore to a destination directory, the server automatically restarts. This operation can be used to review the data you want to restore but does not make any changes to the system.

a. Click the **Select source file name** button to open a browser window.

b. Enter a folder and file name.

c. Click **OK** in the Choose restore source directory browser window.

d. Click the **Select destination directory** button to open a browser window.

e. Enter a folder and file name.

f. Click **OK** in the Choose restore destination directory window.

Step 5 Click **OK** in the Restore System window. You are asked to confirm your selection.

Step 6 Click **OK** to restore the system or click **Cancel** to cancel the procedure.

The following are restored to the destination directory:

- dp.tar, which is automatically untarred and creates the directories: config-<load #> and data
- db.out file, which contains all of the database information
- data directory, which contains all the files from the /opt/vnm/data/dialplan and /opt/vnm/data/batch directories
- config-<load #> directory, which contains all the files from the /opt/vnm/gdpm/config directory

An Information dialog box informs you if the operation is successful. Click **OK**.

Performing a Rollback

A rollback is a VRC function that:

- Clears all information from the VRC database except user information.
- Returns elements to the state they were in after the first Discovery operation.

Note If you execute a Discovery for a region or AD and cancel before the operation is complete, the configurations that were discovered before the cancellation are still stored in the /origconfig directory. Furthermore, a second discovery does not overwrite these files. If you execute a rollback, the configuration stored in the /origconfig directory is used.

Caution You cannot execute a rollback if you have made changes to the topology since the first Discovery operation (for example, changing an IP address or removing an element), or if you have changed the original Discovery information.

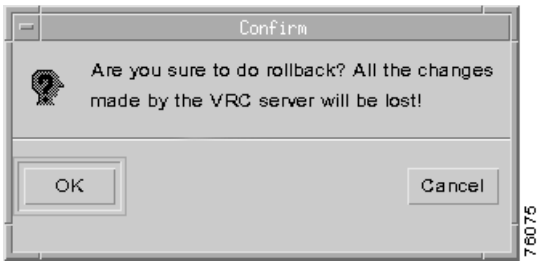
To return a dial plan to its original configuration:

Step 1 From the VRC console window, click the **Operations** tab.

Step 2 Click the **Rollback** button from the System Admin Operations area.

A Confirm dialog box appears (Figure 6-7).

Figure 6-7 Confirm Rollback Dialog Box



Step 3 Click **OK** to roll back to the original configuration discovered for each element or click **Cancel** to cancel this operation.

Viewing Currently Logged-On Users

The Security Operations area in the Operations tab (Figure 6-1) displays the View Current Logged-On User List button. The Security Operations allows you to only view users currently logged on to the VRC.

To review current users:

Step 1 From the VRC Console window, click the **Operations** tab.

Step 2 Click the **View Current Logged-On Users List** button from the Security Operations area. A Current Logon Users window appears with a list of account names.

Step 3 When you finish reviewing this list, click **OK**.

Security Administration appears under the Security area of operation but it is managed through the CNS Security Services user interface.

Setting the Debug Operation

This section describes how to set up debugging for selected subsystems. You can turn debugging on or off for one or all subsystems.

Logger levels are the different filters for logging error messages, for example, debug. It refers to the tags on the error messages.

Note When you enable debugging from the console, it is only persistent until theVRC software is restarted, at which time the default setting of disabled is reinstated.

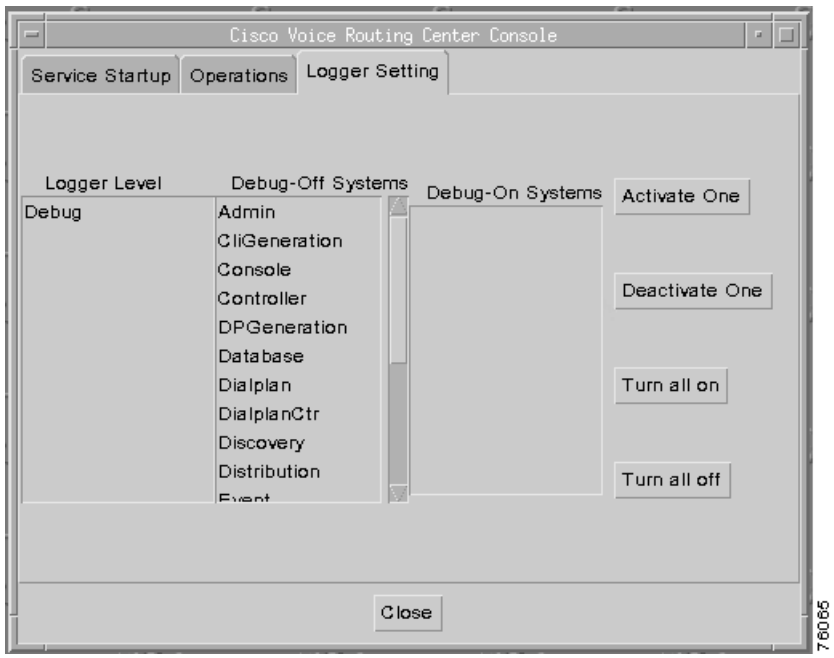
The following log files are located in the /opt/vnm/gdpm/data/log directory and can contain debugging information:

- GdpmInternal.log
- GdpmAudit.log
- GdpmSystem.log

To set up debugging:

Step 1 From the VRC Console window, click the **Logger Setting** tab. The Logger Setting window appears (Figure 6-8).

Figure 6-8 Logger Setting Tab



Step 2 Select the subsystem that you want to change the setting for.

From the Logger Setting window, you can:

- Turn debugging *on for one subsystem*, go to Step 3
- Turn debugging *on for all subsystems*, go to Step 4
- Turn debugging *off for one subsystem*, go to Step 5
- Turn debugging *off for all subsystems*, go to Step 6

Step 3 To turn debugging on for one subsystem, follow these steps:

a. Select **Debug** from the Logger Level list and the subsystem (Validation, for example) from the Debug-Off Systems list.

b. Click the **Activate One** button. The selected subsystem is moved to the Debug-On Systems list.

Step 4 To turn debugging on for all subsystems, follow these steps:

a. Click the **Turn all on** button.

b. A Confirm window appears asking if you want to turn the debug on for all subsystems.

c. Click **OK** to move all subsystems to the Debug-On Systems list or click **Cancel** to cancel the procedure.

Step 5 To turn debugging off for one subsystem, follow these steps:

a. Select Debug from the Logger Level list and the subsystem (Validation, for example) from the Debug-Off Systems list.

b. Click the **Deactivate One** button. The subsystem is moved to the Debug-Off Systems List.

Step 6 To turn debugging off for all subsystems, follow these steps:

a. Click the **Turn all off** button.

b. A Confirm window appears asking if you want to turn the debug off for all subsystems.

c. Click **OK** to move all subsystems to the Debug-Off Systems list or click **Cancel** to cancel the procedure.

Step 7 Click the **Close** button to close the Logger Setting window.

Closing the Console

To close the console window:

Step 1 See Connecting to and Shutting Down the VRC Server, page 6-3 to access the Service Startup window.

Step 2 Click the **Close** button at the bottom of the window.

The console window closes.

Step 3 Exit your Xclient application. Type `exit` to close the console terminal window.

Frequently Used VRC Operations

This appendix gives a step-by-step approach to accomplishing some frequently used VRC operations. Most of the tasks are performed within a VRC design session. Multiple tasks can be performed within the same design session. Changes made within a design session do not take effect until the design is committed.

Designing a New Dial Plan

To design a new dial plan in VRC, perform these tasks in the following order:

1. Prepare the dial plan infrastructure.
2. Create routes.
3. Validate the design and fix any discrepancies found.
4. Preview the design.
5. Commit the design.
6. Distribute the baseline dial plan design.

Preparing the Dial Plan Infrastructure

Use this procedure to prepare the dial plan infrastructure in VRC.

Note Your elements must already be in the topology, gateways must have voice ports assigned, and you are in the Design View.

To prepare the dial plan infrastructure, perform these tasks in the following order:

1. For the Administrative Domain (AD):
   a. Choose the routing type.
   b. Add technology prefixes.
   c. Add trunk or carrier IDs, as needed.

2. Create regions. For each region that you create, you must:
   a. Create a directory gatekeeper group (DGKGrp) if you want the region to be hierarchical.
   b. Assign directory gatekeepers (DGKs) to the directory gatekeeper group.
   c. Create gatekeeper groups (GKGrps).
   d. Assign gatekeepers to the gatekeeper groups.
   e. Create zones.
   f. Assign gateways to the zones.

Creating Routes

Use this procedure to create routes for each zone in your dial plan.

Note The dial plan infrastructure must already be defined and the dial plan is open in the Design View. If you have not defined the dial plan infrastructure, see Preparing the Dial Plan Infrastructure, page A-1.

To create routes, perform these tasks in the following order:

1. Locate the zone in the dial plan.
2. Assign zone prefixes to the zone.
3. Assign hopoff technology prefixes (optional).
4. Assign a gatekeeper group to the zone.
5. Create translation profiles and rules (optional).
6. Create a route scope for the zone.
7. Create egress routes and ingress routes.

Adding a Gateway to an Existing Network

Use this procedure to add a new gateway to your dial plan and enhance network capacity. You can configure a new gateway to operate like other gateways in your dial plan.

Note The baseline dial plan must be defined, the gateway is in the topology, and you are in the Design View.

To add a new gateway to an existing network, perform these tasks in the following order:

1. Add a gateway to the dial plan in the desired zone.
2. Verify that existing routes apply to that gateway. For example, any routes with a route scope of the whole managed zone.
3. Add any new routes, if needed.
4. Commit your changes. The baseline dial plan is updated.

Adding a Redundant Gatekeeper

Use this procedure to add a new gatekeeper to an existing dial plan for redundancy purposes. You can configure a second gatekeeper as an alternate or configure a cluster (high-capacity gatekeeper feature) with multiple gatekeepers.

Note Before you add a redundant gatekeeper, be sure that the baseline dial plan has been defined, the gatekeeper is in the topology, and you are in the Design View.

To add a redundant gatekeeper, perform these tasks in the following order:

1. Select the gatekeeper group that needs a redundant device.
2. Specify the redundancy mechanism (cluster, overlap, HSRP, or both).
3. Commit your changes to the baseline dial plan.

Note Configure an overlap redundant gatekeeper configuration at the gateway. Configure a clustered redundant gatekeeper configuration at the gatekeeper.

Adjusting the Dial Plan for an NPA Overlap

Use this procedure to make adjustments to your dial plan if a Numbering Plan Area (NPA) overlap occurs.

Prerequisites

The baseline dial plan must be defined, you are adding no additional gateways, and you are in the Design View.

To adjust the dial plan for an NPA overlap, perform these tasks in the following order:

1. Locate the affected zone.
2. Set up the following parameters for the affected zone:
   a. Add new (overlap) zone prefix to the zone.
   b. Create egress routes for the new prefix (create new route scopes if necessary).
   c. Create new ingress routes if necessary.
3. Commit your changes to the baseline dial plan.

Adjusting the Dial Plan for an NPA Split

Use this procedure to make adjustments to your dial plan if a Numbering Plan Area (NPA) split occurs.

Prerequisites

The baseline dial plan must be defined and you are in the Design View.

To adjust the dial plan for an NPA split, perform these tasks in the following order:

1. Locate the affected zone.
2. Create a new zone in the same region.
3. Add gateways to the new zone by one of the following methods:
   a. Move a subset of gateways from the old zone to the new zone.
   b. Use new gateways if they are available.
4. Set up the following parameters for the new zone:
   a. Assign a zone prefix.
   b. Assign gatekeeper group (should be same as the original).
   c. Create a route scope and ingress and egress routes.
5. Commit your changes to the baseline dial plan.

Setting Up Hairpinning

Use this procedure to set up hairpinning on a gateway. Hairpinning is a call routing capability that sends a call back to the PSTN portion of the network if the call cannot be serviced by the Voice-over-IP (VoIP) portion of the network.

Prerequisites

The baseline dial plan is defined and you are in the Design View.

To set up hairpinning, perform these tasks in the following order:

1. Create a route scope for the hairpin route.
2. Set up an ingress route.
   a. Set the dial peer type to both.
   a. Enter a destination pattern (dial string containing up to 32 digits and ending with the letter T).
   b. Set the priority to 1.
   c. Set the address resolution authority (ARA) type to GKGrp, OSPServer, or ipv4.
   d. Assign the route scope that was created in Step 1.
3. Set up an egress route.
   a. Use the same destination pattern as ingress route created in Step 2.
   b. Set the dial peer type to POTS.
   c. Set the priority to a low number, such as 10.
   d. Assign the route scope created in Step 1.

Configuring an Egress Route for Prefix Routing

Use this procedure to configure an egress route for prefix routing. If your CSR route type is set for trunk-label or carrier, see Configuring an Egress Route for CSR, page A-5.

Prerequisites

The managed zone for this route must already exist and you have already defined the route scope for this route.

To configure an egress route for prefix routing, perform these tasks in the following order:

1. Add an egress route to the zone.
2. Specify a VRC feature set (must be dp1.0 for prefix routing).
3. Set a destination pattern for the route.
4. Define an ANI (answer address) and a DNIS (incoming called-number) for the route. An inbound VoIP dial peer is only created if one of these two values is set.
5. Specify a translation profile (optional).
6. Specify a route scope. Choose from the route scope or the managed zone. If you choose route scope, the feature sets must match.
7. Specify a call block (optional).
8. Select a technology prefix (optional).
9. Specify a voice class codec (optional).
10. Set the hunt-stop behavior (optional).
11. Define the necessary route parameters for the route (optional).

Configuring an Egress Route for CSR

Use this procedure to configure an egress route to support carrier sensitive routing (CSR). If the CSR route type for the AD is set to None, see Configuring an Ingress Route for Prefix Routing, page A-6.

Prerequisites

The following conditions must exist before you can configure an egress route to support CSR.

- The managed zone has a route scope with a feature set of dp1.1 or later.
- The gateways in the route scope have the required trunk group defined.
- The required carrier-id must be defined at the AD level.
- The AD's CSR route type must be set to carrier or trunk-label.

To configure an egress route for CSR, perform these tasks in the following order:

1. Specify a feature set of dp1.1 or later.
2. Associate a source carrier ID from the available list. Use this to define an inbound VoIP dial peer.
3. Associate a target carrier ID from the available list. Use this to define an outbound POTS dial peer.
4. Associate an incoming-side translation profile from the enclosing zone.
5. Associate an outgoing-side translation profile from the enclosing zone.
6. Define a destination pattern for the route (optional).
7. Associate a route scope that supports trunk groups or hunt groups to the route. The hunt group type must be trunk group.
8. Set other egress route attributes and parameters.

Configuring an Ingress Route for Prefix Routing

Use this procedure to configure an ingress route for prefix routing. If your CSR route type is set for trunk-label or CSR, see Configuring an Ingress Trunk Route for CSR, page A-6.

Prerequisites

The managed zone for this route must already exists and you have already defined the route scope for this route.

To configure an ingress route for prefix routing, perform these tasks in the following order:

1. Add an ingress route to the zone.
2. Specify a VRC feature set (must be dp1.0 for prefix routing).
3. Set a destination pattern for the route.
4. Define an ANI (answer address) and a DNIS (incoming called-number) for the route (optional).
5. Specify a translation profile (optional).
6. Specify a route scope. Choose from the route scope or the managed zone. If you choose route scope, the feature sets must match.
7. Specify a call block.
8. Select a technology prefix (optional).
9. Specify a voice class codec (optional).
10. Set the hunt-stop behavior (optional).
11. Define the necessary route parameters for the route (optional).
12. Set the address resolution authority (ARA) type for the route. Choose from GKGrp, OSP Server, Hairpin, or ipv4.

Configuring an Ingress Trunk Route for CSR

Use this procedure to configure an ingress route to support carrier sensitive routing (CSR). If your CSR routing type is set to None, see Configuring an Ingress Route for Prefix Routing, page A-6.

Prerequisites

The following conditions must exist before you can configure an ingress route to support CSR:

- The managed zone has a route scope with a feature set of dp1.1 or later.
- The gateways in the route scope have the required trunk group defined.
- The required carrier-id must be defined at the AD level.
- The AD's CSR route type must be set to carrier or trunk-label.

To configure an ingress route to support CSR, perform these tasks in the following order:

1. Specify a feature set of dp1.1 or later.
2. Associate a source carrier ID from the available list. This is used to define an inbound plain old telephone service (POTS) dial peer.
3. Associate an incoming-side call block translation profile from the enclosing zone. This is used to define the call block in an inbound POTS dial peer.

4. Associate an outgoing-side translation profile from the enclosing zone.
5. Define a destination pattern for the route.
6. Define a call block disconnect cause. If there is a call blocking profile, then there can also be a disconnect cause.
7. Associate a route scope that supports trunk groups or hunt groups to the route. The hunt group type must be set to trunk group.
8. Set other ingress route attributes and parameters.

Setting Up Dial Peer Call Blocking

You can set up incoming call blocking based on the call number after the two-stage dialing or overlap dialing finishes. Use a reject rule in the translation rule and apply these rules for calling number, called number, or redirect called number of an incoming call. You can set up call blocking for both ingress and egress routes.

Prerequisites

- Call blocking parameters must be configured on outbound dial peers.
- The route that you want to set up call blocking for must have a feature set of dp1.1 or later.
- You must already have feature set dp1.1 or later set up with reject rules configured in the translation rules.

To configure a voice source group for call blocking based on an IP access list, see Adding a Voice Source Group, page 5-83.

To set up call blocking attributes for a route, perform these tasks in the following order:

1. Modify an existing egress or ingress route or create a new route.
2. Set up a call blocking profile for the route.
3. Assign the translation profile with reject rules to the route.
4. Add the disconnect cause to the call blocking profile.

Troubleshooting Cisco VRC

This appendix provides information to help you when using the Cisco Voice Routing Center (VRC).

General FAQs

Table B-1 lists general VRC questions.

Table B-1 General Frequently Asked Questions

Question	Answer
What VRC documentation is available?	Cisco Voice Routing Center Software Version 1.2.1 reference documentation is located at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vrc/vrc1_2_1/index.htm • Online Help • Release Notes • User Guide • System Administration Help Files
What PTC documentation is available?	PTC 3.0 reference documentation is located at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ptc/3_0/index.htm
How do I import a file?	You can import a file from the console or the VRC client. • From the console, click the **Operations** tab and choose **Batch Import Network Element**. • From the client, choose **Import Topology** from the Topology menu. When you import files from the client, the batch import file must be located in the /tftpboot/gdpm/batch/ directory.

Table B-1 General Frequently Asked Questions (continued)

Question	Answer
Why do I receive the following error on my browser when I try to launch the VRC client? No Java 2 SDK, Standard Edition v x.x.x support for APPLET!!	You are probably using an unsupported browser. VRC supports Internet Explorer 5.0 or 5.5 and Netscaper 7.
How do I execute a Discovery?	From the Baseline View, right click the Administrative Domain (AD) or region and choose **Discover** from the menu. We recommend that your initial Discovery be done at the AD level.
What is the difference between Normal and Forced Discovery?	**Normal Discovery** stops if an element is unreachable or if a network element is defined incorrectly in the topology (for example, a gateway is really a gatekeeper). See Discovering a Dial Plan, page 3-3 for more details on why normal Discovery causes the Discovery operation to stop. **Forced Discovery** logs these errors and moves on to Discover the next network element.
When I open a saved design file, is it true that I may be out of sync with the Baseline?	Yes. Another user might have changed the baseline dial plan since you last started and saved your dial plan design.

Cisco VRC Error Messages

VRC error messages are presented in the following format:

539=Warning - Element not found in the cache

Where **539** is the internal error message number, **Warning** is the severity of error message, followed by a **brief description**. Error messages are reported numerically by the particular VRC operation or component they relate to.

There are four severityfcevels of error messages in VRC:

- **Error**—The VRC operation cannot continue until this error is fixed. For example, this means that the state of the component is not valid, and the Design View cannot be committed until the problem is corrected.
- **Warning**—A problem was detected during the VRC operation. We recommend that you make the necessary changes to correct the problem. However, the operation can continue if you choose not to fix it.
- **Audit**—VRC records user actions in audit files. The following are examples of user actions that VRC audits:
  - Changes to the topology (adding or removing elements)
  - Changes to the dial plan (design changes)
  - Changes to user administration (adding new user, changing privileges)

  - Logging in
  - Logging out
- **Information**—An action has been completed.

Note If you are required to stop the VRC server and restart it to recover from an error, report the circumstances to Cisco Technical Support.

Note To help you troubleshoot a specific VRC component or subsystem, use the debugging tool on the console.

Table B-2 lists the error message numbers in relation to the VRC component.

Table B-2 Error Message Types

VRC Component	Error Message Number Block
General	100-199
Database	200-299
Topology	300-399
Security	400-499
Dial Plan	500-599
GUI Infrastructure	600-699
Network Element Distribution	700-799
Network Element Discovery	800-899
File Manager	900-999
Request Handler	1000-1099
Network Element Access and Discovery	1100-1199
Design Manager	1200-1299
VRC Server	1300-1399
Administrative Service	1400-1499
Model Persistor	1500-1599
Common Modules	1600-1699
CLI Generator	1700-1799
Dial Plan Generator	1800-1899
Console Backup Restore	1900-1999
Report Service	2000-2999

This section provides general descriptions about error messages for specific VRC components. See the online help for a complete list of VRC error messages for each VRC component.

Database Error Messages

Database error messages are generated when there is an error during database operations. For example, most database errors are internal errors.

There are two kinds of database-related errors:

- Errors related to the MySQL database

  This is typically an internal error while inserting or updating a specific table in the MySQL database. Check the server environment and make sure that the MySQL server is running.

- Errors related to the VRC database operations, such as:
  - Executing a rollback
  - Removing an element from the dial plan
  - Backing up the system

When you encounter database error messages, use the console to set the debug of the Database subsystem to On.

Note Some database errors require you to stop the VRC server and then restart it. Continued use of this corrective action should be reported to Cisco Technical Support.

If you encounter errors with the database schema, you must reinstall the VRC software and reconfigure the database.

Topology Error Messages

Topology-related error messages occur most frequently during the following operations:

- Creating regions

  A region is created in the CNS security service when one is created in the dial plan. If the security service is unable to create the region, you receive errors.

- Persisting element configurations

  VRC must be able to access the dial plan configuration.

When you encounter Topology error messages, use the console to set the debug of the Topology subsystem to On.

Security Error Messages

Security error messages are generated from the security service of the VRC server.

These messages provide details about security-related operations, such as:

- Login
- CNS data access errors due to topology change
- General information about the CNS security system

When you encounter Security error messages, use the console to set the debug of the security subsystem to on.

Note The CNS security services GUI relies on the correct installation of Tomcat, which is part of the VRC installation procedure (or part of the PTC installation procedure if you are using VRC integrated with PTC). See the *Cisco VRC Installation Guide* for more information.

Discovery Error Messages

The following is a list of Discovery errors most frequently encountered:

- The element is unreachable.
- The running configuration for the element does not match the element defined in topology. Two examples of this are:
  - The running configuration is for a gateway but the topology lists this element as a gatekeeper.
  - There is an IP address mismatch where the running configuration does not contain the voice-enabled IP address that the element should have.
- For gateways only—The element is inactive in the dial plan and has no voice ports defined.

When you encounter Discovery error messages, use the console to set the debug of the Discovery subsystem to on.

Design Manager Error Messages

The VRC design manager presides over operations that take place while the user is in a design session. There can be 50 design sessions open at one time.

Most design manager error messages can be avoided if you check for the following issues:

- Make sure that you are in the correct VRC View for the specific operation you are trying to execute. Most operations that involve the design manager take place in the Design View.
- Your scope is the piece of the network over which you have administrative privileges. Only one user can administer a particular scope at a given time.
- Some operations can occur concurrently, but others can only be handled by the VRC server one at a time. If an operation cannot be executed because it cannot be initialized, wait a few moments and try again. VRC might be waiting for an operation to complete, or an operation must be in the initialized state before you can execute it.

When you encounter design manager error messages, use the console to set the debug of the subsystems for the dial plan generation (DPGeneration) and dial plan controller (DialplanCtr) to on.

Troubleshooting the Cisco VRC

This section describes troubleshooting information for the following:

- VRC Client, page B-6
- VRC Server, page B-6
- VRC MySQL, page B-7

VRC Client

This section lists additional troubleshooting information for VRC client operation.

- If the disk space for the client reaches 80 MB, you are prompted to refresh the memory. You must close all instances of Internet Explorer to refresh the memory.
- Operations that access the network elements might take a long time to complete. Note that the operation progress bar is nonlinear.

VRC Server

This section lists additional troubleshooting information for VRC server operation.

The key processes that need to be running for VRC operation are:

- VRCServer
- mysql
- tomcat (grep on security)
- rvrd

The VRC logging structure captures:

- User activity
- Problems with the dial plan
- System activity
- System errors

Debugging information:

- Debug logs are located in the /opt/vnm/gdpm/data/log directory.
- Can be set from the console for individual VRC subsystems.
- Can be set from the gdpm.properties file. This method survives restarts and can be overridden from the console.

Table B-3 shows where the logging information is captured.

Table B-3 Log File Names that Capture Logging Information

Log File	User Activity	Dial Plan Problems	System Activity	System Errors	Debug Trace
Internal (server)	X	X	X	X	X
System (server)	X	X	X		
Audit (server)	X				
User (client)	per user	per user	per user		

Note The maximum size of the log file is fixed in the system properties file. As a result, the log file only grows up to the maximum file size. When the maximum size is reached, the log file is backed (into .old file) and a new file with the same name (for example, GdpmInternal.log) is created for logging.

VRC MySQL

This section lists additional troubleshooting information for the MySQL operations in VRC.

- VRC cannot operate without the MySQL database.
- The VRC database is called gdpm.
- Scripts can be used to drop and create the database in VRC scripts directory /opt/cisco/vnm/gdpm/scripts.
  - Use caution when you use these scripts.
  - You must be logged into MySQL to use these scripts.
  - Can be restarted manually, if necessary.

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

Z