



## **Dial Peer Configuration on Voice Gateway Routers**

Release 12.4

### **Americas 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: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Dial Peer Configuration on Voice Gateway Routers*

© 2009 Cisco Systems, Inc. All rights reserved.



# About Cisco IOS and Cisco IOS XE Software Documentation

---

**Last Updated: March 5, 2009**

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

## Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

## Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

# Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

## Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

## Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y   z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

## Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
<b>Courier font</b>	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

## Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:



**Caution**

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



**Note**

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



**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

## Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

## Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

## Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Cisco IOS XE, and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

### Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

### Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

### Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

### Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

## Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

**Table 1** *Cisco IOS and Cisco IOS XE Configuration Guides and Command References*

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS AppleTalk Configuration Guide</i>	AppleTalk protocol.
<i>Cisco IOS XE AppleTalk Configuration Guide</i>	
<i>Cisco IOS AppleTalk Command Reference</i>	
<i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
<i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<p><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></p> <p><i>Cisco IOS Bridging Command Reference</i></p> <p><i>Cisco IOS IBM Networking Command Reference</i></p>	<ul style="list-style-type: none"> <li>• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</li> <li>• Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.</li> </ul>
<p><i>Cisco IOS Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS XE Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS Broadband and DSL Command Reference</i></p>	<p>Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p>
<p><i>Cisco IOS Carrier Ethernet Configuration Guide</i></p> <p><i>Cisco IOS Carrier Ethernet Command Reference</i></p>	<p>Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).</p>
<p><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS Configuration Fundamentals Command Reference</i></p>	<p>Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.</p>
<p><i>Cisco IOS DECnet Configuration Guide</i></p> <p><i>Cisco IOS XE DECnet Configuration Guide</i></p> <p><i>Cisco IOS DECnet Command Reference</i></p>	<p>DECnet protocol.</p>
<p><i>Cisco IOS Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS XE Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS Dial Technologies Command Reference</i></p>	<p>Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).</p>
<p><i>Cisco IOS Flexible NetFlow Configuration Guide</i></p> <p><i>Cisco IOS Flexible NetFlow Command Reference</i></p>	<p>Flexible NetFlow.</p>

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS H.323 Configuration Guide</i>	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
<i>Cisco IOS Intelligent Services Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Services Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

**Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL:  <a href="http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html">http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html</a>
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO connectionless network service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<p><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></p>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<p><i>Cisco IOS Multi-Topology Routing Configuration Guide</i></p> <p><i>Cisco IOS Multi-Topology Routing Command Reference</i></p>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<p><i>Cisco IOS NetFlow Configuration Guide</i></p> <p><i>Cisco IOS XE NetFlow Configuration Guide</i></p> <p><i>Cisco IOS NetFlow Command Reference</i></p>	Network traffic data analysis, aggregation caches, export features.
<p><i>Cisco IOS Network Management Configuration Guide</i></p> <p><i>Cisco IOS XE Network Management Configuration Guide</i></p> <p><i>Cisco IOS Network Management Command Reference</i></p>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
<p><i>Cisco IOS Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS XE Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS Novell IPX Command Reference</i></p>	Novell Internetwork Packet Exchange (IPX) protocol.
<p><i>Cisco IOS Optimized Edge Routing Configuration Guide</i></p> <p><i>Cisco IOS Optimized Edge Routing Command Reference</i></p>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<p><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS Quality of Service Solutions Command Reference</i></p>	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
<p><i>Cisco IOS Security Configuration Guide</i></p> <p><i>Cisco IOS XE Security Configuration Guide</i></p> <p><i>Cisco IOS Security Command Reference</i></p>	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

**Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
<i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
<i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<i>Cisco IOS Virtual Switch Command Reference</i>	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).  <b>Note</b> For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
<i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
<i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i>	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
<i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

**Table 2** Cisco IOS Supplementary Documents and Resources

Document Title	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of <b>debug</b> commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>

## Additional Resources and Documentation Feedback

*What's New in Cisco Product Documentation* is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

---

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



# Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

---

**Last Updated: March 5, 2009**

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS and Cisco IOS XE Software Documentation](#)” document.

## Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

### Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

---

The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

---

## Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

## Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

**Table 1** CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the <b>logout</b> or <b>exit</b> command.	<ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display device status.</li> </ul>
Privileged EXEC	From user EXEC mode, issue the <b>enable</b> command.	Router#	Issue the <b>disable</b> command or the <b>exit</b> command to return to user EXEC mode.	<ul style="list-style-type: none"> <li>• Issue <b>show</b> and <b>debug</b> commands.</li> <li>• Copy images to the device.</li> <li>• Reload the device.</li> <li>• Manage device configuration files.</li> <li>• Manage device file systems.</li> </ul>
Global configuration	From privileged EXEC mode, issue the <b>configure terminal</b> command.	Router(config)#	Issue the <b>exit</b> command or the <b>end</b> command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the <b>interface</b> command.	Router(config-if)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the <b>line vty</b> or <b>line console</b> command.	Router(config-line)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the <b>reload</b> command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	rommon # >  The # symbol represents the line number and increments at each prompt.	Issue the <b>continue</b> command.	<ul style="list-style-type: none"> <li>Run as the default operating mode when a valid image cannot be loaded.</li> <li>Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.</li> <li>Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.</li> </ul>
Diagnostic (available only on the Cisco ASR1000 series router)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> <li>A user-configured access policy was configured using the <b>transport-map</b> command, which directed the user into diagnostic mode.</li> <li>The router was accessed using an RP auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.</li> </ul>	Router(diag)#	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> <li>Inspect various states on the router, including the Cisco IOS state.</li> <li>Replace or roll back the configuration.</li> <li>Provide methods of restarting the Cisco IOS software or other processes.</li> <li>Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components.</li> <li>Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.</li> </ul>

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



**Note**

A keyboard alternative to the **end** command is Ctrl-Z.

## Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes how to use the Help feature.

**Table 2** CLI Interactive Help Commands

Command	Purpose
<b>help</b>	Provides a brief description of the help feature in any command mode.
<b>?</b>	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

### help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

### ?

```
Router# ?
```

```
Exec commands:
```

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

### partial command?

```
Router(config)# zo?
```

```
zone zone-pair
```

### partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

### command?

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

### command keyword?

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

## Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

**Table 3** CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```

Router(config)# ethernet cfm domain ?
    WORD domain name
Router(config)# ethernet cfm domain dname ?
    level
Router(config)# ethernet cfm domain dname level ?
    <0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
    <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol protocol options
    <cr>
Router(config)# logging host ?
    Hostname or A.B.C.D IP address of the syslog server
    ipv6 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol protocol options
    <cr>

```

## Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.



### Note

Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see [http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_tech\\_note09186a00801746e6.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml).

## Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.



**Note** The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

## Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

## Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

**Table 4** Default Command Aliases

Command Alias	Original Command
<b>h</b>	help
<b>lo</b>	logout
<b>p</b>	ping
<b>s</b>	show
<b>u</b> or <b>un</b>	undebug
<b>w</b>	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

[http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf\\_book.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html).

## Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

## Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at

[http://www.cisco.com/en/US/docs/ios/debug/command/reference/db\\_book.html](http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html).



### Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

## Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (`|`), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

## Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

**Table 5** Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- [Cisco IOS Release 12.2SR System Message Guide](#)
- [Cisco IOS System Messages, Volume 1 of 2](#) (Cisco IOS Release 12.4)
- [Cisco IOS System Messages, Volume 2 of 2](#) (Cisco IOS Release 12.4)

## Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG\_FILE environment variable. The CONFIG\_FILE variable defaults to NVRAM.

## Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:  
[http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf\\_cli-basics.html](http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html)  
or  
“Using Cisco IOS XE Software” chapter of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*:  
[http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using\\_CLI.html](http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html)
- Cisco Product Support Resources  
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)  
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)  
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software  
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)  
<http://tools.cisco.com/Support/CLILookup>

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

<https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl>

---

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.





## Dial Peer Overview

---

Configuring dial peers is the key to implementing dial plans and providing voice services over an IP packet network. Dial peers are used to identify call source and destination endpoints and to define the characteristics applied to each call leg in the call connection.

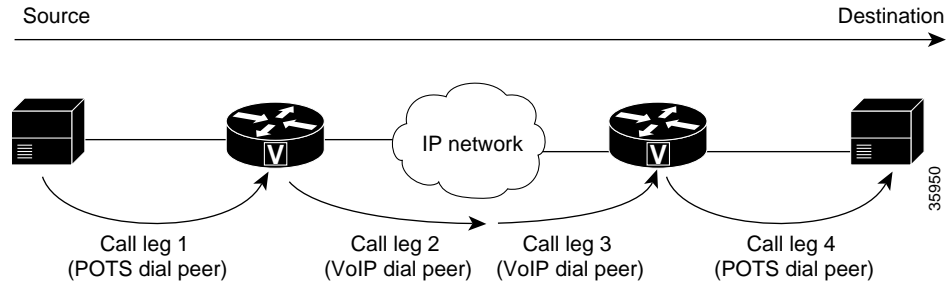
This chapter contains the following sections:

- [Call Legs, page 1](#)
- [POTS Dial Peers, page 4](#)
- [Voice-Network Dial Peers, page 4](#)
- [Data Dial Peers, page 5](#)
- [Creating a Dial Peer Configuration Table, page 5](#)
- [Codecs, page 6](#)
- [Toll Fraud Prevention, page 9](#)

## Call Legs

A traditional voice call over the public switched telephone network (PSTN) uses a dedicated 64K circuit end to end. In contrast, a voice call over the packet network is made up of discrete segments or call legs. A call leg is a logical connection between two routers or between a router and a telephony device. A voice call comprises four call legs, two from the perspective of the originating router and two from the perspective of the terminating router, as shown in [Figure 1](#).



**Figure 1** *Dial Peer Call Legs*

A dial peer is associated with each call leg. Attributes that are defined in a dial peer and applied to the call leg include the codec, quality of service (QoS), voice activity detection (VAD), and fax rate. To complete a voice call, you must configure a dial peer for each of the four call legs in the call connection.

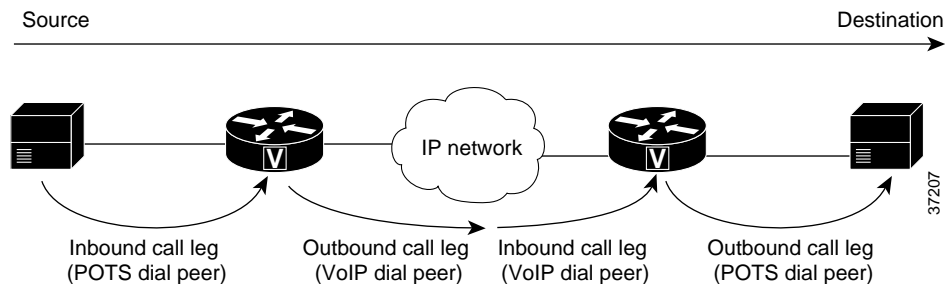
Depending on the call leg, a call is routed using one of the two types of dial peers:

- Plain old telephone system (POTS)—Dial peer that defines the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN, PBX, or telephone.
- Voice-network—Dial peer that defines the characteristics of a packet network connection. Voice-network dial peers map a dialed string to a remote network device, such as the destination router that is connected to the remote telephony device.

Both POTS and voice-network dial peers are needed to establish voice connections over a packet network.

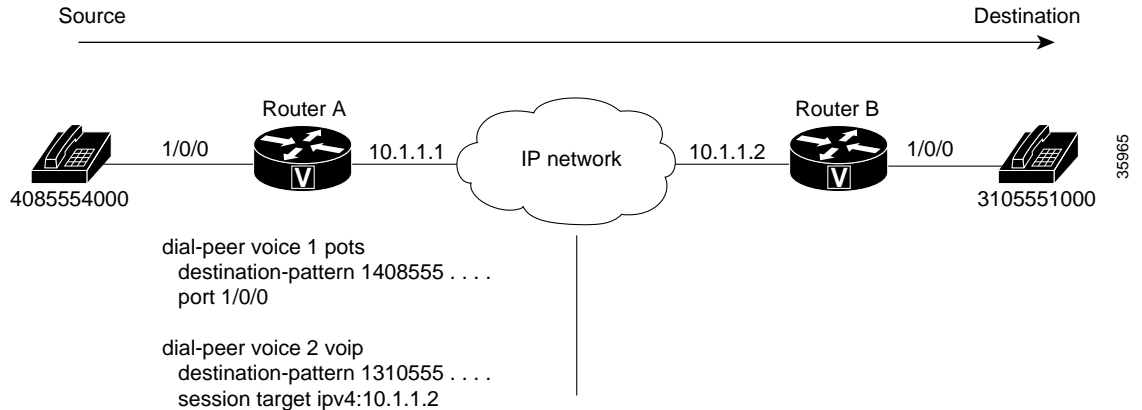
When a voice call comes into the router, the router must match dial peers to route the call. For inbound calls from a POTS interface that are being sent over the packet network, the router matches a POTS dial peer for the inbound call leg and a voice-network dial peer for the outbound call leg. For calls coming into the router from the packet network, the router matches an outbound POTS dial peer to terminate the call and an inbound voice-network dial peer for features such as codec, VAD, and QoS.

Figure 2 shows the call legs and associated dial peers necessary to complete a voice call.

**Figure 2** *Matching Call Legs to Dial Peers*

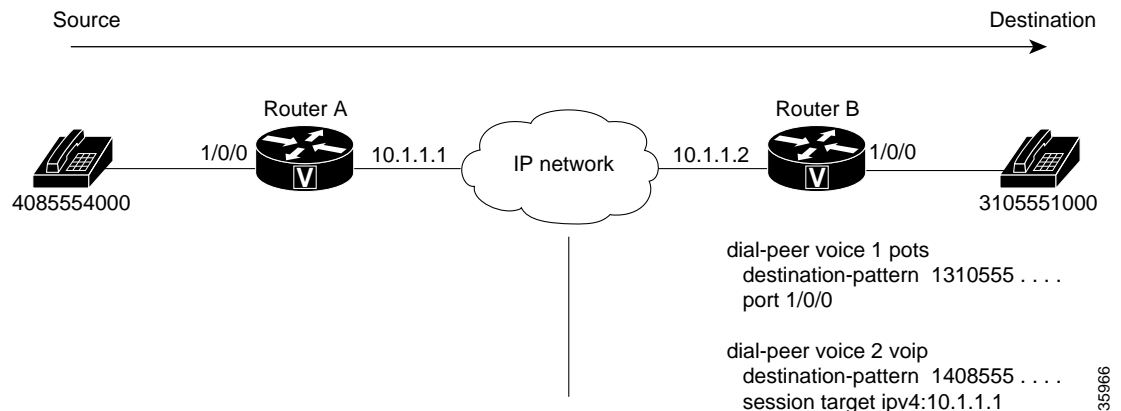
The following configurations show an example of a call being made from 4085554000 to 3105551000.

Figure 3 shows the inbound POTS dial peer and the outbound voice over IP (VoIP) dial peer that are configured on the originating router. The POTS dial peer establishes the source of the call (via the calling number or voice port), and the voice-network dial peer establishes the destination by associating the dialed number with the network address of the remote router.

**Figure 3** *Dial Peers from the Perspective of the Originating Router*

In this example, the dial string 14085554000 maps to telephone number 555-4000, with the digit 1 plus the area code 408 preceding the number. When you configure the destination pattern, set the string to match the local dialing conventions.

[Figure 4](#) shows the inbound VoIP dial peer and outbound POTS dial peer that are configured on the terminating router to complete the call. Dial peers are of local significance only.

**Figure 4** *Dial Peers from the Perspective of the Terminating Router*

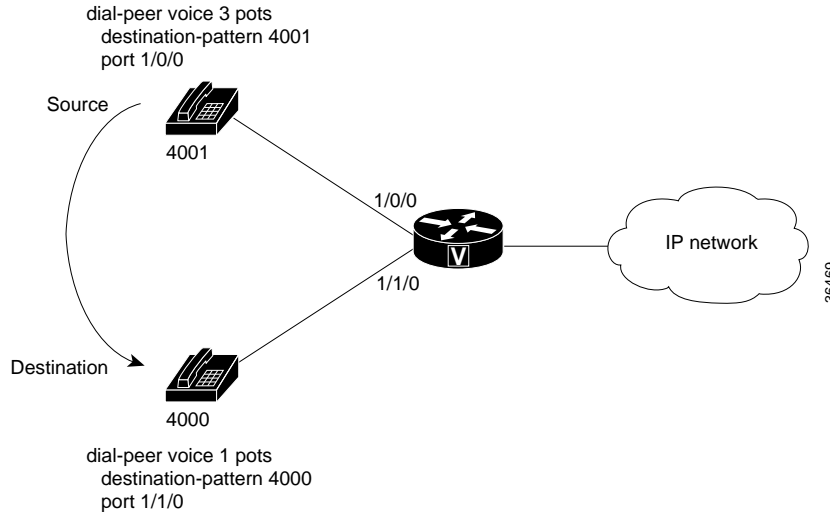
In the previous configuration examples, the last four digits in the VoIP dial peer's destination pattern were replaced with wildcards. Which means that from Router A, calling any telephone number that begins with the digits "1310555" will result in a connection to Router B. This behavior implies that Router B services all numbers beginning with those digits. From Router B, calling any telephone number that begins with the digits "1408555" will result in a connection to Router A. This behavior implies that Router A services all numbers beginning with those digits.

**Note**

It is not always necessary to configure the inbound dial peers. If the router is unable to match a configured dial peer for the inbound call leg, it uses an internally defined default POTS or voice-network dial peer to match inbound voice calls. In the example shown in [Figure 4](#), dial peer 2 is required only when making a call from Router B to Router A.

The only exception to the previous example occurs when both POTS dial peers share the same router, as shown in Figure 5. In this circumstance, you do not need to configure a voice-network dial peer.

**Figure 5** Communication Between Dial Peers Sharing the Same Router



This type of configuration is similar to the configuration used for hairpinning, which occurs when a voice call destined for the packet network is instead routed back over the PSTN because the packet network is unavailable.

## POTS Dial Peers

POTS dial peers retain the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN, PBX, or telephone.

## Voice-Network Dial Peers

Voice-network dial peers are components on an IP network to which a voice gateway router points via the component's IP address specified in the **session-target** command for a particular matching dial peer. The four types of voice-network dial peers (VoIP, voice over ATM (VoATM), voice over Frame Relay (VoFR), and multimedia mail over IP (MMoIP)) are determined according to the given packet network technology and are described as follows:

- VoIP—Points to the IP address of the destination router that terminates the call.
- VoFR—Points to the data-link connection identifier (DLCI) of the interface from which the call exits the router.
- VoATM—Points to the ATM virtual circuit for the interface from which the call exits the router.
- MMoIP—Points to the e-mail address of the simple mail transfer protocol (SMTP) server. This type of dial peer is used only for fax traffic.

# Data Dial Peers

Before Cisco IOS Release 12.2(11)T, a Cisco voice gateway would try to match a voice dial peer before matching and processing a modem call. If a voice dial peer was matched, the call was processed as voice. If there was no voice dial peer match, only then was a call considered to be a modem call. Voice calls always received preference over modem calls. Also, there was no way to assign a subset of addresses in the numbering plan for data calls.

In Cisco IOS Release 12.2(11)T, an interim solution in the form of application called “data\_dialpeer” was introduced to enable gateways to identify dial peers. The application enabled the handling of certain matched calls as modem calls. Refer to the *Fine-Grain Address Segmentation in Dial Peers* feature documentation in Cisco IOS Release 12.2(11)T for more information.

In Cisco IOS Release 12.2(13)T, formal support for data dial peers was released in the form of the *Dial-Peer Support for Data Calls* feature, which enables the configuration and order assignment of dial peers so that the gateway can identify incoming calls as voice or data (modem). You can use the **dial-peer data** and **dial-peer search** commands to perform this configuration. Refer to the “[Data Dial Peers](#)” section on page 33 for configuration steps and examples.

## Creating a Dial Peer Configuration Table

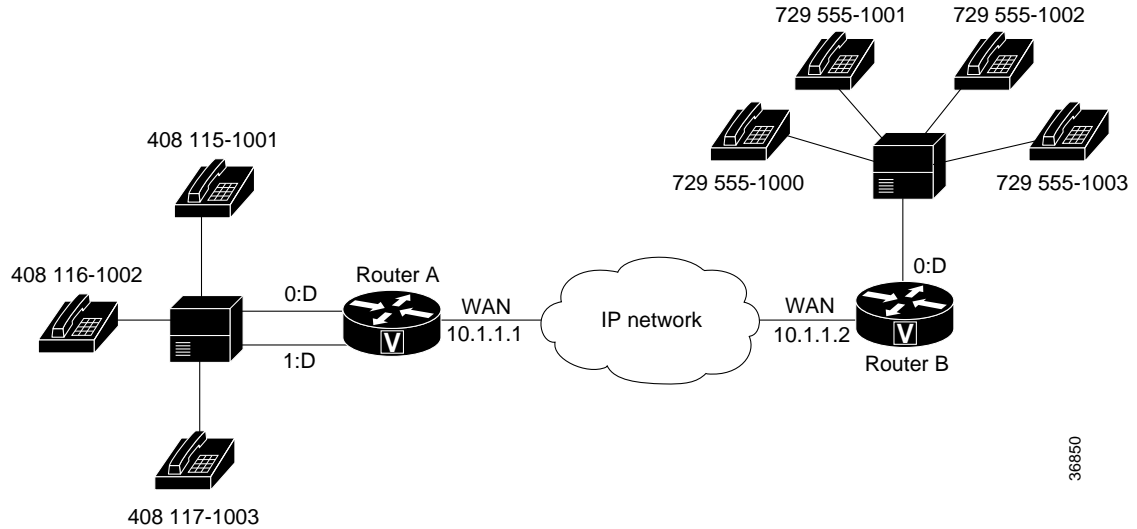
Before you can configure dial peers, you must obtain specific information about your network. One way to identify this information is to create a dial peer configuration table. This table should contain all the telephone numbers and access codes for each router that is carrying telephone traffic in the network. Because most installations require integrating equipment into an existing voice network, the telephone dial plans are usually preset.

[Figure 6](#) shows an example of a network in which Router A, with an IP address of 10.1.1.1, connects a small sales branch office to the main office through Router B, with an IP address of 10.1.1.2.

**Note**

The example in [Figure 6](#) shows a VoIP configuration. The same concepts also apply to VoFR and VoATM applications. The only change is in the format of the session target.

Figure 6 Sample VoIP Network



36850

Three telephone numbers in the sales branch office need dial peers configured for them. Router B is the primary gateway to the main office; as such, it needs to be connected to the company’s PBX. Four devices need dial peers, all of which are connected to the PBX, configured for them in the main office.

Table 1 shows the peer configuration table for the example in Figure 6.

Table 1 Dial Peer Configuration Table for Sample Voice over IP Network

Dial Peer	Extension	Prefix	Destination Pattern	Type	Voice Port	Session Target
<b>Router A</b>						
1	51001	5	1408115....	POTS	0:D	—
2	61002	6	1408116....	POTS	0:D	—
3	71003	7	1408117....	POTS	0:D	—
10	—	—	1729555....	VoIP	—	10.1.1.2
<b>Router B</b>						
1	1000, 1001, 1002, 1003	—	1729555....	POTS	0:D	—
10	—	—	1408.....	VoIP	—	10.1.1.1

## Codecs

The term *codec* stands for *coder-decoder*. A codec is a particular method of transforming analog voice into a digital bit stream (and vice versa) and also refers to the type of compression used. Several different codecs have been developed to perform these functions, and each one is known by the number of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard in which it is defined. For example, two common codecs are the G.711 and the G.729 codecs.

Codecs use different algorithms to encode analog voice into digital bit streams and have different bit rates, frame sizes, and coding delays associated with them. Codecs also differ in the amount of perceived voice quality they achieve. Specialized hardware and software in the digital signal processors (DSPs) perform codec transformation and compression functions, and different DSPs may offer different selections of codecs.

Select the same type of codec at both ends of the call. For instance, if a call was coded with a G.729 codec, it must be decoded with a G.729 codec. Codec choice is configured on dial peers.

Table 2 lists the H.323, SIP, and MGCP codecs that are supported for voice.

**Table 2** Voice Codec/Signaling Support Matrix

Codec	H.323	SIP	MGCP
g711ulaw	Yes	Yes	Yes
g711alaw	Yes	Yes	Yes
g729r8 <sup>1</sup>	Yes	Yes	Yes
g729br8 <sup>1</sup>	Yes	Yes	Yes
g723ar53	Yes	Yes	Yes
g723ar63	Yes	Yes	Yes
g723r53	Yes	Yes	Yes
g723r63	Yes	Yes	Yes
gsmfr	Yes	Yes	No
g726r16 <sup>2</sup>	Yes	Yes	Yes
g726r24 <sup>2</sup>	Yes	Yes	Yes
g726r32	Yes	Yes	Yes
clear-channel <sup>2</sup>	Yes	Yes	Yes
iLBC	Yes	Yes	No

1. Annex A is used in the Cisco platforms that are supported in this software release.

2. For dynamic payload types.

For more information, refer to the “Configuring Dial Plans, Dial Peers, and Digit Manipulation” chapter and the “Configuring Voice Ports” chapter in the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

## Clear Channel (G.Clear) Codec

G.Clear guarantees bit integrity when transferring a DS-0 through a gateway server, supports the transporting of nonvoice circuit data sessions through a Voice over IP (VoIP) network, and enables the VoIP networks to transport ISDN and switched 56 circuit-switched data calls. With the availability of G.Clear, ISDN data calls that do not require bonding can be supported.

In a transit application, because it is possible to have a mix of voice and data calls, not supporting G.Clear limits the solution to voice-only calls. The end-user application is in charge of handling packet loss and error recovery. This packet loss management precludes the use of clear channel with some applications unless the IP network is carefully engineered.

In an MGCP environment, the voice gateway backhauls the public switched telephony network (PSTN) signaling channel to the call agent. The call agent examines the bearer capability and determines when a G.Clear call should be established.

**Note**

G.Clear codecs cannot be configured on a T1 channel associated signaling (CAS) trunk for incoming traffic. T1 CAS trunks use least significant bit-robbing for signaling, which causes the data to be incorrect and re-sent from high level protocols. Traffic on an incoming E1 R2 trunk can be configured.

## GSM Full Rate Codec

The GSMFR codec was introduced in 1987. The GSMFR speech coder has a frame size of 20 ms and operates at a bit rate of 13 kbps. GSMFR is an RPE-LTP (Regular Pulse Excited – Linear Predictive) coder.

In order to write VoiceXML scripts that can function as the user interface for a simple voice-mail system, the network must support GSMFR codecs. The network messaging must be capable of recording a voice message and depositing the message to an external server for later retrieval.

This codec supports the Cisco infrastructure and application partner components required for service providers to deploy unified messaging applications.

## Adaptive Differential PCM Voice Codec—G.726

Adaptive differential pulse code modulation (ADPCM) voice codec operates at bit rates of 16, 24, and 32 kbps. ADPCM provides the following functionality:

- Voice mail recording and playback, which is a requirement for Internet voice mail.
- Voice transport for cellular, wireless, and cable markets.
- High voice quality voice transport at 32 kbps.

## iLBC Codec

The internet Low Bitrate Codec (iLBC) Has the following benefits:

- Is designed specifically for packet-based communication.
- Is royalty free.
- Provides high-voice quality, even in conditions with high-packet loss.
- Has a sampling rate of 8 kHz, for narrow band speech.
- Supports two fixed bit-rate frame lengths:
  - Bit-rate of 13.3 kbps with an encoding frame length of 30 ms
  - Bit-rate of 15.2 kbps with an encoding frame length of 20 ms
- Is designed to be robust, even with packet loss. iLBC treats each packet independently and recovers from packet loss on the packet immediately following the lost one. By utilizing the entire available frequency band, this codec provides a high voice quality.

### Platforms that iLBC Supports

iLBC is supported on Cisco AS5350XM and Cisco AS5400XM Universal Gateways with Voice Feature Cards (VFCs) and IP-to-IP gateways with no transcoding and conferencing.

### Using iLBC with SIP

- For iLBC codecs using SIP, use RFC3952 as a reference for implementation.
- Mid-call codec parameter changes using SIP are supported. For example, iLBC 'mode' and 'ptime' changes are supported using SIP during the call.

### Using iLBC with H.323

- For iLBC codecs using H.323, a new proposal is written and submitted for approval to ITU. The new proposal is added as 'Annex S' in H245, Version 12 which is used as reference for implementation. See H245, version 12 document at [http://www.packetizer.com/voip/h245/Version12/h245\\_ww9.zip](http://www.packetizer.com/voip/h245/Version12/h245_ww9.zip)
- Mid-call codec parameter changes using H.323 are not supported.

## Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports—By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)—Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports—If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060—If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration—If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication—If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.

- Explicit incoming and outgoing dial peers—Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns—Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules—Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts—Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation—Use the “permit hostname” feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)—If you are using DNS as the “session target” on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the [“Cisco IOS Unified Communications Toll Fraud Prevention”](#) paper.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



## Dial Planning

---

A dial plan essentially describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed are all part of a dial plan. For instance, the North American public switched telephone network (PSTN) uses a 10-digit dial plan that includes a 3-digit area code and a 7-digit telephone number. Most PBXs support variable length dial plans that use 3 to 11 digits. Dial plans must comply with the telephone networks to which they connect. Only totally private voice networks that are not linked to the PSTN or to other PBXs can use any dial plan they choose.

Dial plans on Cisco routers are manually defined using dial peers. Dial peers are similar to static routes; they define where calls originate and terminate and what path the calls take through the network. Attributes within the dial peer configuration determine which dialed digits the router collects and forwards to telephony devices. Dial peer configuration allows you to implement both fixed- and variable-length dial plans for your existing voice network and enables you to adjust to future scalability needs that may arise as your voice network expands or contracts.

This chapter contains the following sections:

- [Fixed-Length Dial Plans, page 1](#)
- [Variable-Length Dial Plans, page 2](#)

## Fixed-Length Dial Plans

Fixed-length dialing plans, in which all the dial peer destination patterns have a fixed length, are sufficient for most voice networks because the telephone number strings are of known lengths. Some voice networks, however, require variable-length dial plans, particularly for international calls, which use telephone numbers of different lengths.

If you enter the timeout T-indicator at the end of the destination pattern in an outbound voice-network dial peer, the router accepts a fixed-length dial string and then waits for additional dialed digits. The timeout character must be an uppercase T. The following dial peer configuration shows how the T-indicator is set to allow variable-length dial strings:

```
dial-peer voice 1 voip
destination-pattern 2222T
session target ipv4:10.10.1.1
```



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

In the example, the router accepts the digits 2222, and then waits for an unspecified number of additional digits. The router can collect up to 31 additional digits, as long as the interdigit timeout has not expired. When the interdigit timeout expires, the router places the call.

The default value for the interdigit timeout is 10 seconds. Unless the default value is changed, using the T-indicator adds 10 seconds to each call setup because the call is not attempted until the timer has expired (unless the # character is used as a terminator). You should therefore reduce the voice-port interdigit timeout value if you use variable-length dial plans. You can change the interdigit timeout by using the **timeouts inter-digit** command in voice-port configuration mode.

The calling party can immediately terminate the interdigit timeout by entering the # character. If the # character is entered while the router is waiting for additional digits, the # character is treated as a terminator; it is not treated as part of the dial string or sent across the network. But if the # character is entered before the router begins waiting for additional digits (meaning that the # is entered as part of the fixed-length destination pattern), then the # character is treated as a dialed digit.

For example, if the destination pattern is configured as 2222 . . T, then the entire dialed string of 2222#9999 is collected, but if the dialed string is 2222#99#99, the #99 at the end of the dialed digits is not collected because the final # character is treated as a terminator. You can change the termination character by using the **dial-peer terminator** command.


**Note**

In most cases, you must configure the T-indicator only when the router uses two-stage dialing. If direct inward dialing (DID) is configured in the inbound plain old telephone system (POTS) dial peer, the router uses one-stage dialing, which means that the full dialed string is used to match outbound dial peers. The only exception is when the **isdn overlap-receiving** command is configured; the ISDN overlap-receiving feature requires the T-indicator.

## Variable-Length Dial Plans

In most voice configurations, fixed-length dialing plans, in which all the dial peer destination patterns have the same length, are sufficient because the telephone number strings are all the same length. However, in some voice network configurations, variable-length dial plans are required, especially if the network connects two or more countries where telephone number strings could be different lengths.

If you enter the “T” timer character in the destination pattern for your dial peer, the router can be configured to accept a fixed-length dial string, and then wait for additional dialed digits. For example, the following dial peer configuration shows how the T character can be set to allow variable-length dial strings:

```
dial peer voice 1 pots
destination-pattern 2222T
port 1/1
```

In this example, the router accepts the digits 2222, and then waits for an unspecified number of dialed digits. If digits continue to be entered before the interdigit timeout expires, then the router will continue to gather up to 31 additional digits. Once the interdigit timeout expires, however, the router places the call. You can configure the interdigit timeout value by using the **timeouts inter-digit** command in **voice-port** configuration mode.

The interdigit timeout timer can be terminated by entering the “#” character. If the # character is entered while the router is waiting to accept additional digits, the # character is treated as an end-dial accelerator. The # character is not treated as an actual digit in the destination pattern and is not sent as part of the dialed string across the network.

However, if the # character is entered before the router is ready to accept additional digits (meaning before the “T” character is entered in the destination pattern), then the # character is treated as a dialed digit. For example, if a destination pattern is configured with the string 2222...T, then the digits 2222#####1234567 can be gathered, but the digits 2222#####1234#67 cannot be gathered because the final # character is treated as a terminator.

The default value for the interdigit timeout is 10 seconds. If the duration is not changed, using the “T” timer adds 10 seconds to each call setup time because the call is not attempted until the timer expires (unless the # character is used as a terminator). Because of this dependency, if a variable-length dial plan is used, the interdigit timeout should be reduced to reduce the call setup time. For more information, refer to the [“Variable-Length Matching” section on page 37](#).

---

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





## Dial Peer Features and Configuration

---



**Note**

---

The example configurations in this section show voice over IP (VoIP) dial peers; the same concepts also apply to voice over Frame Relay (VoFR) and voice over ATM (VoATM) dial peers.

---

Establishing voice communication over a packet network is similar to configuring a static route: You are establishing a specific voice connection between two defined endpoints. Call legs define the discrete segments that lie between two points in the call connection. A voice call over the packet network comprises four call legs, two on the originating router and two on the terminating router; a dial peer is associated with each of these four call legs.

## Common Practices

The following three sections cover the bare essential configuration steps necessary to support voice transmission and reception on a typical voice gateway router in your network:

- [Voice Ports, page 1](#)
- [Session Targets, page 2](#)
- [Destination Patterns, page 4](#)

## Voice Ports

Your dial peer configuration cannot function until you have logically assigned a voice port to one or more dial peers. Assigning voice ports to dial peers identifies the physical hardware in the router that will be employed to complete voice communication to and from associated voice network endpoints.

## Assigning Voice Ports

The purpose of this task is to assign a voice port to a plain old telephone system (POTS) dial peer.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* pots**
4. **port *string***

## DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>dial-peer voice <i>number</i> pots</code>  <b>Example:</b> Router(config)# dial-peer voice 864 pots	Enters dial-peer voice configuration mode and defines a local POTS dial peer. <ul style="list-style-type: none"> <li>• The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<code>port <i>string</i></code>  <b>Example:</b> Router(config-dialpeer)# port 1/0:0	Specifies the voice port associated with the given dial peer. The <b>port</b> command syntax is platform-specific. For more information about the syntax of this command, refer to the <b>port</b> command in the <i>Cisco IOS Voice, Video, and Fax Command Reference</i> .



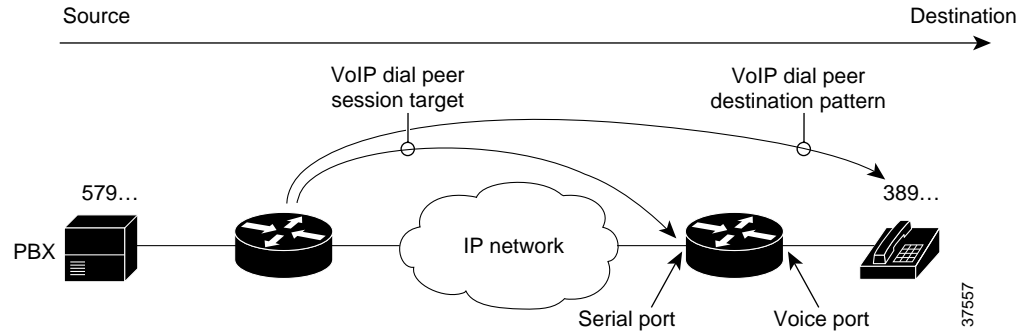
### Note

Voice port assignments are configured for POTS dial peers only.

## Session Targets

The session target is the network address of the remote router to which you want to send a call once a local voice-network dial peer is matched. It is configured in voice-network dial peers by using the **session target** command. For outbound dial peers, the destination pattern is the telephone number of the remote voice device that you want to reach. The session target represents the path to the remote router that is connected to that voice device. [Figure 7](#) illustrates the relationship between the destination pattern and the session target, as shown from the perspective of the originating router.

**Figure 7 Relationship Between Destination Pattern and Session Target**



The address format of the session target depends on the type of voice-network dial peer:

- VoIP—IP address, host name of the Domain Name System (DNS) server that resolves the IP address, **ras** for registration, admission, and status (RAS) if an H.323 gatekeeper resolves the IP address, or **settlement** if the settlement server resolves the IP address
- VoFR—Interface type and number and the data link connection identifier (DLCI)
- VoATM—Interface number, and ATM virtual circuit
- MMoIP—E-mail address



**Note** For inbound dial peers, the session target is ignored.

## Configuring Session Targets

The purpose of this task is to assign a session target to a voice-network dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* { **voip** | **vofr** | **voatm** }
4. **session-target** *ip-address*

### DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.

	Command	Purpose
Step 3	<code>dial-peer voice number {voip   vofr   voatm}</code>  <b>Example:</b> Router(config)# dial-peer voice 864 voip	Enters dial-peer voice configuration mode and defines a local dial peer. <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<code>session-target ip-address</code>  <b>Example:</b> Router(config-dialpeer)# session-target 10.45.44.43	Defines the IP address identifying the next-hop location of the voice network component associated with this dial peer.

## Destination Patterns

The destination pattern associates a dialed string with a specific telephony device. It is configured in a dial peer by using the **destination-pattern** command. If the dialed string matches the destination pattern, the call is routed according to the voice port in POTS dial peers, or the session target in voice-network dial peers. For outbound voice-network dial peers, the destination pattern may also determine the dialed digits that the router collects and then forwards to the remote telephony interface, such as a PBX, a telephone, or the public switched telephone network (PSTN). You must configure a destination pattern for each POTS and voice-network dial peer that you define on the router.

## Configuring Destination Patterns

The purpose of this task is to configure a destination pattern for a dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice number {pots | voip | vofr | voatm}**
4. **destination-pattern [+] string [T]**

### DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command	Purpose
Step 3	<p><code>dial-peer voice number {pots   voip   vofr   voatm}</code></p> <p><b>Example:</b> Router(config)# dial-peer voice 123 voip</p>	<p>Enters dial-peer voice configuration mode and defines a local dial peer.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<p><code>destination-pattern [+] string [T]</code></p> <p><b>Example:</b> Router(config-dialpeer)# destination-pattern 5551234</p>	<p>Defines the telephone number that identifies the destination pattern associated with this dial peer. The keywords and argument are as follows:</p> <ul style="list-style-type: none"> <li>+—(Optional) Character indicating an E.164 standard number.</li> <li><i>string</i>—A series of digits specifying the E.164 or private dial plan telephone number. Valid entries are as follows: <ul style="list-style-type: none"> <li>Digits 0 through 9, letters A through D, pound sign (#), and asterisk (*), which represent specific digits that can be entered.</li> <li>Comma (,), which inserts a pause between digits.</li> <li>Period (.), which matches any entered digit.</li> </ul> </li> <li><b>T</b>—(Optional) Control character indicating that the <b>answer-address</b> value is a variable-length dial string.</li> </ul>

## Digit Manipulation

The router may need to manipulate digits in a dial string before it passes the dial string to the telephony device. Which can be necessary, for instance, when calling PBXs with different capabilities to accept digits, or for PSTN and international calls. You may need to consider different strategies for configuring digit manipulation within your dial peers depending on your existing dial plan, the digits users are expected to dial, and the capabilities of your PBX or key system unit (KSU). These digit-manipulation options, in conjunction with the destination pattern, determine the dial string that the router forwards to the telephony device.

## Wildcards

The destination pattern can be either a complete telephone number or a partial telephone number with wildcard digits, represented by a period (.) character. Each “.” represents a wildcard for an individual digit that the originating router expects to match. For example, if the destination pattern for a dial peer is defined as “555 . . . .”, then any dialed string beginning with 555, plus at least four additional digits, matches this dial peer.

In addition to the period (.), several other symbols can be used as wildcard characters in the destination pattern. These symbols provide additional flexibility in implementing dial plans and decrease the need for multiple dial peers in configuring telephone number ranges.

Table 3 shows the wildcard characters that are supported in the destination pattern.

**Table 3 Wildcard Symbols Used in Destination Patterns**

Symbol	Description
.	Indicates a single-digit placeholder. For example, 555 . . . matches any dialed string beginning with 555, plus at least four additional digits.
[ ]	Indicates a range of digits. A consecutive range is indicated with a hyphen (-); for example, [5-7]. A nonconsecutive range is indicated with a comma (,); for example, [5,8]. Hyphens and commas can be used in combination; for example, [5-7,9]. <b>Note</b> Only single-digit ranges are supported. For example, [98-102] is invalid.
( )	Indicates a pattern; for example, 408(555). It is used in conjunction with the symbol ?, %, or +.
?	Indicates that the preceding digit occurred zero or one time. Enter <b>ctrl-v</b> before entering ? from your keyboard.
%	Indicates that the preceding digit occurred zero or more times. This functions the same as the "*" used in regular expression.
+	Indicates that the preceding digit occurred one or more times.
T	Indicates the interdigit timeout. The router pauses to collect additional dialed digits.

Table 4 shows some examples of how these wildcard symbols are applied to the destination pattern and the dial string that results when dial string 4085551234 is matched to an outbound POTS dial peer. The wildcard symbols follow regular expression rules.

**Table 4 Dial Peer Matching Examples Using Wildcard Symbols**

Destination Pattern	Dial String Translation	String After Stripping <sup>1</sup>
408555.+	408555, followed by one or more wildcard digits. This pattern implies that the string must contain at least 7 digits starting with 408555.	1234
408555.%	408555, followed by zero or more wildcard digits. This pattern implies that the string must contain at least 408555.	1234
408555+	40855, followed by 5 repeated one or more times.	1234
408555%	40855, followed by 5 repeated one or more times. Any explicitly matching digit before the % symbol is not stripped off.	51234
408555?	40855, followed by 5. Any explicitly matching digit before the ? symbol is not stripped off.	51234
40855[5-7].+	40855, followed by 5, 6, or 7, plus any digit repeated one or more times.	51234
40855[5-7].%	40855, followed by 5, 6, or 7, plus any digit repeated one or more times.	51234
40855[5-7]+1234	40855, followed by 5, 6, or 7 repeated one or more times, followed by 1234.	51234
408(555)+1234	408, followed by 555, which may repeat one or more times, followed by 1234.	5551234

1. These examples apply only to one-stage dialing, where direct inward dialing (DID) is enabled on the inbound POTS dial peer. If the router is using two-stage dialing and collecting digits one at a time as dialed, then the call is routed immediately after a dial peer is matched and any subsequent dialed digits are lost.

In addition to wildcard characters, the following characters can be used in the destination pattern:

- Asterisk (\*) and pound sign (#)—These characters on standard touch-tone dial pads can be used anywhere in the pattern. They can be used as the leading character (for example, \*650), except on the Cisco 3600 series.
- Dollar sign (\$)—Disables variable-length matching. It must be used at the end of the dial string.
- Circumflex symbol (^)—When used within brackets, allows you to eliminate a digit from consideration for dial peer matching purposes. For example, a destination pattern including [^7] would not match any string beginning with 7.

Multiple digits can also be called out within brackets to eliminate more than one initial digit from dial peer matching. For example, a destination pattern including [^4^6^8] would not match any digit string beginning with 4, 6, or 8.



**Note** A destination pattern including [^752] would allow matching only for digit strings beginning with 5 or 2, but would not match any digit strings beginning with 7. This destination pattern entry essentially behaves the same way as if you had simply included [52] in the destination pattern.

To eliminate a multiple digit string from dial peer matching consideration, you must represent each digit in the string as a succession of individual exceptions. For example, if you wanted to eliminate matching any digit string beginning with 537 from consideration for dial peer matching, you must ensure that your destination pattern includes [^5][^3][^7].

The same destination pattern can be shared across multiple dial peers to form hunt groups.

## Digit Stripping and Prefixes

When a terminating router receives a voice call, it selects an outbound POTS dial peer by comparing the called number (the full E.164 telephone number) in the call information with the number configured as the destination pattern in the POTS dial peer. The access server or router then strips off the left-justified digits that match the destination pattern. If you have configured a prefix, the prefix is added to the front of the remaining digits, creating a dial string, which the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

For example, consider a voice call whose E.164 called number is 1(408) 555-2222. If you configure a destination-pattern of "1408555" and a prefix of "9," the router strips off "1408555" from the E.164 telephone number, leaving the extension number of "2222." It then appends the prefix, "9," to the front of the remaining numbers, so that the actual numbers dialed are "9, 2222." The comma in this example means that the router will pause for 1 second between dialing the "9" and dialing the "2" to allow for a secondary dial tone.

When the terminating router matches a dial string to an outbound POTS dial peer, by default the router strips off the left-justified digits that explicitly match the destination pattern. Any remaining digits, called *excess digits*, are forwarded to the telephony interface, such as a PBX or the PSTN.

Some telephony interfaces require that any digits stripped from the dial string be recovered to support a particular dial plan. You can strip these digits either by using the **no digit-strip** dial-peer voice configuration command to disable the default digit-stripping behavior or by using the **prefix** dial-peer voice configuration command to add digits to the beginning of the dial string before it is forwarded to the telephony interface. These commands are supported only in POTS dial peers.

The **no digit-strip** command disables the automatic digit-stripping function so that matching digits are not stripped from the dialed string before it is passed to the telephony interface. For example, in the following dial peer configuration, the entire seven-digit dialed string is passed to the telephony interface:

```
dial-peer voice 100 pots
 destination-pattern 555....
 no digit-strip
 port 1/0:1
```

Disabling digit stripping is useful when the telephony interface requires the full dialed string. With some dial plans, however, the dialed digits must be manipulated according to specific rules. The **prefix** command can be used to add specific digits to the beginning of the dialed string before it is forwarded to the telephony interface.

For example, consider a telephone whose E.164 called number is 1(408)555-1234. This telephone can be reached within the company by dialing its extension number, 51234. If you configure a destination pattern of “1408555 . . .” (the periods represent wildcards) for the associated outbound POTS dial peer, the terminating gateway will strip off the digits “1408555” when it receives a call for 1(408)555-1234. For the terminating gateway to forward the call to the appropriate destination, the digit “5” needs to be prepended to the remaining digits. In this case, you would configure a prefix of 5, as shown in the following dial peer configuration.

```
dial-peer voice 100 pots
 destination-pattern 1408555....
 prefix 5
 port 1/0:1
```

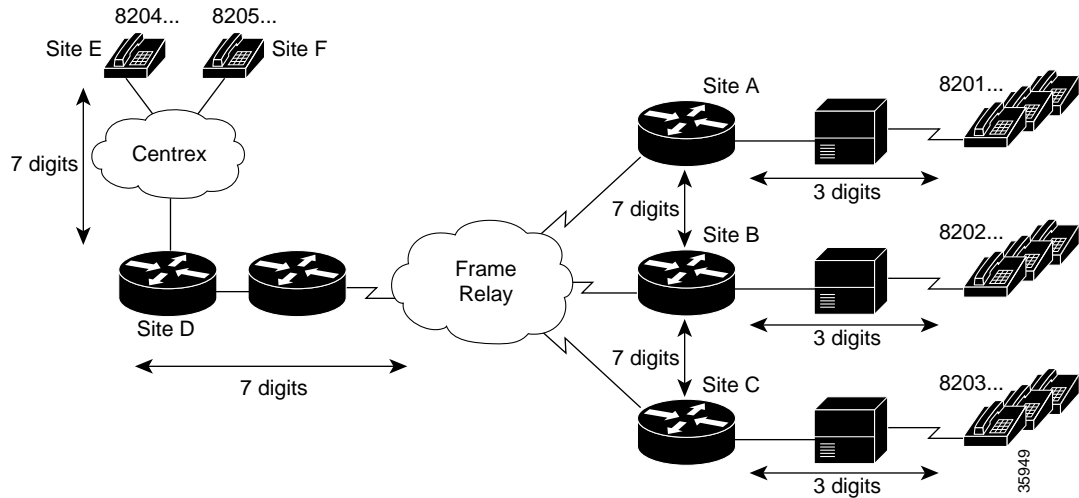
A prefix can also include commas (.). Each comma indicates a 1-second pause in dialing. For example, consider a telephone whose E.164 called number is 1(408)555-1234; to reach this device, you must dial “9.” In this case, you might configure “1408 . . . . .” as the destination pattern, and “9” as the prefix. In this example, the terminating router will strip the digits “1408” from the called number and append the digit “9” to the front of the remaining digits, so that the actual number dialed is “9,5551234.” The router pauses for 1 second between dialing the “9” and the “5551234” to allow for a secondary dial tone. In this example, you would configure the router as follows:

```
dial-peer voice 100 pots
 destination-pattern 1408.....
 prefix 9,
 port 1/0:1
```

Using a comma with the **prefix** command is useful when the router must allow for a secondary dial tone; otherwise the router does not wait for the dial tone before playing out excess digits. Putting commas in the prefix makes the router pause 1 second per comma, allowing for a dial tone to occur before the router transmits the remaining digits.

[Figure 8](#) shows an example of a network using the **no digit-strip** command. In this example, a central site (Site D) is connected to remote sites through routers (Sites A, B, and C), and through a Centrex system for sites still using the PSTN (Sites E and F). The Centrex service requires the full 7-digit dial string to complete calls. The dial peers are configured with a fixed-length 7-digit dial plan.

**Figure 8 Network with Digit Stripping Disabled or Prefixes Enabled**



When Site E (8204. . .) dials 8201999, the full 7-digit dialed string is passed through the Centrex to the router at Site D. Router D matches the destination pattern 8201. . . and forwards the 7-digit dial string to Router A. Router A matches the destination pattern 8201. . ., strips off the matching 8201, and forwards the remaining 3-digit dial string to the PBX. The PBX matches the correct station and completes the call to the proper extension.

Calls in the reverse direction are handled similarly, but because the Centrex service requires the full 7-digit dial string to complete calls, the POTS dial peer at Router D is configured with digit stripping disabled. Alternatively, digit stripping could be enabled and the dial peer could instead be configured with a 4-digit prefix, in this case 8204, which would result in forwarding the full dial string to the Centrex service.

Router A	Router D
<pre>dial-peer voice 1 pots  destination-pattern 8201...  port 1/0:1 ! dial-peer voice 4 vofr  destination-pattern 8204...  session target s0 2 ! dial-peer voice 5 vofr  destination-pattern 8205...  session target s0 2 !</pre>	<pre>dial-peer voice 4 pots  destination-pattern 8204...  no digit-strip  port 1/0:1 ! dial-peer voice 5 pots  destination-pattern 8205...  no digit-strip  port 1/0:1 ! dial-peer voice 1 vofr  destination-pattern 8201...  session target s0 1 !</pre>

### Forwarding Digits

The **forward-digits** command controls the number of digits that are stripped before the dialed string is passed to the telephony interface. On outbound POTS dial peers, the terminating router normally strips off all digits that explicitly match the destination pattern in the terminating POTS dial peer. Only digits matched by the wildcard pattern are forwarded. The **forward-digits** command can be used to forward a fixed number of dialed digits, or all dialed digits, regardless of the number of digits that explicitly match the destination pattern.

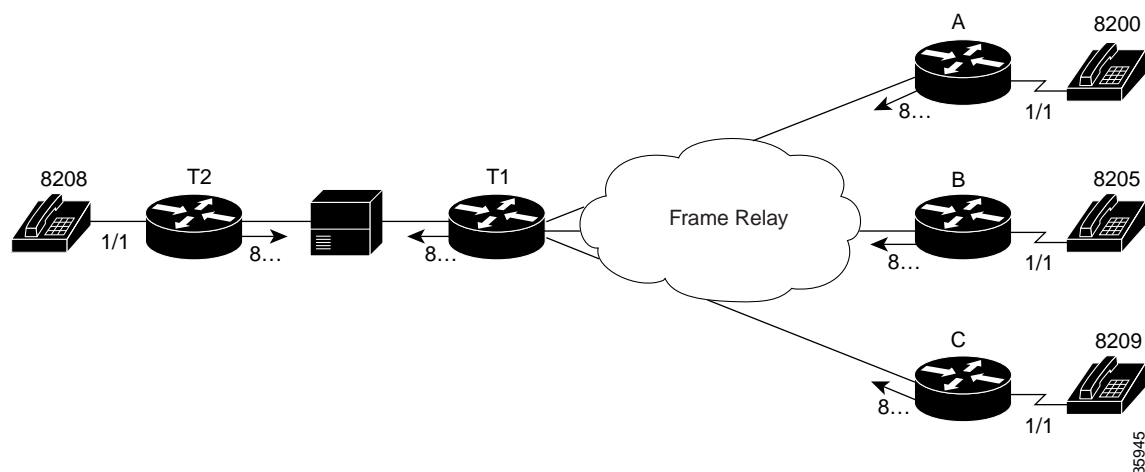
For example, the **forward-digits 4** command tells the router to forward the last four digits in the dialed string. The **forward-digits all** command instructs the router to forward the full dialed string. If the length of the dialed string is longer than the length of the destination pattern, the **forward-digits extra** command forwards the extra trailing digits. Extra digits are not forwarded, however, if the dial peer destination pattern is variable length; for example, 123T, 123 . . . T.

**Note**

The **forward-digits** command is supported only in POTS dial peers.

Figure 9 shows an example of routing voice calls through a PBX using forward digits. In this configuration, Routers T1 and T2 are tandem nodes that must support forward digits so that calls from Routers A, B, or C can make a call to extension 8208.

**Figure 9** Routing Voice Calls Through a PBX Using Forward Digits



In this example, all digits matched with destination 8 . . . are forwarded to the appropriate port. For a call from Router A to reach extension 8208, the call first terminates at Router T1, which transmits the digits 8208 to the voice port connected to the PBX. The PBX then routes the voice call to Router T2. The **forward-digits all** command is used here, but the **forward-digits 4** command could also be used in this example.

The following dial peer configurations are required on each router for this example:

Router T1	Router T2
<pre>dial-peer voice 1 vofr  destination-pattern 8200  session-target s0 1 ! dial-peer voice 6 vofr  destination-pattern 8205  session-target s0 6 ! dial-peer voice 10 vofr  destination-pattern 8209  session-target s0 10 ! dial-peer voice 1 pots  destination-pattern 8...  forward-digits all  port 1/1</pre>	<pre>dial-peer voice 8 pots  destination-pattern 8208  port 1/1 ! dial-peer voice 1000 pots  destination-pattern 8...  forward-digits all  port 1/1 ! dial-peer voice 9999 pots  destination-pattern ...  forward-digits all  port 1/1</pre>

Router A
<pre>dial-peer voice 1 pots  destination-pattern 8200  port 1/1 ! dial-peer voice 1000 vofr  destination-pattern 8...  session-target s0 1</pre>

## Number Expansion

In most corporate environments, the telephone network is configured so that you can reach a destination by dialing only a portion (an extension number) of the full E.164 telephone number. You can define an extension number as the destination pattern for a dial peer. The router can be configured to recognize the extension number and expand it into its full E.164 dialed number when the **num-exp** global configuration command is used with the **destination-pattern** dial-peer voice configuration command.

Number expansion is a globally applied rule that enables you to define a set of digits for the router to prepend to the beginning of a dialed string before passing it to the remote telephony device. Automatically prepending digits in the dial peer configuration reduces the number of digits that a user must dial to reach a remote location. Number expansion is similar to using a prefix, except that number expansion is applied globally to all dial peers.

Using a simple telephony-based example, suppose that user A works in a company where employees extensions are reached by dialing the last four digits of the full E.164 telephone number. The E.164 telephone number is 555-2123; user A's extension number is 2123. Suppose that every employee on user A's floor has a telephone number that begins with the same first four digits: 5552. You could define each dial peer's destination pattern using each extension number, and then use number expansion to prepend the first four digits onto the extension. In this example, the router could be configured as follows:

```
num-exp 2... 5552...
dial peer voice 1 pots
 destination pattern 2123
```

Number expansion can also be used to replace a dialed number with another number, as in the case of call forwarding. Suppose that for some reason, user A needs to have all of his telephone calls forwarded to another number, 555-6611. In this example, you would configure the router as follows:

```
num-exp 2123 5556611
dial-peer voice 1 pots
destination-pattern 2123
```

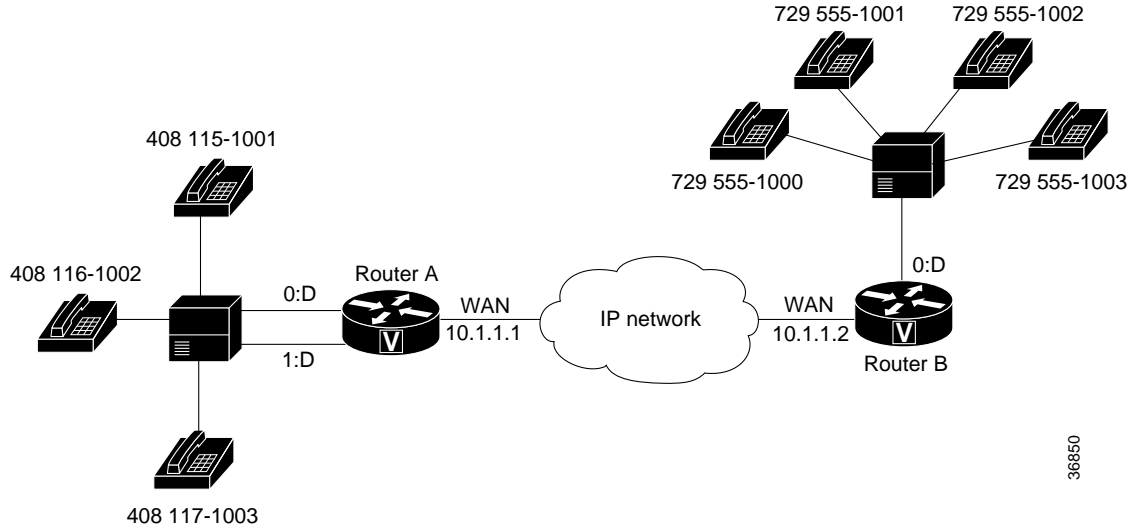
In this example, every time the device receives a call for extension 2123, the dialed digits will be replaced with 555-6611 and the call will be forwarded to that telephone.

Before you configure the **num-exp** command, it is helpful to map individual telephone extensions to their full E.164 dialed numbers. This task can be done easily by creating a number expansion table.

**Creating a Number Expansion Table**

Figure 10 shows a network for a small company that wants to use VoIP to integrate its telephony network with its existing IP network. The destination patterns (or expanded telephone numbers) associated with Router A are 408 115-xxxx, 408 116-xxxx, and 408 117-xxxx, where xxxx identifies the individual dial peers by extension. The destination pattern (or expanded telephone number) associated with Router B is 729 555-xxxx.

**Figure 10** VoIP Example for Number Expansion



36850

Table 5 shows the number expansion table for this scenario. The information included in this example must be configured on both Router A and Router B.

**Table 5** Sample Number Expansion Table

Extension	Destination Pattern	Num-Exp Command Entry
5 . . . .	408115 . . . .	num-exp 5 . . . . 408115 . . . .
6 . . . .	408116 . . . .	num-exp 6 . . . . 408116 . . . .
7 . . . .	408117 . . . .	num-exp 7 . . . . 408117 . . . .
1 . . .	729555 . . . .	num-exp 1 . . . 729555 . . . .

The period (.) character represents wildcards (such as extension numbers) in a telephone number.

### Configuring Number Expansion

The purpose of this task is to expand an extension number into its full telephone number.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **num-exp** *extension-number expanded-number*

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>num-exp extension-number expanded-number</pre> <p><b>Example:</b> Router(config)# num-exp 2123 5556611</p>	Configures number expansion globally for all dial peers. The arguments are as follows: <ul style="list-style-type: none"> <li>• <i>extension-number</i>—Specifies the extension number to expand into the full telephone number that is specified by the <i>expanded-number</i> argument.</li> <li>• <i>expanded-number</i>—Specifies the full telephone number or destination pattern to which the extension number is expanded.</li> </ul>

## Translation Rules

Digit translation rules are used to manipulate the calling number (ANI) or called number (DNIS) digits for a voice call, or to change the numbering type of a call. Translation rules are used to convert a telephone number into a different number before the call is matched to an inbound dial peer or before the call is forwarded by the outbound dial peer. For example, within your company you may dial a 5-digit extension to reach an employee at another site. If the call is routed through the PSTN to reach the other site, the originating gateway must use translation rules to convert the 5-digit extension into the 10-digit format that is recognized by the central office switch.

Translation rules are defined by using the **translation-rule** command. After you define a set of translation rules, you can apply the rules to all inbound VoIP calls, to all inbound calls that terminate at a specific voice port, and to individual inbound or outbound call legs according to the dial peer.

The following example shows a dial peer that is configured to use translation-rule set 1, which contains ten translation rules. The first rule defined is rule 0, in which 910 is the pattern that must be matched and replaced, and 0 is the pattern that is substituted for 910.

```

translation-rule 1
  rule 0 ^910 0
  rule 1 ^911 1
  rule 2 ^912 2
  rule 3 ^913 3
  rule 4 ^914 4
  rule 5 ^915 5
  rule 6 ^916 6
  rule 7 ^917 7
  rule 8 ^918 8
  rule 9 ^919 9
!
!
dial-peer voice 2 voip
  destination-pattern 91.....
  translate-outgoing called 1
  session target ras

```

The configuration results in the stripping of the leading digits 91 from any called number that begins with 91 before the number is forwarded by the outbound VoIP dial peer. Use the caret (^) symbol to specify that the matched digits must occur at the start of a dial string.

**Note**

Wildcard symbols such as the period (.), asterisk (\*), percent sign (%), plus sign (+), and question mark (?) are not valid in translation rules. The router ignores these symbols when converting a number if they are used in a translation rule.

Translation rules can also be used to change the numbering type for a call. For example, some gateways may tag any number with more than 11 digits as an international number, even when the user must dial a 9 to reach an outside line. The following example shows a translation rule that converts any called number that starts with 91, and that is tagged as an international number, into a national number without the 9 before sending it to the PSTN:

```

translation-rule 20
  rule 1 91 1 international national
!
!
dial-peer voice 10 pots
  destination-pattern 91.....
  translate-outgoing called 20
  port 1:D
!

```

**Note**

Using digit translation rules with the **num-exp** or **prefix** command is not recommended unless it is the only way to minimize confusion.

To create digit translation rules, perform the tasks in the following sections:

- [Creating Digit Translation Rules](#) (required)

To apply digit translation rules to VoIP calls, perform one or more of the following procedures:

- [Applying Translation Rules to Inbound POTS Calls](#) (optional)
- [Applying Translation Rules to Inbound VoIP Calls](#) (optional)
- [Applying Translation Rules to Outbound Call Legs](#) (optional)

### Creating Digit Translation Rules

The purpose of this task is to enter translation-rule configuration mode and specify a set of translation rules.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **translation-rule** *name-tag*
4. **rule** *name-tag input-matched-pattern substituted-pattern* [*match-type substituted-type*]

#### DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>translation-rule name-tag</code>  <b>Example:</b> Router(config)# translation-rule 1	Defines a digit translation-rule set and enters translation-rule configuration mode. All subsequent commands that you enter in this mode before you exit will apply to this translation-rule set. <ul style="list-style-type: none"> <li>• The <i>name-tag argument specifies</i> a unique number that identifies the set of translation rules. Valid entries are from 1 to 2147483647.</li> </ul>

	Command	Purpose
Step 4	<pre>rule name-tag input-matched-pattern substituted-pattern [match-type substituted-type]</pre> <p><b>Example:</b> Router(config-translate)# rule 0 ^910 0</p>	<p>Defines an individual translation rule. This command can be entered up to 11 times to add an individual translation rule to the translation rule set defined in Step 1. The arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <i>name-tag</i>—Specifies a unique number that identifies this individual translation rule. Valid entries are from 0 to 10.</li> <li>• <i>input-matched-pattern</i>—Specifies the digit string that must be matched, and then replaced with the <i>substituted-pattern</i> value.</li> <li>• <i>substituted-pattern</i>—Specifies the digit string that replaces the <i>input-matched-pattern</i> value.</li> <li>• <i>match-type</i>—(Optional) Specifies the numbering type that you want to replace with the numbering type defined in the <i>substituted-type</i> value. Enter <b>any</b> for the <i>match type</i> if you want to match on any numbering type.</li> <li>• Otherwise, enter one of the following keywords for each of these arguments: <ul style="list-style-type: none"> <li>– <b>abbreviated</b></li> <li>– <b>international</b></li> <li>– <b>national</b></li> <li>– <b>network</b></li> <li>– <b>reserved</b></li> <li>– <b>subscriber</b></li> <li>– <b>unknown</b></li> </ul> </li> </ul>

To create additional individual translation rules to include in the translation-rule set, repeat [Step 4](#).



**Note**

Applying translation rules to more than one call leg in an end-to-end call is not recommended.

### Applying Translation Rules to Inbound POTS Calls

The purpose of this task is to apply a translation rule set to all inbound POTS calls that terminate on the same voice port.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *location*
4. **translate** { **called** | **calling** } *name-tag*

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	<p>Enters privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<pre>voice-port location</pre> <p><b>Example:</b> Router(config)# voice-port 1/0:1</p>	<p>Specifies the voice port through which the call enters the router.</p> <p>The <b>voice-port</b> command syntax is platform-specific. For more information about the syntax of this command, refer to the <i>Voice Port Configuration Guide</i>.</p>
Step 4	<pre>translate {called   calling} name-tag</pre> <p><b>Example:</b> Router(config-voiceport)# translate called 4</p>	<p>Specifies the translation rule set to apply to the called number or calling number. The keywords and argument are as follows:</p> <ul style="list-style-type: none"> <li><b>called</b>—Applies the translation rule to the called party number.</li> <li><b>calling</b>—Applies the translation rule to the calling party number.</li> <li><b>name-tag</b>—Specifies the reference number of the translation rule. Valid entries are 1 through 2147483647.</li> </ul>

**Note**

When this method is used, the digit translation rules are executed before the inbound POTS dial peer is matched.

**Applying Translation Rules to Inbound VoIP Calls**

The purpose of this task is to apply a translation rule set to all inbound VoIP calls that originate at an H.323 gateway.

## SUMMARY STEPS

- enable
- configure terminal
- voip-incoming translation-rule {called | calling} name-tag

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>voip-incoming translation-rule {called   calling} name-tag</pre> <p><b>Example:</b> Router(config)# voip-incoming translation-rule called 5</p>	Specifies the translation rule set to apply to all inbound VoIP call legs that originate from an H.323 gateway. The keywords and argument are as follows: <ul style="list-style-type: none"> <li><b>called</b>—Applies the translation rule to the called party number.</li> <li><b>calling</b>—Applies the translation rule to the calling party number.</li> <li><i>name-tag</i>—Specifies the reference number of the translation rule. Valid entries are 1 through 2147483647.</li> </ul>

**Note**

When using this method, the digit translation rules are executed before the inbound VoIP dial peer is matched.

**Applying Translation Rules to Outbound Call Legs**

The purpose of this task is to apply a translation rule set to an outbound VoIP or POTS call leg.

## SUMMARY STEPS

- enable
- configure terminal
- dial-peer voice *number* {pots | voip | vofr | voatm}
- translate-outgoing {called | calling} *name-tag*

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dial-peer voice <i>number</i> {pots   voip   vofr   voatm}</b>  <b>Example:</b> Router(config)# dial-peer voice 345 pots	Enters dial-peer voice configuration mode and defines a local dial peer. <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<b>translate-outgoing {called   calling} <i>name-tag</i></b>  <b>Example:</b> Router(config-dialpeer)# translate-outgoing called 6	Specifies the translation rule set to apply to the calling number or called number. The keywords and argument are as follows: <ul style="list-style-type: none"> <li><b>called</b>—Applies the translation rule to the called party number.</li> <li><b>calling</b>—Applies the translation rule to the calling party number.</li> <li><i>name-tag</i>—Specifies the reference number of the translation rule. Valid entries are 1 through 2147483647.</li> </ul>

**Note**

Translation rules that are configured in a dial peer using the **translate-outgoing** command are not applied to inbound call legs. When two-stage dialing is used, the translation rules that are configured in the voice port using the **translate** command are applied twice: after the inbound dial peer is matched, and again after the digits are collected.

**Note**

If the **prefix** command is also configured in the dial peer, the **translate-outgoing** command is executed first.

## Data Dial Peers

In addition to standard voice-network and POTS dial peers, a newer type of dial peer has been introduced to service modem calls over POTS lines with automatic dial peer matching and priority assignment. These new dial peers are called data dial peers.

Traditionally, if a modem call came over a POTS line connected to a voice-network gateway, a procession of matching criteria was required to determine the nature of the incoming call. Only after it was determined that an incoming call was not a voice call could it then be assumed that the transmission was, in fact, a data-based modem call.

Now, however, you have the ability to specify particular dial peers as data dial peers and even assign them priority in relation to other dial peers in the system.

## Configuring Data Dial Peers

The purpose of this task is to configure a POTS dial peer to be a data dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer data *tag* pots**
4. **incoming called-number *string***

### DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>dial-peer data tag pots</pre> <p><b>Example:</b> Router(config)# dial-peer data 2001 pots</p>	Specifies a dial peer for data calls and enters dial-peer voice configuration mode. The keyword and argument are as follows: <ul style="list-style-type: none"> <li>• <i>tag</i>—Specifies the dial peer identifier. The valid range is from 1 to 2147483647.</li> </ul> <p><b>Note</b> You cannot have a data dial peer and a voice dial peer that are assigned to the same <i>tag</i> number. The <i>tag</i> must be unique for all dial peers.</p> <ul style="list-style-type: none"> <li>• <b>pots</b>—Specifies the dial peer as POTS.</li> </ul>
Step 4	<pre>incoming called-number string</pre> <p><b>Example:</b> Router(dial-peer)# incoming called-number 4085551212</p>	Specifies the incoming called number that is associated with the data dial peer. <ul style="list-style-type: none"> <li>• The <i>string</i> argument specifies the number.</li> </ul>

## Configuring a Search for Dial Peers by Type

The purpose of this task is to configure a search for dial peers by type.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer search type {data voice | voice data | none}`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>dial-peer search type {data voice   voice data   none}</code>  <b>Example:</b> Router(config)# dial-peer search type data voice	Specifies the dial-peer search functionality. The keywords are as follows: <ul style="list-style-type: none"> <li>• <b>data</b>—Searches for data dial peers.</li> <li>• <b>voice</b>—Searches for voice dial peers.</li> <li>• <b>none</b>—Searches for all dial peers with the same preference based on the input order.</li> </ul> <p><b>Note</b> The default is <b>data</b> and <b>voice</b>.</p>

## Inbound and Outbound Dial Peers

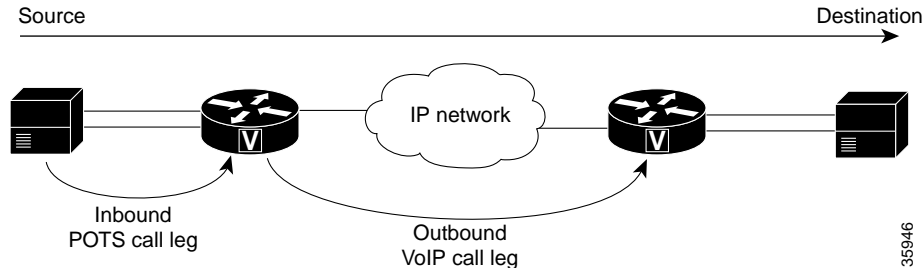
Dial peers are used for both inbound and outbound call legs. It is important to remember that these terms are defined from the perspective of the router. An inbound call leg originates when an incoming call comes *to* the router. An outbound call leg originates when an outgoing call is placed *from* the router. [Figure 11](#) illustrates call legs from the perspective of the originating router; [Figure 12](#) illustrates call legs from the perspective of the terminating router.



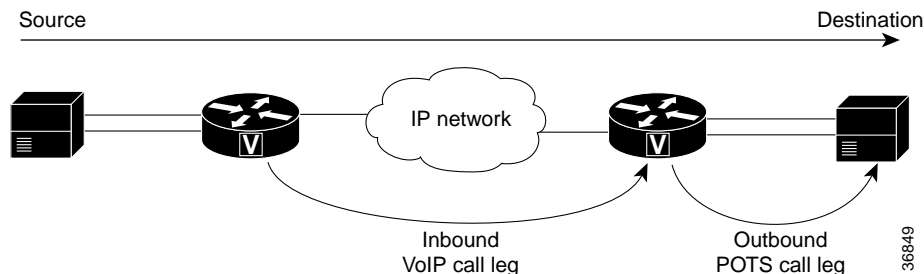
#### Note

[Figure 11](#) and [Figure 12](#) apply to voice calls that are being sent across the packet network. If the originating and terminating POTS interfaces share the same router or if the call requires hairpinning, then two POTS call legs are sufficient.

**Figure 11** Call Legs from the Perspective of the Originating Router



**Figure 12** Call Legs from the Perspective of the Terminating Router



For inbound calls from a POTS interface that are destined for the packet network, the router matches a POTS dial peer for the inbound call leg and a voice-network dial peer, such as VoIP or VoFR, for the outbound leg. For inbound calls from the packet network, the router matches a POTS dial peer to terminate the call and a voice-network dial peer to apply features such as codec or QoS.

For inbound POTS call legs going to outbound voice-network dial peers, the router forwards all digits that it collects. On outbound POTS call legs, the router strips off explicitly matching digits and forwards any excess digits out the designated port.

The following examples show basic configurations for POTS and VoIP dial peers:

```
dial-peer voice 1 pots
 destination-pattern 555....
 port 1/0:1

dial-peer voice 2 voip
 destination-pattern 555....
 session target ipv4:192.168.1.1
```

The router selects a dial peer for a call leg by matching the string that is defined by using the **answer-address**, **destination-pattern**, or **incoming called-number** command in the dial peer configuration.

## Matching Inbound Dial Peers

To match inbound call legs to dial peers, the router uses three information elements in the call setup message and four configurable dial peer attributes. The three call setup elements are:

- Called number or dialed number identification service (DNIS)—A set of numbers representing the destination, which is derived from the ISDN setup message or channel associated signaling (CAS) DNIS.

- Calling number or automatic number identification (ANI)—A set of numbers representing the origin, which is derived from the ISDN setup message or CAS ANI.
- Voice port—The voice port carrying the call.

The five configurable dial peer attributes are:

- Incoming called number—A string representing the called number or DNIS. It is configured by using the **incoming called-number** dial-peer voice configuration command in POTS or multimedia mail over IP (MMoIP) dial peers.
- Answer address—A string representing the calling number or ANI. It is configured by using the **answer-address** dial-peer voice configuration command in POTS or VoIP dial peers and is used only for inbound calls from the IP network.
- Destination pattern—A string representing the calling number or ANI. It is configured by using the **destination-pattern** dial-peer voice configuration command in POTS or voice-network dial peers.
- Application—A string representing the predefined application that you wish to enable on the dial peer. It is configured by using the **application** dial-peer voice configuration command on inbound POTS dial peers.
- Port—The voice port through which calls to this dial peer are placed.

The router selects an inbound dial peer by matching the information elements in the setup message with the dial peer attributes. The router attempts to match these items in the following order:

1. Called number with the **incoming called-number command**
2. Calling number with the **answer-address command**
3. Calling number with the **destination-pattern command**
4. Incoming voice port with the configured voice port

The router must match only one of these conditions. It is not necessary for all the attributes to be configured in the dial peer or that every attribute match the call setup information; only one condition must be met for the router to select a dial peer. The router stops searching as soon as one dial peer is matched and the call is routed according to the configured dial peer attributes. Even if there are other dial peers that would match, only the first match is used.

**Note**

For a dial peer to be matched, its administrative state must be up. The dial peer administrative state is up by default when it is configured with at least one of these commands: **incoming called-number**, **answer-address**, or **destination-pattern**. If the **destination-pattern** command is used, the voice port or session target must also be configured.

## Variable-Length Matching

When matching dial peers, the router defaults to variable-length matching, which means that as long as the left-justified digits in the dial string match the configured pattern in the dial peer, any digits beyond the configured pattern are ignored for the purposes of matching. For example, dial string 5551212 would match both of the following dial peers:

```
dial-peer voice 1 voip
 destination-pattern 555
 session target ipv4:10.10.1.1
```

```
dial-peer voice 2 voip
 destination-pattern 5551212
 session target ipv4:10.10.1.2
```

To disable variable-length matching for a dial peer, add the dollar sign (\$) to the end of the destination pattern, as shown:

```
dial-peer voice 1 voip
 destination-pattern 555$
 session target ipv4:10.10.1.1
```

The \$ character in the configuration prevents this dial peer from being matched for dial string 5551212 because the extra digits beyond 555 are considered in the matching.

With two-stage dialing, the router collects the dialed string digit by digit. It attempts to match a dial peer after each digit is received. As soon as it finds a match, it immediately routes the call. For example, given the following configurations, the router would immediately match dial string 5551212 to dial peer 1.

```
dial-peer voice 1 voip
 destination-pattern 555
 session target ipv4:10.10.1.1

dial-peer voice 2 voip
 destination-pattern 5551212
 session target ipv4:10.10.1.2
```

If the router is performing two-stage dialing and you want to make sure that the full dial string is collected before a dial peer is matched, you can use the timeout T-indicator as in variable-length dial plans. For example, after the router waits until the full dial string is collected, dial string 5551212 would match both of the following dial peers:

```
dial-peer voice 1 voip
 destination-pattern 555T
 session target ipv4:10.10.1.1

dial-peer voice 2 voip
 destination-pattern 5551212T
 session target ipv4:10.10.1.2
```

How the router selects a dial peer also depends on whether the dial peer is being matched for the inbound or outbound call leg.

## Configuring the incoming called-number Command

When a Cisco router is handling both modem and voice calls, it needs to identify the service type of the call—that is, whether the incoming call to the router is a modem or a voice call. When the router handles only modem calls, the service type identification is handled through modem pools. Modem pools associate calls with modem resources based on the called number (DNIS). In a mixed environment, where the router receives both modem and voice calls, you need to identify the service type of a call by using the **incoming called-number** command.

If the **incoming called-number** command is not configured, the router attempts to resolve whether an incoming call is a modem or voice call on the basis of the interface over which the call comes. If the call comes in over an interface associated with a modem pool, the call is assumed to be a modem call; if a call comes in over a voice port associated with a POTS dial peer, the call is assumed to be a voice call.

The purpose of this task is to identify the service type of a call as voice.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **dial-peer voice** *number* {pots | voip | vofr | voatm}
4. **incoming called-number** *number*

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice number {pots   voip   vofr   voatm}</pre> <p><b>Example:</b> Router(config)# dial-peer voice 345 pots</p>	Enters dial-peer voice configuration mode and defines a local dial peer. <ul style="list-style-type: none"> <li>• The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<pre>incoming called-number number</pre> <p><b>Example:</b> Router(config-dialpeer)# incoming called-number 5551212</p>	Defines the telephone number that identifies voice calls associated with this dial peer.

## answer-address Command

The purpose of this task is to specify the answer address for this dial peer.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* {pots | voip | vofr | voatm}
4. **answer-address** [+] *string* [T]

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	<p>Enters privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<pre>dial-peer voice number {pots   voip   vofr   voatm}</pre> <p><b>Example:</b> Router(config)# dial-peer voice 123 pots</p>	<p>Enters dial-peer voice configuration mode and defines a local dial peer.</p> <ul style="list-style-type: none"> <li>• The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<pre>answer-address [+] string [T]</pre> <p><b>Example:</b> Router(config-dialpeer)# answer-address 55534..</p>	<p>Defines the telephone number that identifies voice calls associated with this dial peer. The keywords and argument are as follows:</p> <ul style="list-style-type: none"> <li>• <b>+</b>—(Optional) Character indicating an E.164 standard number.</li> <li>• <i>string</i>—A series of digits specifying the E.164 or private dial plan telephone number. Valid entries are as follows: <ul style="list-style-type: none"> <li>– Digits 0 through 9, letters A through D, pound sign (#), and asterisk (*), which represent specific digits that can be entered.</li> <li>– Comma (,), which inserts a pause between digits.</li> <li>– Period (.), which matches any entered digit.</li> </ul> </li> <li>• <b>T</b>—(Optional) Control character indicating that the <b>answer-address</b> value is a variable-length dial string.</li> </ul>

## Configuring the destination-pattern Command

See the “[Configuring Destination Patterns](#)” section on page 4 for information on configuring the destination pattern for a dial peer.

## Configuring the port Command

See the “[Assigning Voice Ports](#)” section on page 1 for information on associating a voice port with a dial peer.

## Matching Outbound Dial Peers

The method a router uses to select an outbound dial peer depends on whether ISDN DID is configured in the inbound POTS dial peer. If DID is not configured in the inbound POTS dial peer, the router collects the incoming dialed string digit by digit. As soon as one dial peer is matched, the router immediately places the call using the configured attributes in the matching dial peer.

If DID is configured in the inbound POTS dial peer, the router uses the full incoming dial string to match the destination pattern in the outbound dial peer. With DID, the setup message contains all the digits necessary to route the call; no additional digit collection is required. If more than one dial peer matches the dial string, all of the matching dial peers are used to form a rotary group. The router attempts to place the outbound call leg using all of the dial peers in the rotary group until one is successful.

## Using Default Routes

Default routes reduce the number of dial peers that must be configured when calls that are not terminated by other dial peers are sent to a central router, usually for forwarding to a PBX. A default route is a dial peer that automatically matches any call that is not terminated by other dial peers. For example, in the following configuration, the destination pattern 8 . . . is a voice default route because all voice calls with a dialed string that starts with 8 followed by at least three additional digits will either match on 8208 or end with 8 . . . , which is the last-resort voice route used by the router if no other dial peer is matched.

```
dial-peer voice 8 pots
 destination-pattern 8208
 port 1/1
!
dial-peer voice 1000 pots
 destination-pattern 8...
 port 1/1
```

A default route could also be defined by using a single wildcard character with the timeout T-indicator in the destination pattern, as shown in the following example:

```
dial-peer voice 1000 voip
 destination-pattern .T
 session-target ipv4:10.10.1.2
```

You should be careful, however, when using the T-indicator for default routes. Remember, when matching dial peers for outbound call legs, the router places the call as soon as it finds the first matching dial peer. The router could match on this dial peer immediately even if there were another dial peer with a more explicit match and a more desirable route.

**Note**

The timeout T-indicator is appropriate only for two-stage dialing. If the router is configured for one-stage dialing, which means that DID is configured in the inbound POTS dial peer, then the timeout T-indicator is unnecessary.

# Additional Features

## One Stage and Two Stage Dialing

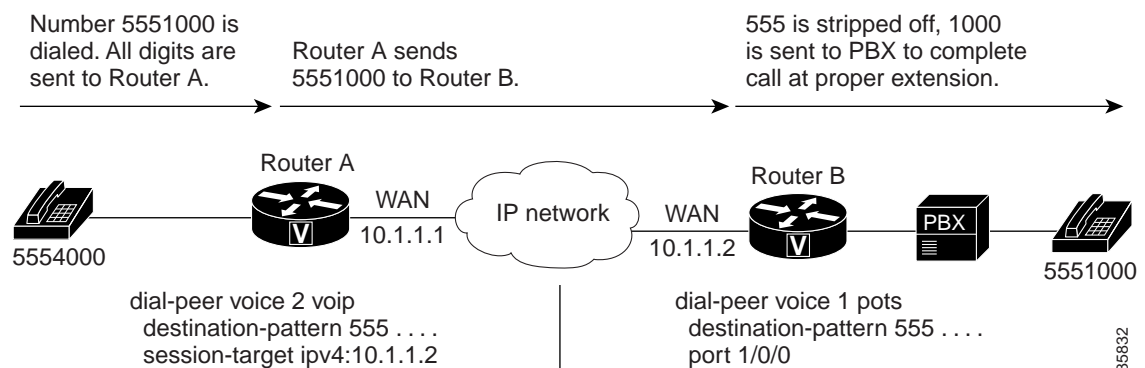
With two-stage dialing, when a voice call enters the network, the originating router collects dialed digits until it can match an outbound dial peer. As soon as the router matches a dial peer, it immediately places the call and forwards the associated dial string. No additional dialed digits are collected. The digits and wildcards that are defined in the destination pattern determine how many digits the originating router collects before matching the dial peer. Any digits dialed after the first dial peer is matched are dropped.

For example, if the dialed string is “1234599” and the originating router matches a dial peer with a destination pattern of 123 . . , then the digits “99” are not collected. The call is placed immediately after the digit “5” is dialed, and the dial string “12345” is forwarded to the next call leg.

On the terminating router, the left-justified digits that explicitly match the terminating POTS dial peer are stripped off. Any trailing wildcard digits are considered excess digits. The terminating router forwards these excess digits to the telephony interface. For example, if the dial string “1234599” is matched on a terminating router to a destination pattern of “123 . . ,” the digits “4599” are excess digits and are forwarded to the telephony interface.

Figure 13 illustrates how the originating router collects a dial string and the terminating router forwards the digits to the telephony device.

**Figure 13** Collecting and Forwarding Dialed Digits



The examples in Table 6 demonstrate how the originating router collects dialed digits for a given destination pattern in the outbound voice-network dial peer.

**Table 6** Digit Collection Based on Destination Pattern

Dialed Digits	Destination Pattern	Dial String Collected <sup>1</sup>
5551234	5 . . . . .	5551234
5551234	555 . . . .	5551234
5551234	555	555
555123499	555 . . . .	5551234

1. These examples apply only to two-stage dialing, in which the router collects the dialed string digit by digit. If DID is enabled in the inbound POTS dial peer, the router performs one-stage dialing, which means that the full dialed string is used regardless of the destination pattern that is matched.

## Direct Inward Dialing



**Note**

DID for POTS dial peers, as described here, is for ISDN connections only. It is not the same as analog DID for Cisco routers, which supports analog DID trunk service. For more information about analog DID see [Analog Direct Inward Dialing](#).

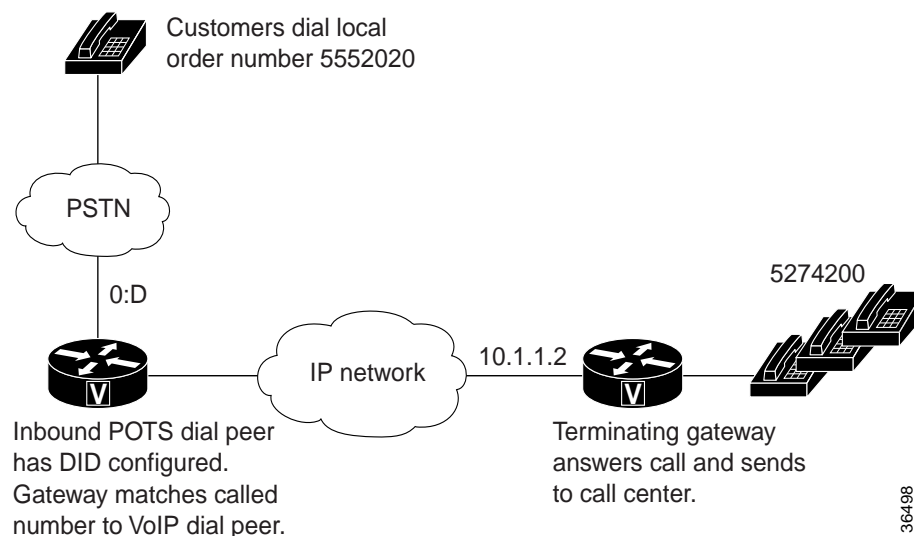
Unless otherwise configured, when a voice call comes into the router, the router presents a dial tone to the caller and collects digits until it can identify an outbound dial peer. This process is called *two-stage dialing*. After the outbound dial peer is identified, the router forwards the call through to the destination as configured in the dial peer.

The DID feature in dial peers enables the router to use the called number (DNIS) to directly match an outbound dial peer when receiving an inbound call from a POTS interface. When DID is configured on the inbound POTS dial peer, the called number (DNIS) is automatically used to match the destination pattern for the outbound call leg.

You may prefer that the router use the called number (DNIS) to find a dial peer for the outbound call leg—for example, if the switch connecting the call to the router has already collected all the dialed digits. DID enables the router to match the called number to a dial peer and then directly place the outbound call. With DID, the router does not present a dial tone to the caller and does not collect digits; it forwards the call directly to the configured destination. This is called *one-stage dialing*.

Figure 14 shows a call scenario using DID.

**Figure 14** VoIP Call Using DID



In Figure 14, the POTS dial peer that matches the incoming called-number has DID configured:

```
dial-peer voice 100 pots
  incoming called-number 5552020
  direct-inward-dial
  port 0:D
```

The **direct-inward-dial** command in the POTS dial peer tells the gateway to look for a destination pattern in a dial peer that matches the DNIS. For example, if the dialed number is 5552020, the gateway matches the following VoIP dial peer for the outbound call leg:

```
dial-peer voice 101 voip
 destination-pattern 5552020
 session target ipv4:10.1.1.2
```

The call is made across the IP network to 10.1.1.2, and a match is found in that terminating gateway:

```
dial-peer voice 555 pots
 destination-pattern 5552020
 port 0:D
 prefix 5274200
```

This dial peer matches on the dialed number and changes that number to 5274200 with the **prefix** command. The result is that the user dials a number, gets connected, and never knows that the number reached is different from the number dialed.

## Configuring Direct Inward Dialing

The purpose of this task is to configure a POTS dial peer for DID.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* pots**
4. **direct-inward-dial**

### DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice <i>number</i> pots</pre> <p><b>Example:</b> Router(config)# dial-peer voice 234 pots</p>	Enters dial-peer voice configuration mode and defines a local dial peer that will connect to the POTS network. <ul style="list-style-type: none"> <li>• The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<pre>direct-inward-dial</pre> <p><b>Example:</b> Router(config-dialpeer)# direct-inward-dial</p>	Specifies DID for this POTS dial peer.



#### Note

DID is configured for inbound POTS dial peers only.

## Hunt Groups

The router supports the concept of *hunt groups*, sometimes called *rotary groups*, in which multiple dial peers are configured with the same destination pattern. Because the destination of each POTS dial peer is a single voice port to a telephony interface, hunt groups help ensure that calls get through even when a specific voice port is busy. If the router is configured to hunt, it can forward a call to another voice port when one voice port is busy.

For example, in the following configuration for Router A, four POTS dial peers are configured with different destination patterns. Because each dial peer has a different destination pattern, no backup is available if the voice port mapped to a particular dial peer is busy with another call.

With a hunt group, if a voice port is busy, the router hunts for another voice port until it finds one that is available. In the following example for Router B, each dial peer is configured using the same destination pattern of 3000, forming a dial pool to that destination pattern.

Router A (Without Hunt Groups)	Router B (With Hunt Groups and Preferences)
<pre>dial-peer voice 1 pots  destination-pattern 3001  port 1/1 ! dial-peer voice 2 pots  destination-pattern 3002  port 1/2 ! dial-peer voice 3 pots  destination-pattern 3003  port 1/3 ! dial-peer voice 4 pots  destination-pattern 3004  port 1/4</pre>	<pre>dial-peer voice 1 pots  destination pattern 3000  port 1/1  preference 0 ! dial-peer voice 2 pots  destination pattern 3000  port 1/2  preference 1 ! dial-peer voice 3 pots  destination pattern 3000  port 1/3  preference 2 ! dial-peer voice 4 pots  destination pattern 3000  port 1/4  preference 3</pre>

To give specific dial peers in the pool a preference over other dial peers, you can configure the preference order for each dial peer by using the **preference** command. The router attempts to place a call to the dial peer with the highest preference. The configuration example given for Router B shows that all dial peers have the same destination pattern, but different preference orders.

The lower the preference number, the higher the priority. The highest priority is given to the dial peer with preference order 0. If the same preference is defined in multiple dial peers with the same destination pattern, a dial peer is selected randomly.

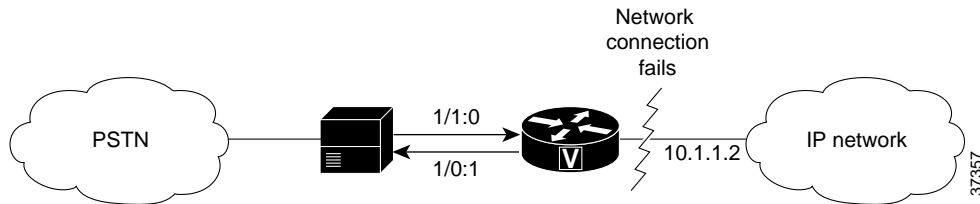
By default, dial peers in a hunt group are selected according to the following criteria, in the order listed:

1. Longest match in phone number—Destination pattern that matches the greatest number of dialed digits. For example, if one dial peer is configured with a dial string of 345 . . . and a second dial peer is configured with 3456789, the router would first select 3456789 because it has the longest explicit match of the two dial peers.
2. Explicit preference—Priority configured by using the **preference** dial peer command.
3. Random selection—All destination patterns weighted equally.

You can change this default selection order or choose different methods for hunting dial peers by using the **dial-peer hunt** global configuration command. An additional selection criterion is “least recent use,” which selects the destination pattern that has waited the longest since being selected.

You can mix POTS and voice-network dial peers when creating hunt groups. Mixing dial peer types can be useful if you want incoming calls to be sent over the packet network, except that if network connectivity fails, you want to reroute the calls back through the PBX to the PSTN. This type of configuration is sometimes referred to as *hairpinning*. Hairpinning is illustrated in [Figure 15](#).

**Figure 15** Voice Call Using Hairpinning



The following configuration shows an example of sending calls to the PSTN if the IP network fails:

```
dial-peer voice 101 voip
 destination-pattern 472....
 session target ipv4:192.168.100.1
 preference 0
!
dial-peer voice 102 pots
 destination-pattern 472....
 prefix 472
 port 1/0:1
 preference 1
```

You cannot use the same preference numbers for POTS and voice-network dial peers within a hunt group. You can set a separate preference order for each dial peer type, but the preference order does not work on both at the same time. For example, you can configure preference order 0, 1, and 2 for POTS dial peers, and you can configure preference order 0, 1, and 2 for the voice-network dial peers, but the two preference orders are separate. The system resolves preference orders among POTS dial peers first.

## Configuring Dial Peer Hunting Options

Dial peer hunting is enabled by default. The purpose of this task is to disable dial peer hunting on an individual dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* {**pots** | **vofr** | **voip** | **voatm**}
4. **huntstop**

## DETAILED STEPS

	Command	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enters privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>dial-peer voice <i>number</i> {pots   voip   vofr   voatm}</code></p> <p><b>Example:</b> Router(config)# dial-peer voice 345 pots</p>	<p>Enters dial-peer voice configuration mode and defines a local dial peer.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<p><code>huntstop</code></p> <p><b>Example:</b> Router(config-dialpeer)# huntstop</p>	<p>(Optional) Disables dial-peer hunting on the dial peer. Once you enter this command, no further hunting is allowed if a call fails on the selected dial peer.</p>

Use the **no huntstop** command to enable dial peer hunting if it has been disabled.

The purpose of this task is to configure dial peer hunting options for all dial peers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer hunt** *hunt-order-number*
4. **voice hunt** {**user-busy** | **invalid-number** | **unassigned-number**}

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

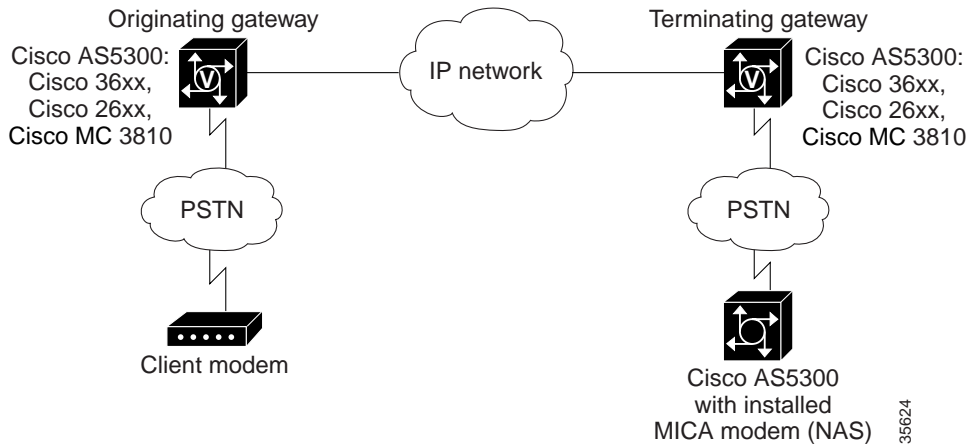
	Command	Purpose
Step 3	<p><code>dial-peer hunt hunt-order-number</code></p> <p><b>Example:</b>  Router(config)# dial-peer hunt 2</p>	<p>(Optional) Specifies the hunt selection order for dial peers in a hunt group. Valid entries are 0 through 7. The default is 0. The allowable values are as follows:</p> <ul style="list-style-type: none"> <li>• 0—Specifies longest match in phone number, explicit preference, random selection.</li> <li>• 1—Specifies longest match in phone number, explicit preference, least recent use.</li> <li>• 2—Specifies explicit preference, longest match in phone number, random selection.</li> <li>• 3—Specifies explicit preference, longest match in phone number, least recent use.</li> <li>• 4—Specifies least recent use, longest match in phone number, explicit preference.</li> <li>• 5—Specifies least recent use, explicit preference, longest match in phone number.</li> <li>• 6—Specifies random selection.</li> <li>• 7—Specifies least recent use.</li> </ul>
Step 4	<p><code>voice hunt {user-busy   invalid-number   unassigned-number}</code></p> <p><b>Example:</b>  Router(config)# voice hunt user-busy</p>	<p>(Optional) Defines how the originating or tandem router handles rotary dial peer hunting if it receives a disconnect cause code from the terminating router. The keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>user-busy</b>—<b>Instructs</b> the router to continue dial peer hunting if it receives a user-busy disconnect cause code from a destination router.</li> <li>• <b>invalid-number</b>—<b>Instructs</b> the router to stop dial peer hunting if it receives a an invalid-number disconnect cause code from a destination router.</li> <li>• <b>unassigned-number</b>—<b>Instructs</b> the router to stop dial peer hunting if it receives an unassigned-number disconnect cause code from a destination router.</li> </ul>

## Modem Pass Through

Like T.38 Fax Relay and Modem Relay, Modem Pass Through functionality can be enabled and configured on a per-dial peer basis. Modem Pass Through behavior enables you to take advantage of features such as the following:

- Repressing bandwidth- and resource-consuming functions like compression, echo cancellation, high-pass filtering, and voice activity detection (VAD).
- Automatically sending redundant packets to minimize the possibility of packet loss.
- Employing automatic static jitter buffers to protect against clock skew.
- Identifying signals that are for modem calls versus voice or fax calls.

Figure 16 illustrates a network featuring Modem Pass Through capability.

**Figure 16 Modem Pass Through Connection Example**

When a call over the network is identified as a modem call, both the originating and terminating voice gateway routers automatically “roll over” to using the G.711 codec for the duration of the modem call. Once the modem call has ceased, the digital signal processors (DSPs) in both the originating and terminating voice gateways revert to default operation, enabling fax and voice calls to be placed and received using those DSPs. The version of the G.711 codec you use (either a-law or u-law) is determined by the type of network on which your voice gateways are operating and the configuration you specify using the **modem passthrough** command in dial-peer voice configuration mode.

## Configuring Modem Pass Through Capability for Individual Dial Peers

The purpose of this task is to configure Modem Pass Through capability for individual dial peers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* {pots | vofr | voip | voatm }
4. **modem passthrough** {system | nse [payload-type *number*] codec {g711ulaw | g711alaw }[redundancy]}

### DETAILED STEPS

	Command	Description
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command	Description
Step 3	<pre>dial-peer voice number {pots   voip   vofr   voatm}</pre> <p><b>Example:</b> Router(config)# dial-peer voice 123 pots</p>	<p>Enters dial-peer voice configuration mode and defines a local dial peer.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the dial peer. Valid entries are from 1 to 2147483647.</li> </ul>
Step 4	<pre>modem passthrough {system   nse [payload-type number] codec {g711ulaw   g711alaw}[redundancy]}</pre> <p><b>Example:</b> Router(config-dialpeer)# modem passthrough codec g711ulaw</p>	<p>Configures the Modem Pass Through feature for a specific dial peer. The keywords and argument are as follows:</p> <ul style="list-style-type: none"> <li><b>system</b>—Defaults to the global configuration.</li> </ul> <p><b>Note</b> When the <b>system</b> keyword is used, the <b>nse</b>, <b>payload-type</b>, <b>codec</b>, and <b>redundancy</b> keywords are not valid. Instead, the values from the global configuration are used.</p> <ul style="list-style-type: none"> <li><b>nse</b>—Named signaling event.</li> <li><b>payload-type</b>—(Optional) NSE payload type. The <i>number</i> argument specifies the value of the payload type. Valid range is from 96 to 119, inclusive. The default value is 100.</li> </ul> <p><b>Note</b> When the payload type is 100, and you use the <b>show running-config</b> command, the <b>payload-type</b> parameter does not appear in the output.</p> <ul style="list-style-type: none"> <li><b>codec</b>—Voice compression for speech or audio signals. Codec selections for upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls, and then slow down when there is only voice traffic.</li> <li><b>g711ulaw</b>—Codec G.711 u-law 64000 bps for T1.</li> <li><b>g711alaw</b>—Codec G.711 a-law 64000 bps for E1.</li> </ul> <p><b>Note</b> Be sure to use the same codec type for both the originating gateway and the terminating gateway. The g711ulaw codec is required for T1, and the g711alaw codec is required for E1.</p> <ul style="list-style-type: none"> <li><b>redundancy</b>—(Optional) Enables packet redundancy (RFC 2198) for modem traffic.</li> <li>The default behavior for Modem Pass Through behavior in dial-peer voice configuration mode is <b>modem passthrough system</b>.</li> </ul>

## Dual Tone Multifrequency Relay

Dual tone multifrequency (DTMF) tones are generated when a button on a touch-tone phone is pressed. When the tone is generated, it is compressed, transported to the other party, and then decompressed. If a low-bandwidth codec, such as G.729 or G.723, is used without a DTMF relay method, the tone may be distorted during compression and decompression.

DTMF relay sends DTMF tones out of band, or separately from the voice stream. Cisco gateways currently support the following methods of DTMF relay:

- Using a Cisco-proprietary Real-Time Transport Protocol (RTP). DTMF tones are sent in the same RTP channel as voice data. However, the DTMF tones are encoded differently from the voice samples and are identified by a different RTP payload type code. Use of this method accurately transports DTMF tones, but because it is proprietary, it requires the use of Cisco gateways at both the originating and terminating endpoints of the H.323 call.
- Using either the H.245 signal or H.245 alphanumeric method. These methods separate DTMF digits from the voice stream and send them through the H.245 signaling channel instead of through the RTP channel. The tones are transported in H.245 User Input Indication messages. The H.245 signaling channel is a reliable channel, so the packets that transport the DTMF tones are guaranteed to be delivered. However, because of the overhead of using a reliable protocol, and depending on network congestion conditions, the DTMF tones may be slightly delayed. All H.323 version 2-compliant systems are required to support the “h245-alphanumeric” method: support of the “h245-signal” method is optional.
- Using Named Telephone Events (NTEs). Using NTE to relay DTMF tones provides a standardized means of transporting DTMF tones in RTP packets according to section 3 of *RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, developed by the IETF Audio/Video Transport (AVT) working group. RFC 2833 defines formats of NTE RTP packets used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints. With the NTE method, the endpoints perform per-call negotiation of the DTMF relay method. They also negotiate to determine the payload type value for the NTE RTP packets.

Cisco H.323 gateways advertise capabilities using the H.245 capabilities messages. By default, they advertise that they can receive all DTMF relay modes. If the capabilities of the remote gateway do not match, the Cisco H.323 gateway sends DTMF tones as in-band voice. Configuring DTMF relay on the Cisco H.323 gateway sets preferences for how the gateway handles DTMF transmission. If multiple methods are configured, the priority is as follows:

- Cisco RTP
- RTP NTE
- H.245 signal
- H.245 alphanumeric

In addition to support for NTE, DTMF Relay provides support for asymmetrical payload types. Payload types can differ between local and remote endpoints. Therefore, the Cisco gateway can transmit one payload type value and receive a different payload type value.

## Configuring DTMF Relay and Payload Type

The purpose of this task is to configure DTMF Relay capability and the respective payload type for individual dial peers.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice number {voip | vofr}`
4. `dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal]`
5. `rtp payload-type nte number`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	Router# <code>dial-peer voice number {voip   vofr}</code>  <b>Example:</b> Router(config)# <code>dial-peer voice 123 voip</code>	Enters dial-peer voice configuration mode and defines a remote VoIP dial peer. The keywords and arguments are as follows: <ul style="list-style-type: none"> <li>• The <i>number</i> argument is one or more digits that identify the dial peer. Valid entries are from 1 to 2147483647.</li> <li>• The <b>voip</b> keyword indicates a VoIP peer that uses voice encapsulation on the IP network.</li> </ul>
Step 4	<code>dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal]</code>  <b>Example:</b> Router(config-dialpeer)# <code>dtmf-relay cisco-rtp</code>	Allows DTMF relay using Cisco proprietary RTP packets. DTMF tones are encoded in the Cisco proprietary format and transported in the same RTP channel as the voice.

	Command	Purpose
Step 5	<pre>rtp payload-type nte number</pre> <p><b>Example:</b>  Router(config-dialpeer)# <b>rtp payload-type nte 100</b></p>	<p>Identifies the payload type of an RTP packet.</p> <ul style="list-style-type: none"> <li>The <b>nte</b> keyword identifies the payload type as an NTE. Number values are 96 through 127. The default value is 101.</li> <li>The following numbers have preassigned values: <ul style="list-style-type: none"> <li>– 96</li> <li>– 97</li> <li>– 100</li> <li>– 121 to 123</li> <li>– 125 to 127</li> </ul> </li> <li>If you use these values for the NTE payload type, the command fails. You must first reassign the value in use to a different unassigned number, for example: <pre>rtp payload-type nse 105 rtp payload-type nte 100</pre> </li> </ul>

## Connection PLAR

You can configure dial peers on your Cisco voice gateway router to take advantage of one-way and two-way private-line automatic ringdown (PLAR) functionality. By using the **connection plar** command you can enhance your voice network to offer a number of useful features including the following:

- Providing an off-premises extension (OPX) from a PBX, thus simulating direct connections between FXS port users on a voice gateway router and the PBX.
- Providing dial-tone from a remote PBX in order to offer toll-bypass functionality. Instead of relying on the gateway routers in your voice network to provide dial-tone, you can employ PLAR behavior to enable remote sites to behave as though they have a direct connection to a PBX.
- Connection PLAR behavior eliminates the need for user dialing, because both of the endpoints for the VoIP call are statically configured.

In addition to the features described, connection PLAR behavior does not dedicate bandwidth to a call unless one or the other of the privately associated endpoints goes off-hook.



### Note

The Connection PLAR and Connection Trunk feature behavior is configured on a per-voice-port basis. Therefore, you cannot employ the same voice port for both Connection PLAR or trunk mode and collect-dialed-digits mode.

## Configuring Connection PLAR

The purpose of this task is to enable Connection PLAR on the specified dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **voice-port** *port-number*
4. **connection plar** *number*
5. **exit**
6. **dial-peer voice** *number* {**voip** | **pots**}
7. **port** *port-number*

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice-port</b> <i>port-number</i>  <b>Example:</b> Router(config)# voice-port 1/0/0	Enters voice-port configuration mode for the voice port specified.
Step 4	<b>connection plar</b> <i>number</i>  <b>Example:</b> Router(config-voiceport)# connection plar 51234	Configures the specified voice port to use the Connection PLAR feature to automatically dial the specified digits.
Step 5	<b>exit</b>  <b>Example:</b> Router(config-voiceport)# exit	Returns to global configuration mode.
Step 6	<b>dial-peer voice</b> <i>number</i> { <b>voip</b>   <b>pots</b> }	Enters dial-peer voice configuration mode to configure a VoIP or POTS dial peer.
Step 7	<b>port</b> <i>port-number</i>  <b>Example:</b> Router(config-dial-peer)# port 1/0/0	Configures the dial peer from the previous step to contact the VoIP network using the specified voice port.

## Connection PLAR Design Considerations

Take the following items into consideration when planning to configure Connection PLAR behavior on your VoIP network:

- Because Connection PLAR is a switched VoIP call (similar to a switched virtual circuit), calls are set up and torn down as needed—bandwidth is taken up only when a call is initiated.

- Connection PLAR will operate between any types of signaling endpoints—E&M, FXO, and FXS—and between any combination of analog and digital interfaces.
- Connection PLAR does not collect digits from the connected telephony device, so you can configure Connection PLAR without any subsequent changes to your dial plan.
- Connection PLAR can be enabled on one or both of the statically configured endpoints, thus allowing you the ability to use one-way or two-way Connection PLAR.

**Note**

---

Because automatically forwarded digits can become distorted over the compressed VoIP audio path when low bit rate codecs like G.729 and G.723.1 are used, you can use the **dtmf relay** command to transport dual tone multifrequency (DTMF) tones out-of-band (separate from the compressed VoIP audio path) to avoid this potential problem. For more information regarding DTMF relay configuration, refer to [“Dual Tone Multifrequency Relay” section on page 38](#).

---

## Connection Trunk

In addition to configuring Connection PLAR, you can configure your dial peers to employ the Connection Trunk feature using the **connection trunk** command. Connection Trunk functionality offers some of the same advantages as Connection PLAR, such as eliminating the need for user dialing because both of the endpoints for the VoIP call are statically configured. In addition, Connection Trunk behavior offers you the ability to pass supplemental call signaling capability like hookflash and point-to-point Hoot-n-Holler between endpoints on the trunk.

However, unlike Connection PLAR, Connection Trunk endpoints are always active (or off-hook) as far as the voice network is concerned, so bandwidth is always being allocated to a trunk that you have configured.

**Note**

---

The Connection PLAR and Connection Trunk feature behavior is configured on a per-voice-port basis. Therefore, you cannot employ the same voice port for both Connection PLAR or trunk mode and collect-dialed-digits mode.

---

## Configuring Connection Trunk

The purpose of this task is to enable Connection Trunk behavior on the specified dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port-number*
4. **connection trunk** *number*
5. **exit**
6. **dial-peer voice** *number* {**voip** | **pots**}
7. **port** *port-number*

## DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice-port port-number</code>  <b>Example:</b> Router(config)# voice-port 1/0/0	Enters voice-port configuration mode for the voice port specified.
Step 4	<code>connection trunk number</code>  <b>Example:</b> Router(config-voiceport)# connection trunk 51234	Configures the specified voice port to use the Connection Trunk feature to automatically dial the specified digits.
Step 5	<code>exit</code>  <b>Example:</b> Router(config-voiceport)# exit	Returns to global configuration mode.
Step 6	<code>dial-peer voice number {voip   pots}</code>  <b>Example:</b> Router(config)# dial-peer voice 123 voip	Enters dial-peer configuration mode to configure a VoIP or POTS dial peer.
Step 7	<code>port port-number</code>  <b>Example:</b> Router(config-dial-peer)# port 1/0/0	Configures the dial peer from the previous step to contact the VoIP network using the specified voice port.

**Note**

Because automatically forwarded digits can become distorted over the compressed VoIP audio path when low bit rate codecs like G.729 and G.723.1 are used, you can use the **dtmf relay** command to transport DTMF tones out-of-band (separate from the compressed VoIP audio path) to avoid this potential problem. For more information regarding DTMF relay configuration, refer to [“Dual Tone Multifrequency Relay”](#) section on page 38.

## Class of Restrictions

The Class of Restrictions (COR) feature provides the ability to deny certain call attempts based on the incoming and outgoing class of restrictions provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, to 900 numbers), and applies different restrictions to call attempts from different originators.

COR is used to specify which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list. The incoming COR list indicates the capability of the dial peer to initiate certain classes of calls. The outgoing COR list indicates the capability required for an incoming dial peer to deliver a call via this outgoing dial peer. If the capabilities of the incoming dial peer are not the same or a superset of the capabilities required by the outgoing dial peer, the call cannot be completed using this outgoing dial peer.

A typical application of COR is to define a COR name for the number that an outgoing dial peer serves, then define a list that contains only that COR name, and assign that list as **corlist outgoing** for this outgoing dial peer. For example, dial peer with destination pattern 5T can have a **corlist outgoing** that contains COR 5x, as shown in the following configuration.

The next step, in the typical application, is to determine how many call permission groups are needed, and define a COR list for each group. For example, group A is allowed to call 5x and 6x, and group B is allowed to call 5x, 6x, and 1900x. Then, for each incoming dial peer, we can assign a group for it, which defines what number an incoming dial peer can call. Assigning a group means assigning a **corlist incoming** to this incoming dial peer.

```
dial-peer cor custom
  name 5x
  name 6x
  name 1900x
!
dial-peer cor list listA
  member 5x
  member 6x
!
dial-peer cor list listB
  member 5x
  member 6x
  member 1900x
!
dial-peer cor list list5x
  member 5x
!
dial-peer cor list list6x
  member 6x
!
dial-peer cor list list1900x
  member 1900x

! outgoing dialpeer 100, 200, 300
dial-peer voice 100 pots
  destination-pattern 5T
  corlist outgoing list5x
dial-peer voice 200 pots
  destination-pattern 6T
  corlist outgoing list6x
dial-peer voice 300 pots
  destination-pattern 1900T
  corlist outgoing list1900x
!
! incoming dialpeer 400, 500
dial-peer voice 400 pots
  answer-address 525...
  corlist incoming listA
dial-peer voice 500 pots
  answer-address 526
  corlist incoming listB
```

## Configuring Classes of Restrictions

To configure classes of restrictions for dial peers, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>dial-peer cor custom</b>	Enters COR configuration mode to specify that named class of restrictions apply to dial peers.
<b>Step 2</b>	Router(config-dp-cor)# <b>name class-name</b>	Specifies a name for a custom class of restrictions.  <b>Note</b> Enter the <b>name</b> (dial-peer cor custom) command for additional class names, as needed. You can define a maximum of 64 COR names. These class names are used to define the COR lists configured in Step 4 and Step 5.
<b>Step 3</b>	Router(config-dp-cor)# <b>exit</b>	Exits COR configuration mode.
<b>Step 4</b>	Router(config)# <b>dial-peer cor list list-name</b>	Defines a COR list name.
<b>Step 5</b>	Router(config-dp-corlist)# <b>member class-name</b>	Adds a COR class to this list of restrictions.  The member is a class named in Step 2.  <b>Note</b> Enter the <b>dial-peer cor list</b> command and <b>member</b> (dial-peer cor list) command (Step 4 and Step 5) to define another list and its membership, as needed.
<b>Step 6</b>	Router(config-dp-corlist)# <b>exit</b>	Exits COR-list configuration mode.
<b>Step 7</b>	Router(config)# <b>dial-peer voice number {pots   voip}</b>	Enters dial-peer configuration mode and defines a dial peer.
<b>Step 8</b>	Router(config-dial-peer)# <b>corlist incoming cor-list-name</b>	Specifies the COR list to be used when this is the incoming dial peer.
<b>Step 9</b>	Router(config-dial-peer)# <b>corlist outgoing cor-list-name</b>	Specifies the COR list to be used when this is the outgoing dial peer.  <b>Note</b> Repeat Step 7 through Step 9 for additional dial peers, as needed.

## Verifying Classes of Restrictions

To check the validity of your classes of restrictions configuration, perform the following tasks:

- Enter the **show dial-peer voice** command to learn whether the COR list fields are set as desired on a dial peer:

```
Router# show dial-peer voice 210
```

```
VoiceEncapPeer210
  information type = voice,
  tag = 210, destination-pattern = `221',
  answer-address = `', preference=0,
  numbering Type = `unknown'
  group = 210, Admin state is up, Operation state is up,
  incoming called-number = `221', connections/maximum = 4/unlimited,
  DTMF Relay = disabled,
  Modem = system passthrough ,
  huntstop = disabled,
```

```

application associated:
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
type = pots, prefix = `221',
forward-digits default
session-target = `', voice-port = `1/0/8:D',
direct-inward-dial = enabled,
digit_strip = enabled,

```

- Enter the **show dial-peer cor** command to display the COR names and lists you defined:

```
Router# show dial-peer cor
```

```

Class of Restriction
name:900block
name:800_call
name:Catchall

```

```

COR list <list1>
member:900block
member:800_call

```

```

COR list <list2>
member:900block

```

```

COR list <list3>
member:900block
member:800_call
member:Catchall

```

## Configuring an iLBC Codec

This section includes the following tasks:

- [Configuring an iLBC Codec on a Dial Peer, page 46](#)
- [Configuring an iLBC Codec in the Voice Class, page 48](#)

### Configuring an iLBC Codec on a Dial Peer

The internet Low Bit-rate Codec (iLBC) is intended for packet-based communication. Perform the following steps to configure the iLBC codec on a dial peer.

#### Prerequisites

iLBC is supported on the following:

- Cisco AS5350XM and Cisco AS5400XM Universal Gateways with Voice Feature Cards (VFCs)
- IP-to-IP gateways with no transcoding and conferencing.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**

4. `rtp payload-type cisco-codec-ilbc [number]`
5. `codec ilbc [mode frame_size [bytes payload_size]]`
6. `exit`

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	<p>Enters global configuration mode.</p>
Step 3	<pre>dial-peer voice tag voip</pre> <p><b>Example:</b> Router(config)# dial-peer voice 10 voip </p>	<p>Enters dial-peer configuration mode for the VoIP dial peer designated by <i>tag</i>.</p>
Step 4	<pre>rtp payload-type cisco-codec-ilbc [number]</pre> <p><b>Example:</b> Router(config-dial-peer)# rtp payload-type cisco-codec-ilbc 100 </p>	<p>Identifies the payload type of a Real-Time Transport Protocol (RTP) packet. Keyword and argument are as follows:</p> <ul style="list-style-type: none"> <li>• <b>cisco-codec-ilbc [number]</b>—Payload type is for internet Low Bit Rate Codec (iLBC). Range: 96 to 127. Default: 116.</li> </ul> <p><b>Note</b> Do not use the following numbers because they have preassigned values: 96, 97, 100, 117, 121 to 123, and 125 to 127.</p> <p>If you use these values, the command will fail. You must first reassign the value in use to a different unassigned number, for example:</p> <pre>rtp payload-type nse 105 rtp payload-type cisco-codec-ilbc 100</pre>
Step 5	<pre>codec ilbc [mode frame_size [bytes payload_size]]</pre> <p><b>Example:</b> Router(config-dial-peer)# codec ilbc mode 30 bytes 200 </p>	<p>Specifies the voice coder rate of speech for a dial peer. Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <b>mode frame_size</b>—The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20.</li> <li>• <b>bytes payload_size</b>—Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50(default), 100, 150, and 200.</li> </ul>

	Command	Purpose
Step 6	<code>exit</code>	Exits the current mode.
	<b>Example:</b> <code>Router(config-dial-peer)# exit</code>	

### Troubleshooting Tips

You can use the following commands to check iLBC status:

- `show voice call summary`
- `show voice call status`
- `show voice dsmp stream`
- `show call active voice`
- `show call history voice`
- `show voice dsp and its extensions`
- `show dial-peer voice`
- `show voice dsp channel operational-status`

### What to Do Next

To set the codec preference, see the [Configuring Multiple Codecs](#) section in the *Cisco IOS H.323 Configuration Guide*.

## Configuring an iLBC Codec in the Voice Class

When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to VoIP dial peers. The **voice class codec** global configuration command allows you to define the voice class that contains the codec selection order. Then, use the **voice-class codec** dial-peer configuration command to apply the class to individual dial peers.

To configure an iLBC codec in the voice class for multiple-codec selection order, perform the following steps.

Follow these procedures to create a voice class. For the complete dial-peer configuration procedure, see the “[Common Practices](#)” section on page 1.

You can configure more than one voice class codec list for your network. Configure the codec lists and apply them to one or more dial peers based on which codecs (and the order) you want supported for the dial peers. Define a selection order if you want more than one codec supported for a given dial peer.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice class codec`
4. `codec preference`
5. `exit`
6. `dial-peer voice voip`

7. `voice-class codec`
8. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>voice class codec tag</pre> <p><b>Example:</b> Router(config)# voice class codec 99 </p>	<p>Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. The argument is as follows:</p> <ul style="list-style-type: none"> <li><i>tag</i>—Unique identifier on the router. Range: 1 to 10000.</li> </ul>
Step 4	<pre>codec preference value ilbc [mode frame_size] [bytes payload_size]</pre> <p><b>Example:</b> Router(config-voice-class)# codec preference 1 ilbc 30 200 </p>	<p>Specifies a list of preferred codecs to use on a dial peer. Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>value</i>—Order of preference, with 1 being the most preferred and 14 being the least preferred.</li> <li><i>mode frame_size</i>—The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20.</li> <li><i>bytes payload_size</i>—Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50(default), 100, 150, and 200.</li> </ul>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-voice-class)# exit </p>	Exits the current mode.
Step 6	<pre>dial-peer voice tag voip</pre> <p><b>Example:</b> Router(config)# dial-peer voice 16 voip </p>	Enters dial-peer configuration mode for the specified VoIP dial peer.

	Command or Action	Purpose
Step 7	<pre>voice-class codec tag</pre> <p><b>Example:</b> Router(config-dial-peer)# voice-class codec 99 </p>	<p>Assigns a previously configured codec selection preference list (the codec voice class that you defined in step 3) to the specified VoIP dial peer.</p> <p><b>Note</b> The <b>voice-class codec</b> command in dial-peer configuration mode contains a hyphen. The <b>voice class</b> command in global configuration mode does not contain a hyphen.</p>
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit </p>	<p>Exits the current mode.</p>

## Where to Go for Dial Peer Troubleshooting Information

Dial peer troubleshooting consists of a vast array of techniques applicable to a variety of dial peer configuration practices. This document does not cover the techniques necessary to effectively troubleshoot potential pitfalls relating to dial peer configuration. Instead, refer to the TAC Web Site at <http://www.cisco.com/public/support/tac/technologies.shtml>.

---

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



## Dial Peer Configuration Examples

---

This appendix contains a series of configuration examples featuring the minimum required components and critical Cisco IOS command lines extracted from voice gateway configuration files necessary to complete an endpoint-to-endpoint call. Each example is designed to focus on a specific combination of components or configuration concept essential to voice over IP (VoIP) communication. This appendix covers the following topics:

- [Two Analog Phones, page 1](#)
- [Two Fax Machines, page 4](#)
- [An Analog Phone and an IP Phone Connected over an IP Network, page 5](#)
- [Two IP Phones Connected via a Voice over Frame Relay Network, page 6](#)
- [Two IP Phones Connected via a Voice over Frame Relay Network, page 6](#)
- [Using Digit Manipulation to Overcome the Obstacle of an IP Network Failure, page 7](#)

### Two Analog Phones

The simplest and most ubiquitous implementation of dial peer configuration involves connecting two standard analog telephones over an IP network. The following two examples illustrate the minimum required configurations necessary to connect two analog phones, where they are attached to the same voice gateway router and where each phone is attached to its own voice gateway router via FXS ports installed in the voice gateway routers in question.



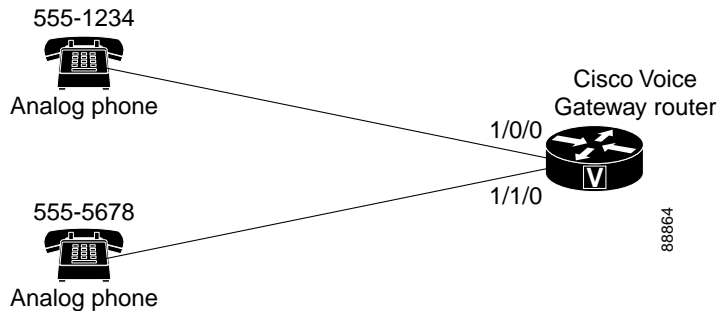
---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Both Connected to the Same Voice Gateway Router

**Figure 17** Two analog phones connected to the same voice gateway router

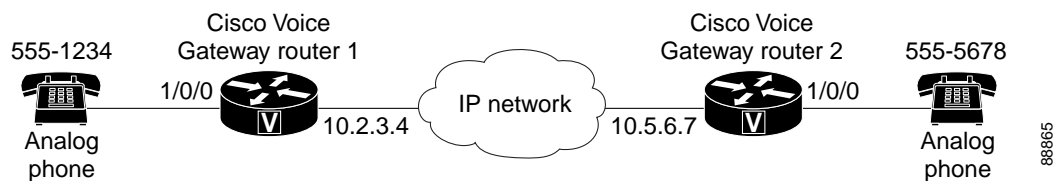


### Voice Gateway Router Configuration File

```
voice-port 1/0/0
!
voice-port 1/0/1
!
!
dial-peer voice 1 pots
 destination-pattern 5551234
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 5555678
 port 1/0/1
```

## Each Connected to Their Own Voice Gateway Router Using the G.711 Codec

**Figure 18** Two analog phones each connected to their own voice gateway router



### Voice Gateway Router 1 Configuration File

```
voice-port 1/0/0
!
dial-peer voice 1 pots
 destination-pattern 5551234
 port 1/0/0
!
dial-peer voice 10 voip
 destination-pattern 5555678
 session target ipv4:10.5.6.7
 codec g711ulaw
```

**Voice Gateway Router 2 Configuration File**

```

voice-port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 5555678
 port 1/0/0
!
dial-peer voice 20 voip
 destination-pattern 5551234
 session target ipv4:10.2.3.4
 codec g711ulaw

```

**Each Connected to Their Own Voice Gateway Routers Using the G.729r8 Codec****Voice Gateway Router 1 Configuration File**

```

voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
voice-port 1/0/0
!
voice-port 1/0/1
!
!
dial-peer voice 1 pots
 destination-pattern 5551234
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5555678
 voice-class codec 1
 session target ipv4:10.5.6.7

```

**Voice Gateway Router 2 Configuration File**

```

voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
voice-port 1/0/0
!
voice-port 1/0/1
!
!
dial-peer voice 1 pots
 destination-pattern 5555678
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5551234
 voice-class codec 1
 session target ipv4:10.2.3.4

```

# Two Fax Machines

Once the connection between two analog phones over the IP network can be set up, you can then alter the configuration slightly to enable fax communication over the IP network. [Figure 19](#) illustrates the configuration files necessary to establish T.38 Fax Relay functionality over the IP network.

**Figure 19** Two fax machines connected via T.38 Fax Relay



### Voice Gateway Router 1 Configuration File

```
interface FastEthernet0/0
 ip address 10.21.9.4 255.255.255.0
 !
voice-port 1/0/0
 !
voice-port 1/0/1
 !
dial-peer voice 1 pots
 destination-pattern 5551234
 port 1/0/0
 !
dial-peer voice 2 voip
 destination-pattern 5555678
 session target ipv4:10.5.6.7
 codec g711ulaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
 fax rate voice
```

### Voice Gateway Router 2 Configuration File

```
interface FastEthernet0/0
 ip address 10.21.7.61 255.255.255.0
 !
voice-port 1/0/0
 !
voice-port 1/0/1
 !
dial-peer voice 1 pots
 destination-pattern 5555678
 port 1/0/0
 !
dial-peer voice 2 voip
 destination-pattern 5551234
 voice-class codec 1
 session target ipv4:10.2.3.4
 codec g711ulaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
 fax rate voice
```

88896

# An Analog Phone and an IP Phone Connected over an IP Network

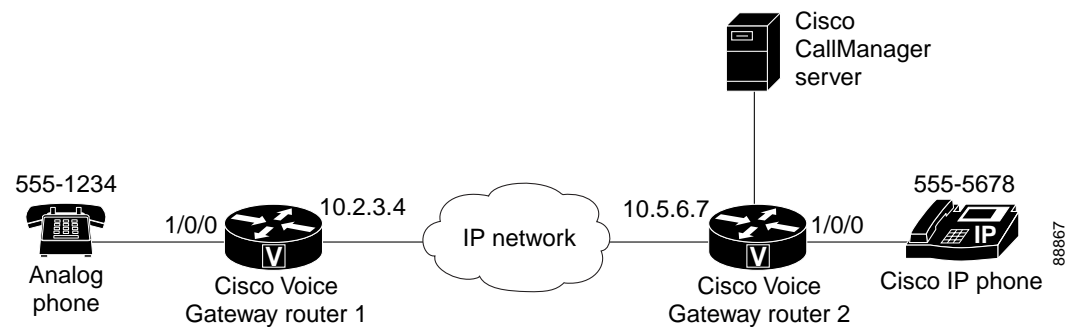
Once you are able to establish the connection of two analog phones over an IP network, you can then expand the scope of configuration coverage to include an analog phone and an IP phone connected over the IP network. The configuration for each of the voice gateway routers is essentially the same as if you were connecting two analog phones; you will need to ensure that you have allowed for a Cisco CallManager server connection to the appropriate Cisco voice gateway router to accommodate the introduction of the IP phone.



## Note

A CallManager server has been used in this configuration to manage the Cisco IP phone. However, this document does not address Cisco CallManager configuration. For more information on Cisco CallManager setup and configuration, refer to the Cisco CallManager documentation available on Cisco.com.

**Figure 20** An analog phone and an IP phone each connected to their own voice gateway router



### Voice Gateway Router 1 Configuration File

```
voice-port 1/0/0
!
dial-peer voice 1 pots
 destination-pattern 5551234
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5555678
 session target ipv4:10.5.6.7
```

### Voice Gateway Router 2 Configuration File

```
voice-port 1/0/0
!
dial-peer voice 1 pots
 destination-pattern 5555678
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5551234
 session target ipv4:10.2.3.4
```

# Two IP Phones Connected via a Voice over Frame Relay Network

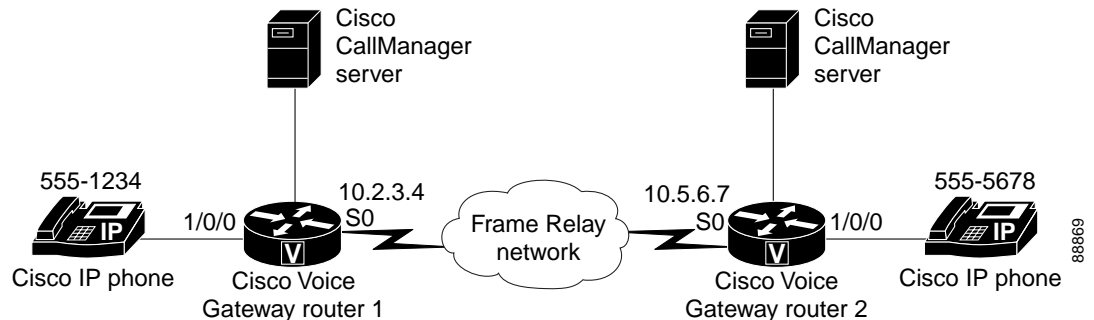
The examples thus far in this appendix have described connecting endpoints over an IP network based primarily on Ethernet connections. However, you may find that you must configure a Frame Relay WAN to effectively serve the voice communications demands for your system. [Figure 21](#) and the subsequent Cisco voice gateway router configuration examples illustrate the dial peer configuration and Frame Relay Cisco IOS commands necessary to enable Frame Relay communication across your IP network.



## Note

Although it is an essential portion of the configuration of this system, and the following configuration files contain the Cisco IOS commands necessary to establish Frame Relay connectivity, Frame Relay configuration is not addressed in this document. For more information on Frame Relay configuration, refer to the appropriate documentation available on Cisco.com.

**Figure 21** Two IP phones connected over a Frame Relay network



## Voice Gateway Router 1 Configuration File

The configuration for this voice gateway features a Cisco 3620 running Cisco IOS Release 12.2(11)T6.

```
interface Serial0/0
 ip address 10.2.1.1 255.0.0.0
 encapsulation frame-relay
 !
 voice-port 1/0/0
 !
 voice-port 1/0/1
 !
 voice-port 1/1/0
 !
 voice-port 1/1/1
 !
 dial-peer cor custom
 !
 dial-peer voice 1 pots
 destination-pattern 5551234
 port 1/0/0
 !
 dial-peer voice 1000 voip
 preference 1
 destination-pattern 5555678
 session target ipv4:10.5.6.7
```

**Voice Gateway Router 2 Configuration File**

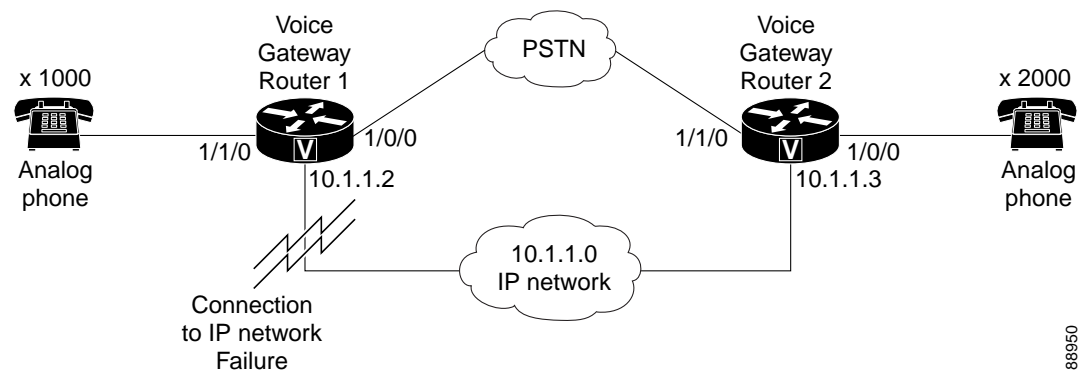
The configuration for this voice gateway features a Cisco 3620 running Cisco IOS Release 12.2(15)T.

```
interface Serial0/0
 ip address 10.2.3.4 255.0.0.0
 encapsulation frame-relay
 clockrate 2000000
 no fair-queue
 !
 voice-port 1/0/0
 !
 voice-port 1/0/1
 !
 voice-port 1/1/0
 !
 voice-port 1/1/1
 !
 dial-peer cor custom
 !
 dial-peer voice 1 pots
 destination-pattern 5555678
 port 1/0/0
 !
 dial-peer voice 2000 voip
 preference 1
 destination-pattern 5551234
 session target ipv4:10.2.3.4
```

## Using Digit Manipulation to Overcome the Obstacle of an IP Network Failure

Figure 22 and the subsequent Cisco voice gateway router configuration examples illustrate the dial peer configuration necessary to automatically route an outgoing voice call over the PSTN in the event of a temporary IP network outage. An advantage to this method of setting up and connecting the call over the PSTN (while still originating the transmission from a voice gateway router) is more commonly known as “toll bypass.”

**Figure 22** Using the PSTN in the event of an IP network failure

**Voice Gateway Router 1 Configuration File**

The configuration for this voice gateway features a Cisco 3620 running Cisco IOS Release 12.2(15)T.

88950

```

translation-rule 21
  Rule 1 ^2 5552
!
translation-rule 11
  Rule 1 ^5551 1
!
interface FastEthernet0/0
  ip address 10.1.1.2 255.255.255.0
  duplex auto
  speed auto
!
voice-port 1/0/0
  translate called 11
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer cor custom
!
dial-peer voice 1 pots
  destination-pattern 1000
  port 1/1/0
!
dial-peer voice 2000 voip
  preference 1
  destination-pattern 2000
  session target ipv4:10.1.1.3
!
dial-peer voice 20 pots
  preference 2
  destination-pattern 2000
  translate-outgoing called 21
  port 1/0/0
  forward-digits all

```

### Voice Gateway Router 2 Configuration File

The configuration for this voice gateway features a Cisco 3620 running Cisco IOS Release 12.2(11)T6.

```

translation-rule 11
  Rule 1 ^1 5551
!
translation-rule 21
  Rule 1 ^5552 2
!
interface Ethernet0/0
  ip address 10.1.1.3 255.255.255.0
  full-duplex
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
  translate called 21
!
voice-port 1/1/1
!
dial-peer cor custom
!
dial-peer voice 1 pots

```

```
destination-pattern 2000
port 1/0/0
!
dial-peer voice 1000 voip
preference 1
destination-pattern 1000
session target ipv4:10.1.1.2
!
dial-peer voice 10 pots
preference 2
destination-pattern 1000
translate-outgoing called 11
port 1/1/0
forward-digits all
```

---

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

