



Configuring AAA for Cisco Voice Gateways

Release 12.4T

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, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

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.

Configuring AAA for Cisco Voice Gateways

© 2008 Cisco Systems, Inc. All rights reserved.



About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

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 ^D or Ctrl-D 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
bold	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.
	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.
Courier font	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 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/all_release/all_mcl.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"> • Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • 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.
<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 Service Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Service 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)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<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: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
<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)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<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)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<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). Note 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 debug 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: http://www.cisco.com/go/mibs
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: http://www.rfc-editor.org/

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 Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

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.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



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

Last updated: August 6, 2008

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 logout or exit command.	<ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the enable command.	Router#	Issue the disable command or the exit command to return to user EXEC mode.	<ul style="list-style-type: none"> • Issue show and debug commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the configure terminal command.	Router(config)#	Issue the exit command or the end command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the interface command.	Router(config-if)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the line vty or line console command.	Router(config-line)#	Issue the exit command to return to global configuration mode or the end 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 reload command. Press the Break 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 continue command.	<ul style="list-style-type: none"> Run as the default operating mode when a valid image cannot be loaded. Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
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"> A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. The router was accessed using an RP auxiliary port. A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. 	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"> Inspect various states on the router, including the Cisco IOS state. Replace or roll back the configuration. Provide methods of restarting the Cisco IOS software or other processes. Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

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
help	Provides a brief description of the help feature in any command mode.
?	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.

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
h	help
lo	logout
p	ping
s	show
u or un	undebug
w	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.

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.



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
or
“Using Cisco IOS XE Software” chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:
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>
- *White Paper: Cisco IOS Reference Guide*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- 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 Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

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.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



Overview of AAA on Voice Gateways

This chapter consists of the following:

- [AAA, page 1](#)
- [AAA Requests to Multiple RADIUS Servers, page 8](#)
- [Customizing Accounting Records, page 10](#)
- [Related Features and Technologies, page 12](#)
- [Related Documents, page 13](#)

AAA

For a gateway to provide authentication and accounting services, enable and configure it to support authentication, authorization, and accounting (AAA) services. AAA enables the gateway to interact with a RADIUS security server to authenticate users (typically incoming calls) and to perform accounting services. For more information about RADIUS and AAA security services, refer to the *Cisco IOS Security Configuration Guide*.

AAA Authentication

The gateway normally uses AAA with interactive voice response (IVR) to check the legitimacy of a prospective gateway user on the basis of an account number (collected by IVR) or Automatic Number Identification (ANI). When the gateway uses AAA with IVR, the IVR application collects the user account and personal identification number (PIN) information and then passes it to the AAA interface. The AAA interface makes a RADIUS authentication request using the given information and, based on the information received from the RADIUS server, forwards either a pass message or a fail message to the IVR application.

For more information about authentication services using AAA, refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.



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

© 2007 Cisco Systems, Inc. All rights reserved.

AAA Accounting

A call leg is a discrete segment of a call connection that lies between two points in the connection. Each call made through the gateway consists of two call legs: incoming and outgoing. The RADIUS server collects basic start-stop connection accounting data or syslog accounting information during the accounting process for each call leg created on the gateway.

To collect basic start-stop connection accounting data, the gateway must be configured to support gateway-specific H.323 accounting functionality. The gateway sends accounting data to the RADIUS server in one of four ways, as is shown in the following sections:

- [Using RADIUS AV Pairs, page 2](#)
- [Appendix 1, “Using RADIUS AV Pairs”Overloading the Acct-Session-Id Field, page 5](#)
- [Using Vendor-Specific RADIUS Attributes, page 6](#)
- [Using Syslog Records, page 8](#)

Using RADIUS AV Pairs

Basic start-stop connection accounting data and standard RADIUS attributes are used where possible using standard Internet Engineering Task Force (IETF) RADIUS attribute/value (AV) pairs. [Table 1](#) shows the accounting-related IETF RADIUS attributes supported in Cisco IOS Release 12.2.

Table 1 Supported IETF RADIUS Accounting Attributes

Number	Attribute	Description
30	Called-Station-Id	Allows the network access server to send the called telephone number as part of the Access-Request packet (using Dialed Number Identification Service [DNIS] or similar technology). This attribute is only supported on ISDN and on modem calls on the Cisco AS5200 and Cisco AS5300 routers if used with ISDN PRI.
31	Calling-Station-Id	Allows the network access server to send the calling telephone number as part of the Access-Request packet (using ANI or similar technology). This attribute has the same value as the remote-addr attribute from TACACS+. This attribute is supported only on ISDN and on modem calls on the Cisco AS5200 and Cisco AS5300 routers if used with ISDN PRI.
40	Acct-Status-Type	(Accounting) Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).
41	Acct-Delay-Time	(Accounting) Indicates how many seconds the client has been trying to send a particular record.
42	Acct-Input-Octets	(Accounting) Indicates how many octets have been received from the port over the course of this service being provided.
43	Acct-Output-Octets	(Accounting) Indicates how many octets have been sent to the port in the course of delivering this service.

Table 1 Supported IETF RADIUS Accounting Attributes (continued)

Number	Attribute	Description
44	Acct-Session-Id	(Accounting) A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power cycled or the software is reloaded. To send this attribute in access-request packets, use the radius-server attribute 44 include-in-access-req command in global configuration mode.
45	Acct-Authentic	(Accounting) Indicates how the user was authenticated, whether by RADIUS, the network access server itself, or another remote authentication protocol. This attribute is set to “radius” for users authenticated by RADIUS; “remote” for TACACS+ and Kerberos; or “local” for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted.
46	Acct-Session-Time	(Accounting) Indicates how long (in seconds) the user has received service.
47	Acct-Input-Packets	(Accounting) Indicates how many packets have been received from the port over the course of this service being provided to a framed user.
48	Acct-Output-Packets	(Accounting) Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.

Table 1 Supported IETF RADIUS Accounting Attributes (continued)

Number	Attribute	Description
49	Acct-Terminate-Cause	<p>(Accounting) Reports details on why the connection was terminated. Termination causes are indicated by a numeric value as follows:</p> <ol style="list-style-type: none"> 1. User request 2. Lost carrier 3. Lost service 4. Idle timeout 5. Session timeout 6. Admin reset 7. Admin reboot 8. Port error 9. NAS error 10. NAS request 11. NAS reboot 12. Port unneeded 13. Port pre-empted 14. Port suspended 15. Service unavailable 16. Callback 17. User error 18. Host request <p>Note For attribute 49, Cisco IOS supports values 1 to 6, 9, 12, and 15 to 18.</p>
50	Acct-Multi-Session-Id	<p>(Accounting) A unique accounting identifier used to link multiple related sessions in a log file.</p> <p>Each linked session in a multilink session has a unique Acct-Session-Id value, but shares the same Acct-Multi-Session-Id.</p>
51	Acct-Link-Count	<p>(Accounting) Indicates the number of links known in a given multilink session at the time an accounting record is generated. The network access server can include this attribute in any accounting request that might have multiple links.</p>
52	Acct-Input-Gigawords	<p>Indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of the provided service.</p>

Table 1 Supported IETF RADIUS Accounting Attributes (continued)

Number	Attribute	Description
53	Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} while delivering service.
55	Event-Timestamp	<p>Records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC. To send RADIUS attribute 55 in accounting packets, use the radius-server attribute 55 include-in-acct-req command.</p> <p>Note Before the Event-Timestamp attribute can be sent in accounting packets, you <i>must</i> configure the clock on the router. (For information on setting the clock on your router, refer to the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i>.)</p> <p>To avoid configuring the clock on the router every time the router is reloaded, you can enable the clock calendar-valid command. (For information on this command, refer to the <i>Cisco IOS Configuration Fundamentals Command Reference</i>.)</p>

For complete information about RADIUS and the use of IETF-defined attributes, refer to the *Cisco IOS Security Configuration Guide*.

Overloading the Acct-Session-Id Field

Attributes that cannot be mapped to standard RADIUS attributes are packed into the Acct-Session-Id attribute field as ASCII strings separated by the “/” character. The Acct-Session-Id attribute contains the RADIUS account session ID, a unique identifier that links accounting records associated with the same login session for a user. To support additional fields, the following string format has been defined for this field:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/
<call type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

Table 2 shows the field attributes to be used with the Overloaded Acct-Session-Id method and provides a brief description of each.

Table 2 *Field Attributes in Overloaded Acct-Session-Id*

Field Attribute	Description
SESSION-ID	Specifies the standard RADIUS account session ID.
SETUP-TIME	Provides the Q.931 setup time for this connection in Network Time Protocol (NTP) format. NTP time formats are displayed as %H:%M:%S.%k %Z %tw %tn %td %Y where: <ul style="list-style-type: none"> • %H is hour (00 to 23). • %M is minutes (00 to 59). • %S is seconds (00 to 59). • %k is milliseconds (000 to 999). • %Z is time zone string. • %tw is day of week (Saturday through Sunday). • %tn is month name (January through December). • %td is day of month (01 to 31). • %Y is year including century (for example, 1998).
GATEWAY-ID	Indicates the name of the underlying gateway in the form of "gateway.domain_name."
CALL-ORIGIN	Indicates the origin of the call relative to the gateway. Possible values are originate and answer .
CALL-TYPE	Indicates call leg type. Possible values are telephony and VoIP .
CONNECTION-ID	Specifies the unique global identifier used to correlate call legs that belong to the same end-to-end call. The field consists of 4 long words (128 bits). Each long word is displayed as a hexadecimal value and is separated by a space character.
CONNECT-TIME	Provides the Q.931 connect time for this call leg, in NTP format.
DISCONNECT-TIME	Provides the Q.931 disconnect time for this call leg, in NTP format.
DISCONNECT-CAUSE	Specifies the reason a call was taken offline as defined in the Q.931 specification.
REMOTE-IP-ADDRESS	Indicates the address of the remote gateway port where the call is connected.

Because of the limited size of the Acct-Session-Id string, it is not possible to embed many information elements in it. Therefore, this feature supports only a limited set of accounting information elements.

Use the **gw-accounting h323** command to configure the overloaded session ID method of applying H.323 gateway-specific accounting.

Using Vendor-Specific RADIUS Attributes

The IETF draft standard specifies a method for communicating vendor-specific information between the network access server (NAS) and the RADIUS server by using the vendor-specific attribute (Attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes that are

not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string of the format:

```
protocol: attribute sep value *
```

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate AV pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. The full set of features available for TACACS+ authorization can also be used for RADIUS.

For complete and current information on voice-related vendor-specific RADIUS attributes, refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm

Some of the VSA fields and their ASCII values are listed in [Table 3](#). You can review the rest at the location noted above.

Table 3 VSA Fields and Their ASCII Values

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute Name	Description
26	9	23	h323-remote-address	Indicates the IP address of the remote gateway.
26	9	24	h323-conf-id	Identifies the conference ID.
26	9	25	h323-setup-time	Indicates the setup time for this connection in Coordinated Universal Time (UTC), formerly known as Greenwich Mean Time (GMT) and Zulu time.
26	9	26	h323-call-origin	Indicates the origin of the call relative to the gateway. Possible values are originating and terminating, which are equivalent to originate and answer in the Call-Origin field.
26	9	27	h323-call-type	Indicates call leg type. Possible values are telephony and VoIP .
26	9	28	h323-connect-time	Indicates the connection time for this call leg in UTC.
26	9	29	h323-disconnect-time	Indicates the time this call leg was disconnected in UTC.
26	9	30	h323-disconnect-cause	Specifies the reason a connection was taken offline per the Q.931 specification.
26	9	31	h323-voice-quality	Specifies the impairment/calculated planning impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	h323-gw-id	Indicates the name of the underlying gateway.

Use the **gw-accounting h323 vsa** command to configure the VSA method of applying H.323 gateway-specific accounting.

Using Syslog Records

The syslog accounting option exports the information elements associated with each call leg through a system log message, which can be captured by a syslog daemon on the network. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of AV pairs>
```

The syslog message fields are listed in [Table 4](#).

Table 4 Syslog Message Output Fields

Field	Description
server timestamp	The time stamp created by the server when it receives the message to log.
gateway id	The name of the gateway that emits the message.
message number	The number assigned to the message by the gateway.
message label	A string that identifies the message category.
list of AV pairs	A string consisting of <attribute name> <attribute value> pairs separated by commas.

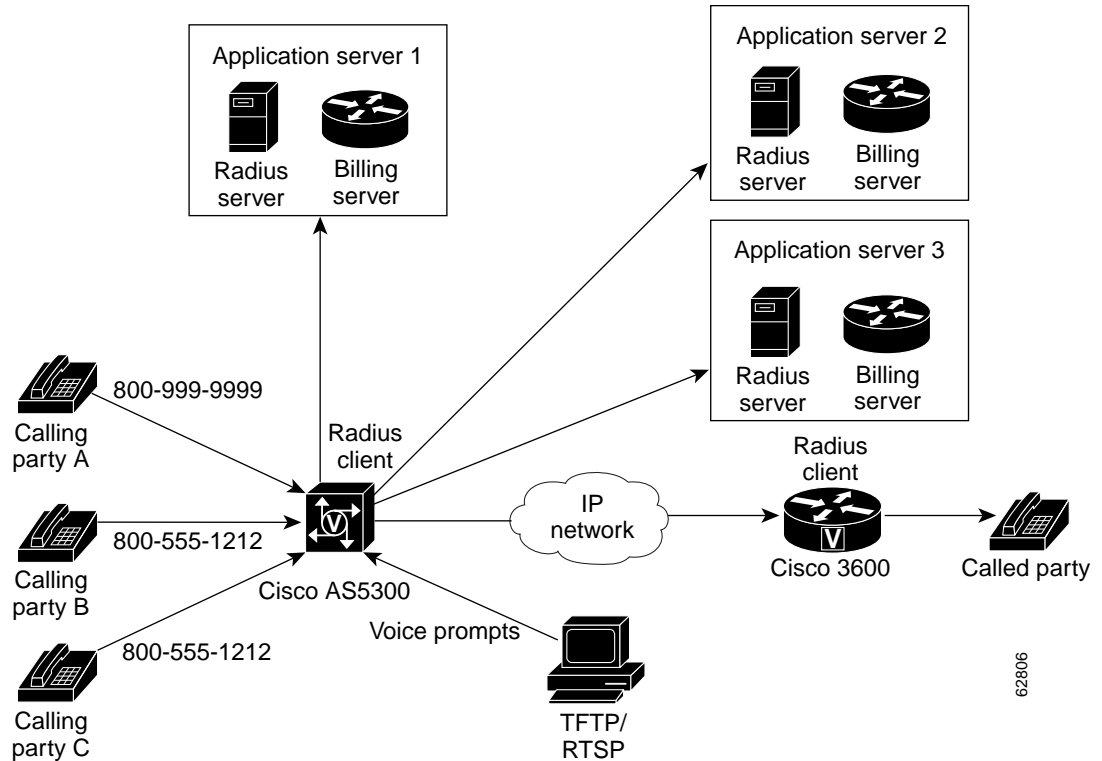
Use the **gw-accounting h323 syslog** command to configure the syslog record method of gathering H.323 accounting data.

AAA Requests to Multiple RADIUS Servers

AAA requests can be made to different RADIUS servers based on account number, called party number, and incoming trunk groups.

Consider the topology shown in [Figure 1](#) below.

Figure 1 RADIUS/Billing Selection Based on DNIS and Card Number



In [Figure 1](#), the gateway identifies the TCL IVR application to be invoked based on:

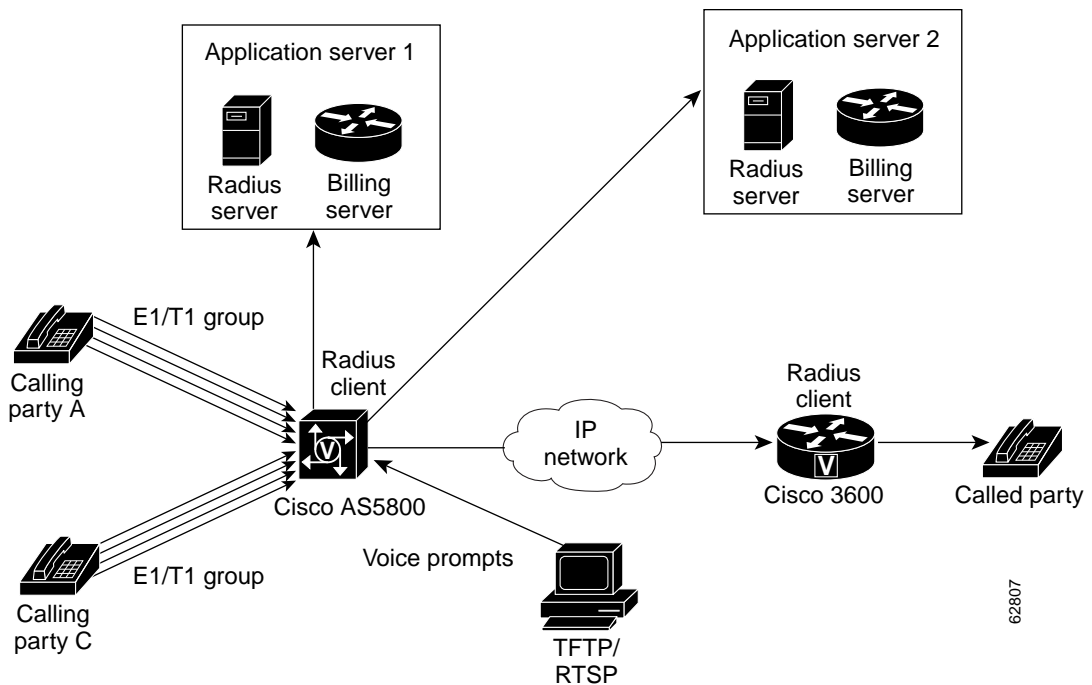
- The access number dialed by the caller, or
- The account number or card number

Calling party A has a different access number compared to calling parties B and C. Because calling parties B and C use the same access number, the service provider can use the TCL IVR script to manipulate the call and direct the AAA information to the appropriate billing/RADIUS server based on the individual card numbers entered by callers B and C. If a caller is using an account number instead of a prepaid calling card, the service provider can use the caller’s account number to direct the AAA information to the appropriate RADIUS/billing server that is used to authorize calls based on account numbers.

[Figure 2](#) below shows RADIUS/Billing server selections based on T1/E1 trunk groups. For example, if caller A is using a pre-paid application, the service provider directs AAA information to the appropriate RADIUS/Billing server based on the T1/E1 trunk group that is assigned to receive prepaid application calls.

62806

Figure 2 RADIUS/Billing Server Selection Based on T1/E1 Trunk Groups



Customizing Accounting Records

You can create an accounting template to customize your accounting records based on your billing needs. An accounting template is a text-based interface that allows you to customize and define the content of that template and helps reduce billing traffic from the gateway to the accounting servers.

A sample accounting template applicable to POTS and VoIP dial-peers is shown below.

Vendor specific attributes (VSAs) used in session applications such as h323-ivr-out, h323-credit-amount, h323-credit-time, h323-billing-model, are only controlled in the TCL script and not in the accounting template. If you specify these VSAs in the accounting template, they are ignored and no error messages are reported. You cannot control h323-conf-id and h323-incoming-conf-id; they are mandatory VSAs required for co-relating accounting messages on the incoming and outgoing legs.

Session applications also use some VSAs for authentication and authorization which are not controlled by the accounting template. For example, h323-ivr-out, h323-credit-amount, h323-credit-time, and h323-billing-model are only controlled by the TCL script. The VSAs listed in this template are voice-specific only. Non-voice specific attributes cannot be controlled through this template. To add new attributes not defined in this template, contact your Cisco marketing representative.

To delete an attribute, add the # sign in front of the attribute name.

62807

Accounting Template

You can create a custom accounting template by selecting only those VSAs that are applicable to your billing needs. The list below shows some VSAs that can be used to create custom accounting templates.

Each accounting template attribute is unique. For example, the attribute disconnect-time is applied to a stop message because you can only get that information at the end of a call and not at the start of that call.

If you want to generate individual accounting templates for different incoming trunk calls on an accounting server, you can define multiple templates and associate them with different sets of incoming dial-peers. You can customize the template by deleting attributes that are not required for your specific template.


Note

For the latest list of VSAs, refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide*.

Attribute Name	Usage and Restrictions
h323-gw-id	
h323-call-origin	
h323-call-type	
h323-setup-time	
h323-connect-time	
h323-disconnect-time	
h323-disconnect-cause	
h323-remote-address	
h323-voice-quality-subscriber	ICPIF
Detail CallHistory	
acom-level	#POTS leg only
noise-level	#POTS leg only
img-pages-count	#POTS leg only
voice-tx-duration	#POTS leg only
tx-duration	#POTS leg only
charged-units	#
disconnect-text	#

peer-if-index	#
logical-if-index	#
codec-type-rate	#
codec-bytes	#IP leg only
session-protocol	#IP leg only
vad-enable	#IP leg only
remote-udp-port	#IP leg only
hiwater-playout-display	#IP leg only
lowater-playout-display	#IP leg only
receive-delay	#IP leg only
round-trip-delay	#IP leg only
ontime-rv-playout	#IP leg only
gapfill-with-silence	#IP leg only
gapfill-with-prediction	#IP leg only
gapfill-with-interpolation	#IP leg only
gapfill-with-redundancy	#IP leg only
lost-packets	#IP leg only
early-packets	#IP leg only
late-packets	#IP leg only

Related Features and Technologies

- *Service Provider feature set for VoIP* uses the IVR for interaction with the caller; collects digits for accounting and billing purposes.
- *Authentication, Authorization, and Accounting (AAA)* feature is used in conjunction with IVR.
- *Settlement for Packet Telephony on Cisco Access Platforms* uses the TCL IVR scripts for the billing process.
- *Debit Card for Packet Telephony on Cisco Access Platforms* uses TCL IVR extensively for interoperability.

- *Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response* allows you to implement and add support for new languages and text-to-speech (TTS) notations to the core IVR infrastructure on Cisco voice gateways.

Related Documents

For related information on the features described in this document, refer to the following documents:

- *Internetworking Terms and Acronyms*
- Hardware and software guides for Cisco 5000 series universal voice gateways for information on installing the hardware and performing basic configuration
- *Platform Specific Information for Cisco 2600 Series Routers*
- *Platform Specific Information for Cisco 3600 Series Routers*
- *Voice over IP for the Cisco AS5300*, the section “VFC Management” provides VCWare download instructions
- *Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response*, Cisco IOS Release 12.2(2)T feature module, describes multi-language support for dynamic prompts
- *Configuring Debit Card Applications*, for information on debit card applications that work in conjunction with Cisco interactive voice response (IVR) software, AAA, RADIUS, and an integrated third party billing system
- *Cisco IOS Voice, Video, and Fax Configuration Library*, Cisco IOS Release 12.3
- *Cisco IOS Voice, Video, and Fax Command Reference*, Cisco IOS Release 12.3, for command reference information on Cisco IOS commands
- “Authentication, Authorization, and Accounting (AAA)” chapter in the *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.2, for information on configuring accounting records
- *RADIUS Vendor-Specific Attributes Voice Implementation Guide*
- *TCL IVR API Version 2.0 Programmer's Guide* for information about creating and implementing Tool Command Language (TCL) IVR scripts
- *Cisco Prepaid Debitcard Multi-language Programmer's Reference*
- *Enhanced Multi-Language Support for Cisco IOS Interactive Voice Response*

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.



Cisco IOS Configuration

This chapter includes the following sections:

- [Prerequisite Configuration, page 1](#)
- [Directing AAA Requests to a RADIUS Server, page 3](#)
- [Enabling and Disabling Accounting for any Call Leg, page 6](#)
- [Customizing Accounting Packets, page 7](#)

Prerequisite Configuration

The following general tasks are prerequisites to configuring the Cisco IOS features described in this document:

- Establish a working IP network. For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*.
- Configure Voice over IP. For more information about configuring Voice over IP, refer to the *Cisco IOS Voice Configuration Library*.
- Program and configure the interface between the RADIUS server and the Cisco voice gateway to operate with vendor specific attributes (VSAs). Refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide*.
- Download the TCL scripts that are not embedded in Cisco IOS from the Cisco CCO software support URL:
<http://www.cisco.com/public/sw-center/>
- Define and apply IVR applications on the dial peer to direct AAA requests to a RADIUS server. For more information, see the *Cisco IOS TCL and VoiceXML Application Guide*

Configuring AAA Basics

You must follow these steps to set up AAA before you start directing AAA requests to a RADIUS server:

Step 1 Enable authentication, authorization, and accounting (AAA) security services:

```
Router(config)# aaa new-model
```



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

© 2007 Cisco Systems, Inc. All rights reserved.

Example:

```
aaa new-model
```

Step 2 Define a RADIUS server host by entering the following command:

```
Router(config)# radius server host ipaddress auth-port port-number acct-port port-number
```

Example:

```
radius server host 1.5.35.10 auth-port 2001 acct-port 2002
```

Step 3 Use the RADIUS server defined in Step 2 to define a AAA group.

a. To define a group name, enter the following command in global configuration mode:

```
Router(config)# aaa group server radius group-name
```



Note For the argument **group-name** in the command, enter the name of the specific RADIUS server (for example server1) you want to authenticate, or enter the argument **radius** if you want to authenticate all RADIUS servers.

Example:

```
aaa group server radius server1
```

b. To configure the IP address of the RADIUS server for the group server, enter the following command in group server configuration mode:

```
Router(config-sg-radius)# server ip-address auth-port port-number acct-port port-number
```

Example:

```
server 1.5.35.10 auth-port 2001 acct-port 2002
```

Step 4 Exit group server configuration mode.

```
Router(config-sg-radius)# exit
```

Step 5 To specify the password for use between the gateway and the RADIUS server, enter the following command in global configuration mode:

```
Router(config)# radius-server key key
```

Example:

```
radius-server key luser23
```

Step 6 Use the AAA group defined in Step 2 above to define an AAA method list.

a. For voice authentication, enter the **aaa authentication login** command

a. .

```
Router(config)# aaa authentication login list-name method1 [method2...]
```

Examples:

```
aaa authentication login h323 group server2
aaa authentication login MIS-access group radius
```

b. For voice authorization, enter the **aaa authorization** command.

```
Router(config)# aaa authorization exec list-name method1 [method2...]
```

Examples:

```
aaa authorization exec h323 group server2
aaa authorization exec MIS-access group radius
```

- c. For voice accounting, enter the **aaa accounting** command in global configuration mode.

```
Router(config)# aaa accounting connection list-name start-stop method1 [method2..]
```

Example:

```
aaa accounting connection h323 start-stop group server1
```

Directing AAA Requests to a RADIUS Server

You can use TCL scripts or the CLI to direct AAA requests to a specific RADIUS server based on:

- Customer account number
- Called party number
- Trunk group

Directing AAA Requests by Using Account Numbers

It is easier to use TCL scripts instead of the CLI to direct AAA requests using account numbers.

To use TCL scripts for directing AAA requests using account numbers, follow the steps below:

-
- Step 1** Before you start using TCL scripts to direct AAA requests using account numbers, you must define and apply the interactive voice response (IVR) application on the dial peer.
- Step 2** Use the authentication, authorization, and accounting TCL verbs to customize your TCL scripts. Refer to the [Accounting Template, page 21](#) in [Chapter 1, “Overview of AAA on Voice Gateways”](#) for an example of a TCL script.

The authentication, accounting, and authorization TCL verbs are:

- a. Authentication: Use the following TCL verb:

```
aaa authenticate account password [-a avlistSend][-s servertag]
```

- b. Authorization: Use the following TCL verb:

```
aaa authorize account password ani destination {legID|info-tag} [-s servertag]
```

- c. Accounting: Use the following TCL verbs to start or update accounting messages:

```
aaa accounting start {legID|info-tag} [-s servertag]
```

- Step 3** (Optional). If you use the accounting TCL verb, then use the **accounting suppress** command to suppress accounting on the same dial peer on which you have specified your application.

Follow the steps below to suppress accounting on the dial peer:

- a. Enter the **voice class aaa** command in global configuration mode.

```
Router(config)# voice-class aaa tag
```

Example:

```
voice-class aaa 1001
```

- b. Enter the **accounting suppress** command in voice class configuration mode.

```
Router(config-class)# accounting suppress
```

- c. Enter the **voice class aaa** command in dial peer configuration mode.

```
Router(config)# dial-peer voice tag {pots|voip}  
Router(config-dial-peer)# voice class aaa tag
```

Example:

```
dial-peer voice 101 voip  
voice class aaa 1001
```

Directing AAA Requests using Called Party Number

You can use the called party number to direct AAA requests in dial peer configuration mode as follows:

Step 1 Define a dial peer.

- a. Enter dial peer configuration mode using the **dial peer voice** command. The argument **number** defines a particular dial peer.

```
Router(config)# dial-peer voice tag {pots|voip}
```

Example:

```
dial-peer voice 202 pots
```

- b. Specify the incoming called number using the **incoming called number** command in dial peer configuration mode. The argument *string* is a series of digits that specifies the incoming called number.

```
Router(config-dial-peer)# incoming called number string
```

Example:

```
incoming called number 5550900
```

Step 2 Define the voice class.

- a. Enter the **voice class aaa** command in global configuration mode. The argument *tag* identifies the dial peer.

```
Router(config)# voice class aaa tag
```

Example:

```
voice-class aaa 202
```

- b. Define authentication, authorization, and accounting methods. Enter the authentication, authorization and accounting commands in voice class mode. The argument *methodListName* is used to name the list of authentication, authorization or accounting methods applicable to each command.

```
Router(config-class)# authentication method methodListName  
Router(config-class)# accounting method methodListName  
Router(config-class)# authorization method methodListName
```

Example:

```
authentication method pw
accounting method rd
authorization method pc
```

- c. Define voice class in dial peer configuration mode. Enter dial peer configuration mode and then define the voice class in that mode. The argument **tag** identifies the same dial peer as in step a) above.

```
Router(config)# dial-peer voice tag {pots|voip}
Router(config-dial-peer)# voice-class aaa tag
```

Example:

```
dial-peer voice 202 pots
voice-class aaa 202
```

Directing AAA Requests Using Trunk Groups

To direct AAA requests using trunk groups, a trunk group must first associate with a dial peer. To use this method, group all the interfaces using one trunk group and define only one dial peer instead of individual ports for the interfaces using that trunk group.

You can direct AAA requests using trunk groups in dial-peer configuration mode as follows:

- Step 1** Define the trunk group by entering the **trunk group** command in global configuration mode. The argument *tag* is a number.

```
Router(config)# trunk group tag
```

Example:

```
trunk group 303
```

- Step 2** Use the trunk group tag in Step 1 to group the interfaces.
 - a. Enter the **interface serial** command in global configuration mode to specify a serial interface on the channelized T1 or E1 controller. The argument *slot/port* denotes the slot and port number where the channelized T1 or E1 controller is located. The argument *timeslot* denotes the ISDN D channel timeslot which is 15 for channelized E1 and 23 for channelized T1.

```
Router(config)# interface serial slot/port: timeslot
```

Example:

```
interface serial 1/1:23
```

- b.** Enter the **trunk group** command.

```
Router(config-inter-serial)# trunk group tag
```

Example:

```
trunk group 303
```

- Step 3** Use the *tag* defined in Step 2b) above.

- a.** Enter the **voice class aaa** command in global configuration mode.

```
Router(config)# voice-class aaa tag
```

Example:

```
voice-class aaa 303
```

- b. Define authentication, accounting, and authorization methods. Enter the **authentication method**, **accounting method**, and **authorization method** commands in voice class mode. The argument *methodListName* is used to name the list of authentication, accounting, or authorization methods applicable to each command.

```
Router(config-class)# authentication method methodListName
Router(config-class)# accounting method methodListName
Router(config-class)# authorization method methodListName
```

Example:

```
authentication method ab
accounting method cd
authorization method ef
```

- c. Enter dial peer configuration mode using the **dial peer voice** command.

```
Router(config)# dial-peer voice tag {pots|voip}
```

Example:

```
dial-peer voice 303 pots
```

- d. Define the voice class in dial peer configuration mode. The argument *tag* identifies the same dial peer as in Step a above.

```
Router(config-dial-peer)# voice-class aaa tag
```

Example:

```
voice-class aaa 303
```

- e. Define the trunk group in dial peer configuration mode. The argument *tag* is the the same number as in Step b) above.

```
Router(config-dial-peer)# trunk group tag
```

Example:

```
trunk group 303
```

Enabling and Disabling Accounting for any Call Leg

Enabling voice accounting by using the **gw-accounting aaa** command will send only the default list of VSAs to the accounting server.

Global Configuration Mode

To enable and disable accounting for any call leg in global configuration mode, follow these steps:

- Step 1** To enable accounting for any call leg, enter the **gw-accounting aaa** command in global configuration mode. Use the no form of the command to disable accounting.

```
Router (config)# gw-accounting aaa
Router (config)# no gw-accounting aaa
```

To disable accounting based on the type of dial peer, use the following command:

Step 2 To disable accounting based on the type of dial peer, use the following commands:

- a. Enter the **gw-accounting aaa** command.

```
Router(config)# gw-accounting aaa
```

- b. Enter the **suppress** command.

```
Router(config-gw-accounting-aaa)# suppress
```

You have a choice of entering **pots** or **voip**, based on the type of dial peer.

- c. Enter the **suppress pots** or **suppress voip** command.

```
Router(config-gw-accounting-aaa)# suppress pots
```

or

```
Router(config-gw-accounting-aaa)# suppress voip
```

dial-peer configuration mode

To disable accounting in dial-peer configuration mode, follow these steps:

Step 1 Enter the **voice class aaa** command in global configuration mode.

```
Router(config)# voice class aaa tag
```

Example:

```
voice-class aaa 303
```

Step 2 Enter the **accounting suppress** command in voice class aaa mode.

```
Router(config-class)# accounting suppress [in-bound|out-bound]
```

Example:

```
accounting suppress
```

Step 3 Enter the **voice class aaa** command in dial peer configuration mode.

```
Router(config)# dial-peer voice tag {pots|voip}
```

```
Router(config-dial-peer)# voice-class aaa tag
```

Example:

```
dial-peer voice 303 pots
```

```
voice-class aaa 303
```

Customizing Accounting Packets

This section contains the following sub-sections:

- [Configuration Overview, page 8](#)

- [Configuration Tasks for Customizing Accounting Packets, page 9](#)

Configuration Overview

Accounting packets for voice calls consist of voice-specific attributes as well as those that are not specific to voice. This document focuses only on voice-specific attributes. You can add some application-level attributes through the TCL script and fine tune the attribute list created by the system; the result is an accounting template that is customized to your accounting needs.

To customize your accounting packets, first create accounting templates.



Note

If you do not want to customize your accounting packets, enable voice accounting by using the **gw-accounting aaa** command to generate accounting packets. A specific set of attributes, which include both non voice-specific and voice-specific attributes, is automatically sent by the gateway to the RADIUS server.

To view the current list of VSAs, refer to the *RADIUS Vendor Specific Attributes Voice Implementation Guide*. For example, in the “[Accounting Template](#)” section on page 21 of [Chapter 1, “Overview of AAA on Voice Gateways”](#), the default attributes are:

```
h323-gw-id
h323-call-origin
h323-call-type
h323-setup-time
h323-connect-time
h323-disconnect-time
h323-disconnect-cause
h323-remote-address
h323-voice-quality    ICPIF
subscriber
```

To send all the VSAs to the accounting server use the **template callhistory-detail** command in global configuration mode. The [Accounting Template, page 21](#) in [Chapter 1, “Overview of AAA on Voice Gateways”](#) includes the default and new VSAs. Refer to the “[Using Callhistory-detail to Send All VSAs](#)” section on [page 9](#) for configuration details.

For the latest list of VSAs, refer to *RADIUS Vendor-Specific Attributes Voice Implementation Guide*.

To fine tune your accounting packets based on your billing needs, create accounting templates using specific VSAs that are applicable to your accounting needs. For example, to target different accounting servers for incoming calls from different trunks, you must define multiple accounting templates and associate them with different sets of incoming dial peers. To create a template, remove the attributes that are not applicable by adding the # sign in front of each of those attributes.

To tunr your accounting packets, remove attributes that do not apply to your billing needs. Deleting these attributes creates a custom accounting template that acts as a filter, allowing only the defined attributes to be sent to the accounting server. To apply acustomized template, first define the template using the **call accounting template voice** command in global configuration mode, and then apply it using either TCL scripts or the CLI. If you are using the CLI, you can apply the template either in global configuration or dial-peer configuration mode. Refer to the [“Defining and Applying Customized Accounting Templates” section on page 10](#) for configuraion details.

Specific VSAs that cannot be controlled by the accounting template are sent as attribute-value (AV) pairs through the *avlistSend* argument of the TCL verbs used in the script, and they are:

- h323-ivr-out
- h323-ivr-in
- h323-credit-amount
- h323-return-code
- h323-prompt-id
- h323-time-and-delay
- h323-redirect-number
- h323-preferred-lang
- h323-redirect-ip-addr
- h323-billing-model
- h323-currency

Configuration Tasks for Customizing Accounting Packets

Use the [“Configuration Overview” section on page 8](#) to plan your customizing needs before you begin the applicable configuration tasks below.

Generate Accounting Packets by Enabling Voice Accounting

To automatically generate accounting packets by enabling voice accounting, enter the **gw-accounting aaa** command in global configuration mode.

```
Router(config)# gw-accounting aaa
Router(gw-accounting aaa)# exit
```

Using Callhistory-detail to Send All VSAs

To send all VSAs (default and new) to the accounting server:

Step 1 Enter the **gw-accounting aaa** command to enter C mode.

```
Router(config)# gw-accounting aaa
```

- Step 2** Enter the **acct-template callhistory-detail** command in V mode.

```
Router(config-gw-accounting-aaa)# acct-template callhistory-detail
Router(config-gw-accounting-aaa)#
```

Defining and Applying Customized Accounting Templates

To define an accounting template:

- Step 1** Enter the **call accounting-template voice** command in global configuration mode. Enter the template name for *acctTemplateName*. The *url* is the address where you store the template. Always assign a .cdr extension to the filename in the URL.

```
Router(config)# call accounting-template voice acctTemplateName url
```

Example:

```
call accounting-template voice cdr1 tftp://highway/mjs/templates/cdr1.cdr
```



Note

After bootup, if the template file fails to load from the TFTP server, the system tries to automatically reload the file at five minute intervals.

You can use an accounting template through the CLI (in global configuration or dial-peer configuration mode), or by using TCL verbs.

To use an accounting template through the CLI in global configuration mode, use the following commands:

- Step 1** Enter the **gw-accounting aaa** command to enter gateway accounting AAA mode.

```
Router(config)# gw-accounting aaa
```

- Step 2** Enter the **acct-template** command. Assign your template name to *acctTemplateName*.

```
Router (config-gw-accounting-aaa)# acct-template acctTemplateName
```

Example:

```
acct-template aprill
```

Applying a Customized Accounting Template through the CLI in Dial-Peer Configuration Mode

To apply a customized accounting template through the CLI in dial peer configuration mode, follow these steps:

- Step 1** Enter the **call accounting-template voice** command in global configuration mode. Assign your template name to *acctTemplateName* and your template address (usually your tftp address) to *url*.

```
Router(config)# call accounting-template voice acctTemplateName url
```

Example:

```
call accounting-template voice cdr1 tftp://highway/mjs/templates/cdr1.cdr
```

- Step 2** Enter the **voice class aaa** command in global configuration mode. Assign a numerical value to *tag*.

```
Router(config)# voice class aaa tag
```

Example:

```
voice-class aaa 404
```

- Step 3** Enter the **accounting-template** command in voice class AAA mode. Assign your template name to *acctTempName*.

```
Router(config-class)# accounting-template acctTempName
```

Example:

```
accounting-template april1
```

- Step 4** Change configuration mode from global to dial peer and using the **dial peer voice** command, enter the **voice class aaa** command in dial-peer configuration mode. The numerical value of *tag* is the same value of *tag* in Step 2 above.

```
Router(config)# dial peer voice number [pots|voip]
```

```
Router(config-dial-peer)# voice class aaa tag
```

Example:

```
dial-peer voice 404 pots
```

```
voice-class aaa 404
```

Applying a Customized Accounting Template through a TCL Script

Use the **aaa accounting start** TCL verb. Assign an incoming or outgoing call leg, or assign an information tag. Assign your template name to *acctTempName*.

```
aaa accounting start {legID|info-tag} -t acctTempName
```

Adding Attributes to Accounting Packets through TCL scripts

To add attributes to accounting packets through TCL scripts, follow these steps:

- Step 1** Use the *avlistSend* argument in the TCL verbs to send the following attributes:

- h323-ivr-out
- h323-ivr-in
- h323-credit-amount
- h323-return-code
- h323-prompt-id
- h323-time-and-delay
- h323-redirect-number
- h323-preferred-lang
- h323-redirect-ip-addr
- h323-billing-model
- h323-currency

Step 2 Use TCL verbs for authentication, authorization, and accounting.

a. For authentication, use the **aaa authenticate** TCL verb.

```
aaa authenticate account password [-a avlistSend]
```

b. For authorization, use the **aaa authorize** TCL verb.

```
aaa authorize account password ani destination {legID | info-tag} [-a avlistSend]
```

c. For accounting, use the **aaa accounting start** TCL verb.

```
aaa accounting start {legID | info-tag} [-a avlistSend]
```

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.



Examples

This chapter includes Cisco IOS configuration examples and application scenarios of p sending customized accounting templates to billing servers and directing AAA requests based on account number, called number, and trunk grouping.

This chapter includes the following examples:

- [Directing a AAA Request Based on Trunk Grouping, page 1](#)
- [Directing a AAA Request Using an Account Number, page 2](#)
- [Directing AAA Traffic Using Called Number, page 9](#)
- [Directing Accounting Templates Using Called Number, page 12](#)

Directing a AAA Request Based on Trunk Grouping

A Cisco IOS configuration example for directing a AAA request based on trunk grouping is shown below:

```
aaa new-model
aaa group server radius sg1
server 10.1.0.1 auth-port 1645 acct-port 1646
!
aaa group server radius sg2
server 10.20.0.1 auth-port 1645 acct-port 1646
!
aaa group server radius sg-def
server 10.0.50.50 auth-port 1645 acct-port 1646
!
aaa authentication login abc group sg1
aaa authentication login def group sg2
aaa authentication login h323 group sg-def
aaa authorization exec abc group sg1
aaa authorization exec def group sg2
aaa authorization exec h323 group sg-def
aaa accounting connection abc start-stop group sg1
aaa accounting connection def start-stop group sg2
aaa accounting connection h323 start-stop group sg-def
!
gw-accounting aaa
!
```



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

© 2007 Cisco Systems, Inc. All rights reserved.

```

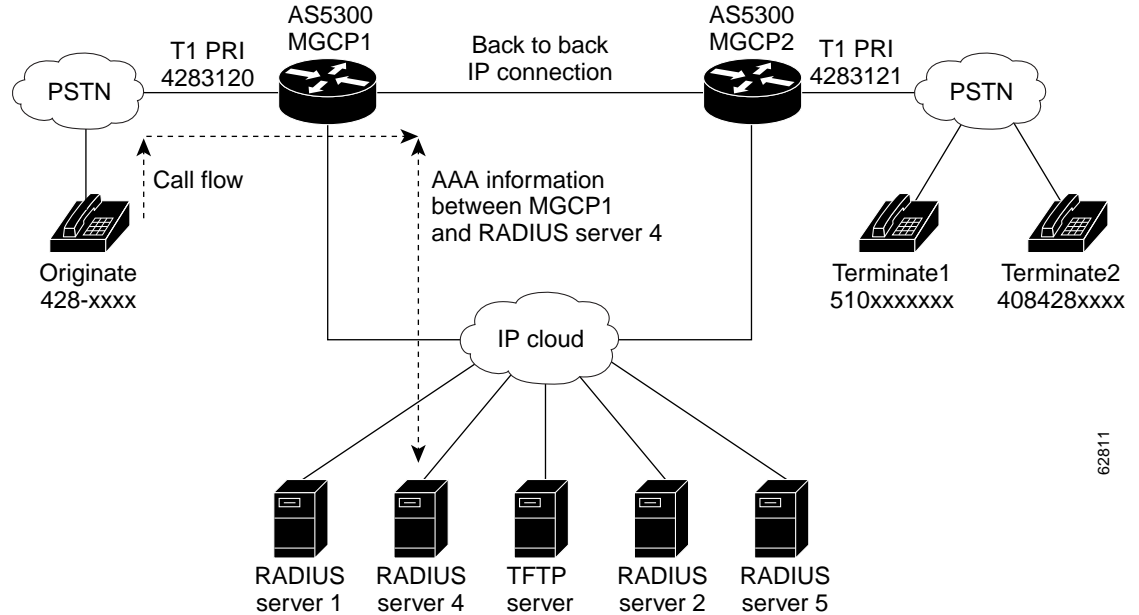
radius-server host 10.1.0.1 auth-port 1645 acct-port 1646 key abc
radius-server host 10.20.0.1 auth-port 1645 acct-port 1646 key ghi
radius-server host 10.0.50.50 auth-port 1645 acct-port 1646 key ghi
!
trunk group 101
!
interface Serial1/0/0:23
no ip address
no ip directed-broadcast
isdn switch-type primary-ni
isdn protocol-emulate network
isdn incoming-voice modem
no cdp enable
trunk-group 101
!
interface Serial1/0/1:23
no ip address
no ip directed-broadcast
isdn switch-type primary-ni
isdn protocol-emulate network
isdn incoming-voice modem
no cdp enable
trunk-group 101
!
voice-class aaa 1
authentication abc
authorization abc
accounting abc
!
voice-class aaa 1
authentication def
authorization def
accounting def
!
dial-peer voice 700 pots
destination-pabcern 1700.....
voice-class aaa 1
trunkgroup 101
!
dial-peer voice 900 pots
destination-pabcern 1900.....
voice-class aaa 2
trunkgroup 202
!

```

Directing a AAA Request Using an Account Number

In [Figure 1](#), the caller places a call to MGCP 1 with a modified debit card application applied to an incoming POTS dial peer. After the caller enters the card number (for example, 555550001), AAA requests are directed to RADIUS 4.

Figure 1 AAA Redirect Using An Account Number : Scenario 1



62811

A Cisco IOS configuration example for the topology in [Figure 1](#) is shown below:

```

Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
mgcp1#
02:27:24: %ISDN-6-CONNECT: Interface Serial3:22 is now connected to 4111234567
02:27:30: %ISDN-6-CONNECT: Interface Serial3:22 is now connected to 4111234567
02:27:44: RADIUS/ENCODE(00000024): Unsupported AAA attribute timezone
02:27:44: RADIUS(00000024): Encoding nas-port...Only port-type avlbl
02:27:44: RADIUS(00000024): sending
02:27:44: RADIUS(00000024): Encoding nas-port...Only port-type avlbl
02:27:44: RADIUS/ENCODE(00000024): acct_session_id: 36
02:27:44: RADIUS(00000024): sending
02:27:44: RADIUS(00000024): Encoding nas-port...Only port-type avlbl
02:27:44: RADIUS/ENCODE(00000024): acct_session_id: 36
02:27:44: RADIUS(00000024): sending
02:27:44: RADIUS: Send to unknown id 10 10.5.20.60:1234, Accounting-Request, len 480 <--
Accounting request sent
02:27:44: RADIUS: authenticator CD F1 66 D1 C1 CB A1 68 - B7 3F 5C 2B 21 D6 B7 4B
to AAA server 4 instead
02:27:44: RADIUS: User-Name [1] 12 "4111234567" server 2.
02:27:44: RADIUS: Acct-Status-Type [40] 6 Start [1]
02:27:44: RADIUS: Acct-Session-Id [44] 10 "00000024"
02:27:44: RADIUS: Vendor, Cisco [26] 25
02:27:44: RADIUS: h323-gw-id [33] 19 "h323-gw-id=mgcp1."
02:27:44: RADIUS: Vendor, Cisco [26] 56
02:27:44: RADIUS: Conf-Id [24] 50 "h323-conf-id=2E17E6F2 8E6611D4 8048FAFD
CD27A5B5"
02:27:44: RADIUS: Vendor, Cisco [26] 65
02:27:44: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=2E17E6F2 8E6611D4
8048FAFD CD27A5B5"
02:27:44: RADIUS: Vendor, Cisco [26] 38
02:27:44: RADIUS: Cisco AVpair [1] 32 "h323-ivr-out=account range: 55"
02:27:44: RADIUS: Vendor, Cisco [26] 33
02:27:44: RADIUS: Cisco AVpair [1] 27 "h323-ivr-out=color:violet"
02:27:44: RADIUS: Vendor, Cisco [26] 41

```

Directing a AAA Request Using an Account Number

```

02:27:44: RADIUS: Cisco AVpair [1] 35 "h323-ivr-out=MethodName:sanjo_aaa4"
02:27:44: RADIUS: Vendor, Cisco [26] 38
02:27:44: RADIUS: Cisco AVpair [1] 32 "h323-ivr-out=account range: 55"
02:27:44: RADIUS: Vendor, Cisco [26] 33
02:27:44: RADIUS: Cisco AVpair [1] 27 "h323-ivr-out=color:red"
02:27:44: RADIUS: Vendor, Cisco [26] 41
02:27:44: RADIUS: Cisco AVpair [1] 35 "h323-ivr-out=MethodName:sanjo_aaa4"
02:27:44: RADIUS: NAS-Port-Type [61] 6 Async [0]
02:27:44: RADIUS: Vendor, Cisco [26] 19
02:27:44: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
02:27:44: RADIUS: Calling-Station-Id [31] 12 "4111234567"
02:27:44: RADIUS: Called-Station-Id [30] 7 "13120"
02:27:44: RADIUS: Service-Type [6] 6 Login [1]
02:27:44: RADIUS: NAS-IP-Address [4] 6 10.6.20.500
02:27:44: RADIUS: Delay-Time [41] 6 0
02:27:44: RADIUS: Send to unknown id 20 10.6.20.60:1704, Access-Request, len 170 <--
Authentication request sent
02:27:44: RADIUS: authenticator 12 F5 47 5D 2D 07 74 A4 - 97 02 33 36 14 34 DE 07 to
server specified in
02:27:44: RADIUS: User-Name [1] 8 "555555" application and defined in
02:27:44: RADIUS: User-Password [2] 18 * CLI. NOTE: authentication
02:27:44: RADIUS: Vendor, Cisco [26] 56 Is not used in standard debit app
02:27:44: RADIUS: Conf-Id [24] 50 "h323-conf-id=2E17E6F2 8E6611D4 8048FAFD
CD27A5B5"
02:27:44: RADIUS: Vendor, Cisco [26] 37 but was included here to exercise
02:27:44: RADIUS: Cisco AVpair [1] 31 "h323-ivr-out=transactionID:20" AAA
authentication tcl verb.
02:27:44: RADIUS: NAS-Port-Type [61] 6 Async [0] Also
authentication
02:27:44: RADIUS: Vendor, Cisco [26] 19 done using account number
02:27:44: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23" instead of ANI.
02:27:44: RADIUS: NAS-IP-Address [4] 6 10.6.20.500
02:27:44: RADIUS: Send to unknown id 21 10.6.20.60:1704, Access-Request, len 200 <--
Authorization request
02:27:44: RADIUS: authenticator CA 67 12 31 EE 78 19 F4 - 4E 4E 21 1B FB DB B2 06
02:27:44: RADIUS: User-Name [1] 8 "0555550"
02:27:44: RADIUS: User-Password [2] 18 *
02:27:44: RADIUS: Vendor, Cisco [26] 56
02:27:44: RADIUS: Conf-Id [24] 50 "h323-conf-id=2E17E6F2 8E6611D4 8048FAFD
CD27A5B5"
02:27:44: RADIUS: Vendor, Cisco [26] 37
02:27:44: RADIUS: Cisco AVpair [1] 31 "h323-ivr-out=transactionID:21"
02:27:44: RADIUS: Calling-Station-Id [31] 12 "4111234567"
02:27:44: RADIUS: NAS-Port-Type [61] 6 Async [0]
02:27:44: RADIUS: Vendor, Cisco [26] 19
02:27:44: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
02:27:44: RADIUS: Calling-Station-Id [31] 12 "4111234567"
02:27:44: RADIUS: Service-Type [6] 6 Login [1]
02:27:44: RADIUS: NAS-IP-Address [4] 6 10.6.20.500
02:27:44: RADIUS: Received from id 10 10.5.20.60:1234, Accounting-response, len 20 <--
AccountingResponse from 02:27:44: RADIUS: authenticator E8 35 04 32 38 3E 78 78 - F1 D4
38 10 41 F3 EE F3 Radius observed
02:27:44: RADIUS: Received from id 20 10.6.20.60:1704, Access-Accept, len 200
<-- Response from Radius
02:27:44: RADIUS: authenticator 46 30 66 55 18 DC 82 A0 - 05 14 ED D8 3B 17 0C E7
02:27:44: RADIUS: Vendor, Cisco [26] 27
02:27:44: RADIUS: Cisco AVpair [1] 21 "h323-ivr-in=sanjose"
02:27:44: RADIUS: Vendor, Cisco [26] 34
02:27:44: RADIUS: Cisco AVpair [1] 28 "h323-credit-amount=5555.55"
02:27:44: RADIUS: Vendor, Cisco [26] 26
02:27:44: RADIUS: Cisco AVpair [1] 20 "h323-return-code=0"
02:27:44: RADIUS: Vendor, Cisco [26] 30
02:27:44: RADIUS: h323-credit-time [102] 24 "h323-credit-time=54123"
02:27:44: RADIUS: Vendor, Cisco [26] 33

```

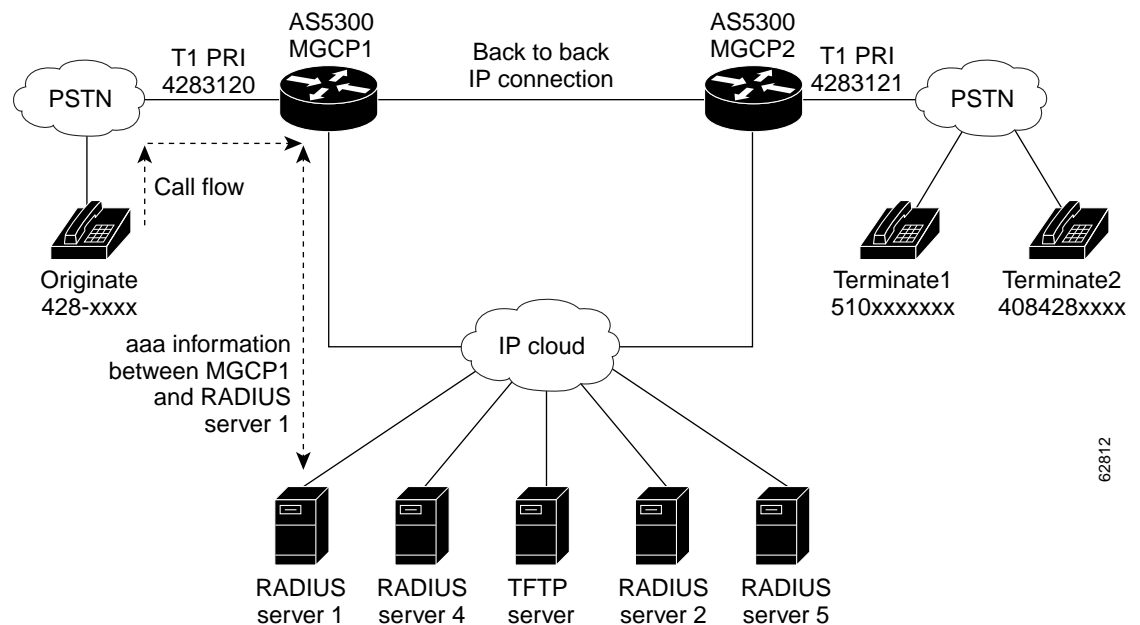
```

02:27:44: RADIUS: h323-billing-model [109] 27 "h323-billing-model=prepay"
02:27:44: RADIUS: Vendor, Cisco [26] 24
02:27:44: RADIUS: h323-currency [110] 18 "h323-currency=US"
02:27:44: RADIUS: Idle-Timeout [28] 6 30
02:27:44: RADIUS: Received from id 24
02:27:44: RADIUS: Received from id 21 10.6.20.60:1704, Access-Accept, len 200
02:27:44: RADIUS: authenticator 0F 13 36 EA B1 FC B3 95 - 85 FC CC FE 1F 2F 95 D0
02:27:44: RADIUS: Vendor, Cisco [26] 27
02:27:44: RADIUS: Cisco AVpair [1] 21 "h323-ivr-in=sanjose"
02:27:44: RADIUS: Vendor, Cisco [26] 34
02:27:44: RADIUS: Cisco AVpair [1] 28 "h323-credit-amount=5555.55"
02:27:44: RADIUS: Vendor, Cisco [26] 26
02:27:44: RADIUS: Cisco AVpair [1] 20 "h323-return-code=0"
02:27:44: RADIUS: Vendor, Cisco [26] 30
02:27:44: RADIUS: h323-credit-time [102] 24 "h323-credit-time=54123"
02:27:44: RADIUS: Vendor, Cisco [26] 33
02:27:44: RADIUS: h323-billing-model [109] 27 "h323-billing-model=prepay"
02:27:44: RADIUS: Vendor, Cisco [26] 24
02:27:44: RADIUS: h323-currency [110] 18 "h323-currency=US"
02:27:44: RADIUS: Idle-Timeout [28] 6 30
02:27:44: RADIUS: Received from id 24

```

In [Figure 2](#), the caller places a call to MGCP 1 with a modified debit card application applied to an incoming POTS dial peer. After the caller enters the card number (for example, 7777770001), the AAA requests are directed to RADIUS server 1.

Figure 2 AAA Redirect Using An Account Number: Scenario 2



Shown below are some Cisco IOS configuration examples for the topology in [Figure 2](#):

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mgcp1
!

```

```
aaa new-model
!
!
aaa group server radius sg1
  server 10.6.20.60 auth-port 1698 acct-port 1699
!
aaa group server radius sg4
  server 10.6.20.60 auth-port 1704 acct-port 1705
!
aaa group server radius sg6
  server 10.6.20.60 auth-port 1708 acct-port 1709
!
aaa authentication login sanjo_aaa1 group sg1
aaa authentication login sanjo_aaa4 group sg4
aaa authentication login sanjo_aaa6 group sg6
aaa authorization exec sanjo_aaa1 group sg1
aaa authorization exec sanjo_aaa4 group sg4
aaa authorization exec sanjo_aaa6 group sg6
aaa accounting connection sanjo_aaa1 start-stop group sg1
aaa accounting connection sanjo_aaa4 start-stop group sg4
aaa accounting connection sanjo_aaa6 start-stop group sg6
aaa session-id common
!
resource-pool disable
!
ip subnet-zero
ip host milp 10.223.254.255
!
isdn switch-type primary-5ess
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 3
  framing esf
  clock source line secondary
  linecode b8zs
  pri-group timeslots 1-24
!
gw-accounting aaa
!
interface Ethernet0
  ip address 10.0.254.255
  no ip redirects
  no ip mroute-cache
  no cdp enable
!
interface Serial0:23
  no ip address
  isdn switch-type primary-5ess
  isdn T321 0
  isdn T310 4000
  no cdp enable
!
interface Serial3:23
  no ip address
  trunk-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  isdn T321 0
  no cdp enable
!
interface FastEthernet0
  ip address 10.1.2.3 254.254.255.0
```

```

duplex auto
speed auto
!
ip classless
ip route 254.255.1.0 223.254.10.0.1.5.0.1 <- Route to tftp server
no ip http server 10.223.254.255
radius-server host 10.6.20.60 auth-port 1704 acct-port 1705
radius-server host 10.6.20.60 auth-port 1698 acct-port 1699
radius-server retransmit 3
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
call rsvp-sync
call accounting-template voice cdr1 tftp://10.223.254.255/johndoe/sanjose/cdr/cdr1.cdr
call accounting-template voice cdr2 tftp://10.223.254.255/johndoe/sanjose/cdr/cdr2.cdr
call language voice en tftp://milp/does/scripts/multi-lang/en_translate.tcl
!
call application voice integ_debit
tftp://10.223.254.255/johndoe/sanjose/apps/debitcard_int_redirect.tcl
call application voice integ_debit uid-len 6
call application voice integ_debit language 1 en
call application voice integ_debit language 2 sp
call application voice integ_debit set-location en 0
tftp://10.223.254.255/johndoe/prompts/en/
call application voice integ_debit set-location sp 0 tftp://10.6.20.50/prompts/
!
call application voice plain_debit
tftp://10.223.254.255/johndoe/sanjose/apps/debitcard.tcl
call application voice plain_debit uid-len 6
call application voice plain_debit language 1 en
call application voice plain_debit language 2 sp
call application voice plain_debit set-location en 0
tftp://10.223.254.255/johndoe/prompts/en/
call application voice plain_debit set-location sp 0 tftp://10.6.20.50/prompts/
!
voice-port 3:D
!
voice-port 0:D
!
dial-peer cor custom
dial-peer voice 100 pots
  application integ_debit <----- !Modified debit app to play
  incoming called-number 13120      new dynamic prompts, do
dial-peer voice 101 voip            authentication,
  destination-pabcern 510.....     authorization,
  session target ipv4:10.0.0.1     accounting redirect
!                                   and use accounting
dial-peer voice 102 voip            template.
  destination-pabcern 408.....
  session target ipv4:10.0.0.1
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
end

```

Debit Card Application for Directing AAA Requests Using an Account Number

A debit card application for directing AAA requests using an account number is shown below:

```

proc act_GotCardNumber { } {
    global count
    global retryCnt
    global promptFlag
    global account
    global pin
    global accountLen
    global cardLen
    global pinLen
    global ani
    global method
    global acct-template

    set status [infotag get evt_status]

    # Do we need to calculate len ???
    if { $status == "cd_005" } {
        set number [infotag get evt_dcdigits]
        set numberLen [ string length $number ]
        if { $numberLen == $cardLen } {
            set account [ string range $number 0 [expr $accountLen -1]]
            set pin [ string range $number $accountLen [expr $cardLen -1]]

            #####
            # Select Servertag based on first 2 #
            # digits of account number.      #
            #####
            set spcode [ string range $account 0 1]

            if { $spcode == 77 } {
                set method "sanjo_aaa1"
                set avList(h323-ivr-out,1) "account range: 77"
                set avList(h323-ivr-out,2) "color:violet"
                set avList(h323-ivr-out,3) "MethodName:sanjo_aaa1"
                puts "note that accounting template cdr1 needs to be defined in IOS CLI"
                set acct-template "cdr1"
            }
            puts "$spcode"
            set method "sanjo_aaa4"
            set avList(h323-ivr-out,1) "account range: 55"
            set avList(h323-ivr-out,2) "color:red"
            set avList(h323-ivr-out,3) "MethodName:sanjo_aaa4"
            set acct-template "cdr2"
        } else {
            set method "h323"
            set acct-template "none"
        }

            puts "THIS IS THE METHOD LIST USED: $method \r"
            puts "THIS IS THE TEMPLATE USED   : $template \r"

            #Do accounting
            if { $method != "h323" } {
                aaa accounting start leg_incoming -a avList -s $method -t $template
                set avList(h323-ivr-out,2) "color:purple"
                aaa accounting update leg_incoming -a avList -s $method -t $template

                # suppress service provide module automatically generating

```

```

# accounting records on outgoing call leg

infotag set leg_suppress_outgoing_auto_acct 1

#Do authenticate
puts "\r DOING AUTHENTICATION on account number and pin \r"
aaa authenticate $account $pin -s $method

puts "\r DOING AUTHORIZATION \r"
# DO authorize
aaa authorize $account $pin $ani "" leg_incoming -s $method

} else {
aaa accounting start leg_incoming -a avList -s $method
set avList(h323-ivr-out,2) "color:indigo"
aaa accounting update leg_incoming -a avList -s $method

# suppress service provide module automatically generating
# accounting records on outgoing call leg

infotag set leg_suppress_outgoing_auto_acct 1
infotag set leg_suppress_outgoing_auto_acct 1

#Do authenticate
puts "\r DOING AUTHENTICATION on account number and pin \r"
aaa authenticate $account $pin -s $method

puts "\r DOING AUTHORIZATION \r"
# DO authorize
aaa authorize $account $pin $ani "" leg_incoming -s $method

} else {
aaa accounting start leg_incoming -a avList -s $method
set avList(h323-ivr-out,2) "color:indigo"
aaa accounting update leg_incoming -a avList -s $method

# suppress service provide module automatically generating
# accounting records on outgoing call leg

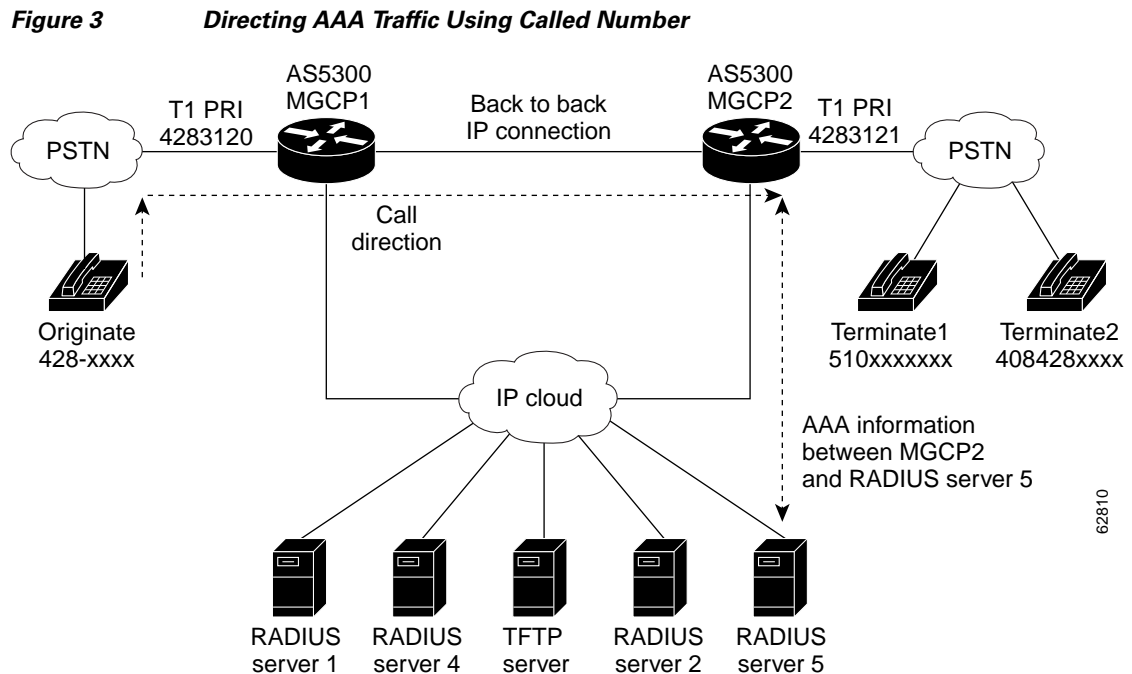
infotag set leg_suppress_outgoing_auto_acct 1

#Do authenticate for using default h323 method list
puts "\r DOING AUTHENTICATION \r"
aaa authenticate $account $pin -s $method
puts "\r DOING AUTHORIZATION \r"
aaa authorize $account $pin $ani "" leg_incoming -s $method
}

```

Directing AAA Traffic Using Called Number

In [Figure 3](#), the caller places a phone call to MGCP 1. A modified debit card application is applied to an incoming POTS dial peer. The caller enters the card number and the destination number sequence which is completed at MGCP 1. The destination number (for example 408-428-xxxx) is now dialed and directed to MGCP 2. Accounting information based on the called number is directed from MGCP 2 to RADIUS server 5.



62810

An example of a AAA redirect using the called number is shown below:

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mgcp2
!
aaa new-model
!
!
aaa group server radius sg2
server 10.6.20.60 auth-port 1700 acct-port 1701
!
aaa group server radius sg5
server 10.6.20.60 auth-port 1706 acct-port 1707
!
aaa group server radius sg6
server 10.6.20.60 auth-port 1708 acct-port 1709
!
aaa accounting connection sanjo_aaa5 start-stop group sg5
aaa accounting connection sanjo_aaa2 start-stop group sg2
aaa session-id common
!
username lab password 0 lab
!
!
resource-pool disable
!
ip subnet-zero
!
isdn switch-type primary-5ess
voice class aaa 2
accounting method sanjo_aaa2
!
voice class aaa 5

```

```
    accounting method sanjo_aaa5
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 0
    framing sf
    clock source line primary
    linecode ami
!
controller T1 1
    framing sf
    clock source line secondary 1
    linecode ami
!
controller T1 2
    framing sf
    linecode ami
!
controller T1 3
    framing esf
    linecode b8zs
    pri-group timeslots 1-24
!
gw-accounting aaa
!
!
!
interface Ethernet0
    ip address 10.6.20.501 254.255.1.0
    no cdp enable
interface Serial3:23
    no ip address
    isdn switch-type primary-5ess
    isdn incoming-voice modem
    no cdp enable
!
interface FastEthernet0
    ip address 10.0.0.1 255.255.255.0
    duplex auto
    speed auto
!
ip classless
ip route 254.255.1.0 223.254.10.0.1.5.0.1
no ip http server
!
!
!
radius-server host 10.6.20.60 auth-port 1700 acct-port 1701 key cisco
radius-server host 10.6.20.60 auth-port 1706 acct-port 1707 key cisco
radius-server retransmit 3
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication

voice-port 3:D
!
!
mgcp profile default
!
```

On the terminating side, the incoming dial peers are VoIP. In this configuration, if the incoming called number begins with 510, VoIP dial peer 101 is applied. If the incoming called number begins with 408, VoIP dial peer 102 is applied.

```
dial-peer voice 100 pots
 destination-pabcern 510 .....
 port 3:D
 prefix 91510 .....
!
dial-peer voice 101 voip
 incoming called-number 510 .....
 voice-class aaa 5
!
dial-peer voice 200 pots
 destination-pabcern 408.....
 port 3:D
 prefix 9
!
dial-peer voice 102 voip
 incoming called-number 408.....
 voice-class aaa 2
!
dial-peer voice 300 pots
 application integ_debit
 incoming called-number .
 port 3:D
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

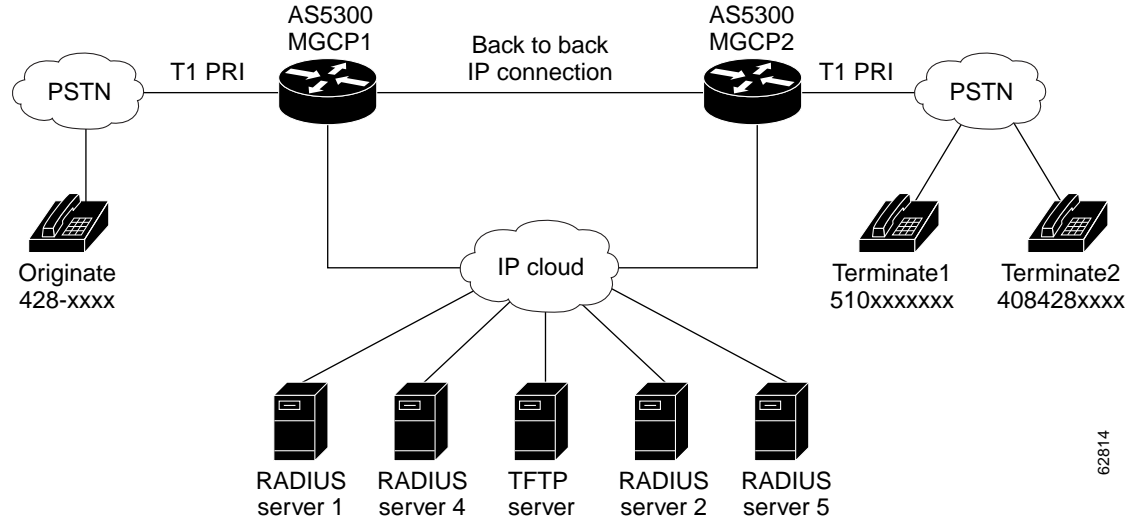
Directing Accounting Templates Using Called Number

In [Figure 4](#) below, accounting template cdr1 allows h323-gw-id av pair but does not allow h323-call-origin. Accounting template cdr2 allows h323-call-origin but does not allow h323-gw-id av pair. The caller places a phone call to MGCP 1. A modified debit card application is applied to an incoming POTS dial peer.

Accounting template cdr1 is selected using an account number (for example 7777770001). To verify that cdr1 was applied correctly, examine the accounting record on RADIUS server 1.

Accounting template cdr2 is selected using an account number (for example 5555550001). To verify that cdr2 was applied correctly, examine the accounting record on RADIUS server 2.

Figure 4 *Selecting Accounting Templates Using an Account Number*



62814

Shown below is an example of directing an accounting template using an incoming called number:

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mgcp1
!
aaa new-model
!
!
aaa group server radius sg1
server 10.6.20.60 auth-port 1698 acct-port 1699
!
aaa group server radius sg4
server 10.6.20.60 auth-port 1704 acct-port 1705
!
aaa group server radius sg6
server 10.6.20.60 auth-port 1708 acct-port 1709
!
aaa authentication login sanjo_aaa1 group sg1
aaa authentication login sanjo_aaa4 group sg4
aaa authentication login sanjo_aaa6 group sg6
aaa authorization exec sanjo_aaa1 group sg1
aaa authorization exec sanjo_aaa4 group sg4
aaa authorization exec sanjo_aaa6 group sg6
aaa accounting connection sanjo_aaa1 start-stop group sg1
aaa accounting connection sanjo_aaa4 start-stop group sg4
aaa accounting connection sanjo_aaa6 start-stop group sg6
aaa session-id common
!
!
!
resource-pool disable
!
ip subnet-zero
ip host milp 10.223.254.255
trunk group 1
carrier-id test
hunt-scheme least-used both

```

```
!
isdn switch-type primary-5ess
!
voice class aaa 1
!
voice class aaa 6
  authentication method sanjo_aaa6
  authorization method sanjo_aaa6
  accounting method sanjo_aaa6
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 0
  framing sf
  linecode ami
!
controller T1 1
  framing sf
  clock source line secondary 1
  linecode ami
!
controller T1 2
  framing sf
  linecode ami
!
controller T1 3
  framing esf
  clock source line primary
  linecode b8zs
  pri-group timeslots 1-24
!
gw-accounting aaa
!
interface Ethernet0
  ip address 10.0.254.255
  no ip redirects
  no ip mroute-cache
  no cdp enable
!
interface Serial3:23
  no ip address
  trunk-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  isdn T321 0
  no cdp enable
!
interface FastEthernet0
  ip address 10.1.2.3 254.254.255.0
  duplex auto
  speed auto
!
ip classless
ip route 254.255.1.0 223.254.10.0.1.5.0.1
no ip http server
!
radius-server host 10.6.20.60 auth-port 1708 acct-port 1709
radius-server host 10.6.20.60 auth-port 1704 acct-port 1705
radius-server host 10.6.20.60 auth-port 1698 acct-port 1699
radius-server host 10.6.43.255 auth-port 1645 acct-port 1646
radius-server host 10.6.37.10 auth-port 1645 acct-port 1646
```

```
radius-server retransmit 3
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
call rsvp-sync
call accounting-template voice cdr1 tftp://10.223.254.255/johndoe/sanjose/cdr/cdr1.cdr
call accounting-template voice cdr2 tftp://10.223.254.255/johndoe/sanjose/cdr/cdr2.cdr
call language voice en tftp://milp/doi/scripts/multi-lang/en_translate.tcl
!
call application voice acct_redirect_debit
tftp://10.6.20.50/sanjose/apps/debitcard_acct_redirect.tcl
call application voice acct_redirect_debit uid-len 6
call application voice acct_redirect_debit language 1 en
call application voice acct_redirect_debit language 2 sp
call application voice acct_redirect_debit set-location en 0 tftp://10.6.20.50/prompts/
call application voice acct_redirect_debit set-location sp 0 tftp://10.6.20.50/prompts/
!
call application voice integ_debit
tftp://10.223.254.255/johndoe/sanjose/apps/debitcard_int_redirect.tcl
call application voice integ_debit uid-len 6
call application voice integ_debit language 1 en
call application voice integ_debit language 2 sp
call application voice integ_debit set-location en 0
tftp://10.223.254.255/johndoe/prompts/en/
call application voice integ_debit set-location sp 0 tftp://10.6.20.50/prompts/
!
call application voice plain_debit
tftp://10.223.254.255/johndoe/sanjose/apps/debitcard.tcl
call application voice plain_debit uid-len 6
call application voice plain_debit language 1 en
call application voice plain_debit language 2 sp
call application voice plain_debit set-location en 0
tftp://10.223.254.255/johndoe/prompts/en/
call application voice plain_debit set-location sp 0 tftp://10.6.20.50/prompts/
!
voice-port 3:D
!
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 100 pots
debitcard_acct_redirect.tcl
incoming called-number .
!
dial-peer voice 101 voip
destination-pattern 1111234567
session target ipv4:10.0.0.1
!
dial-peer voice 102 voip
destination-pattern 408.....
session target ipv4:10.0.0.1
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

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.



Cisco IOS Troubleshooting

Troubleshooting

This chapter contains the following sections:

- [Using Debug Commands, page 1](#)
- [Using Show Commands, page 8](#)

Using Debug Commands

debug radius

The output below is from troubleshooting AAA redirect using called number for an incoming POTS dial peer.

!In this example, an incoming call is set up using **dial-peer voice 1000 pots**. Applying **voice-class aaa 1** to **dial-peer voice 1000** redirects AAA requests to the server specified for method list **sanj_aa1:10.6.20.70 auth-port 1698 acct-port 1699**.

```
aaa group server radius sg1
  server 10.6.20.70 auth-port 1698 acct-port 1699
!
aaa group server radius sg6
  server 10.6.20.70 auth-port 1704 acct-port 1705
!
aaa group server radius sg7
  server 10.6.20.70 auth-port 1720 acct-port 1721
!
aaa authentication login sanj_aa1 group sg1
aaa authorization exec sanj_aa1 group sg1
aaa accounting connection sanj_aa1 start-stop group sg1
!
aaa authentication login sanj_aa6 group sg6
aaa authorization exec sanj_aa6 group sg6
aaa accounting connection sanj_aa6 start-stop group sg6
!
aaa authentication login sanj_aa7 group sg7
aaa authorization exec sanj_aa7 group sg7
aaa accounting connection sanj_aa7 start-stop group sg7
```



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

© 2007 Cisco Systems, Inc. All rights reserved.

```

!
voice class aaa 1
 authentication method sanj_aa1
 authorization method sanj_aa1
 accounting method sanj_aa1
 accounting template cdr1
!
voice class aaa 2
 authentication method sanj_aaa6
 authorization method sanj_aaa6
 accounting method sanj_aaa6
 accounting template cdr2
!
voice class aaa 3
 authentication method sanj_aaa7
 authorization method sanj_aaa7
 accounting method sanj_aaa7
!
dial-peer voice 1000 pots
 application plain_debit
 incoming called-number 12345
 voice-class aaa 1
 port 0:D
!
dial-peer voice 1001 pots
 application plain_debit
 incoming called-number 12346
 voice-class aaa 2
 port 1:D

debug radius
Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
debug isdn q931
ISDN Q931 packets debugging is on

00:17:55: ISDN Se0:23: RX <- SETUP pd = 8 callref = 0x009D
00:17:55: Bearer Capability i = 0x8090A2
00:17:55: Channel ID i = 0xE1808397
00:17:55: Calling Party Number i = 0x0080, '4081234567', Plan:Unknown,
Type:Unknown
00:17:55: Called Party Number i = 0xE9, '12345', Plan:Private, Type:Abbreviated
00:17:55: RADIUS/ENCODE(0000000C): Unsupported AAA attribute timezone
00:17:55: RADIUS(0000000C): Encoding nas-port...Only port-type av1b1
00:17:55: RADIUS(0000000C): sending
00:17:55: RADIUS: Send to unknown id 4 10.6.20.70:1699, Accounting-Request, len 262
00:17:55: RADIUS: authenticator 10 41 58 99 4C F2 B1 CD - 44 3E E3 60 5D 10 C3 A9
00:17:55: RADIUS: Acct-Session-Id [44] 10 "0000000C"
00:17:55: RADIUS: Vendor, Cisco [26] 56
00:17:55: RADIUS: Conf-Id [24] 50 "h323-conf-id=B8FE8B7F BF1711D3 800CE483
89ADC43B"
00:17:55: RADIUS: Vendor, Cisco [26] 31
00:17:55: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
00:17:55: RADIUS: Vendor, Cisco [26] 65
00:17:55: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=B8FE8B7F BF1711D3
800CE483 89ADC43B"
00:17:55: RADIUS: User-Name [1] 12 "4081234567"
00:17:55: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:17:55: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:17:55: RADIUS: Vendor, Cisco [26] 19
00:17:55: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
00:17:55: RADIUS: Calling-Station-Id [31] 12 "4081234567"

```

```

00:17:55: RADIUS: Called-Station-Id [30] 7 "12345"
00:17:55: RADIUS: Service-Type [6] 6 Login [1]
00:17:55: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:17:55: RADIUS: Delay-Time [41] 6 0
00:17:55: ISDN Se0:23: TX -> CALL_PROC pd = 8 callref = 0x809D
00:17:55: Channel ID i = 0xA98397
00:17:55: ISDN Se0:23: TX -> CONNECT pd = 8 callref = 0x809D
00:17:55: RADIUS: Received from id 4 10.6.20.70:1699, Accounting-response, len 20
00:17:55: RADIUS: authenticator DC CD BA E8 7E 02 EA D1 - 12 67 DC 57 3C 73 56 75
00:17:55: ISDN Se0:23: RX <- CONNECT_ACK pd = 8 callref = 0x009D
00:17:55: ISDN Se0:23: CALL_PROGRESS: CALL_CONNECTED call id 0x63, bchan 22, dsl 0
00:17:55: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4081234567
00:18:01: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4081234567
00:18:06: RADIUS(0000000C): Encoding nas-port...Only port-type avlbl
00:18:06: RADIUS/ENCODE(0000000C): acct_session_id: 12
00:18:06: RADIUS(0000000C): sending
00:18:06: RADIUS: Send to unknown id 3 10.6.20.70:1698, Access-Request, len 199
00:18:06: RADIUS: authenticator 4B 2C 8C D7 12 54 45 3D - 51 44 30 05 C3 9B 44 B1
00:18:06: RADIUS: User-Name [1] 8 "777777"
00:18:06: RADIUS: User-Password [2] 18 *
00:18:06: RADIUS: Vendor, Cisco [26] 56
00:18:06: RADIUS: Conf-Id [24] 50 "h323-conf-id=61A46F2C 00000003 62E66E40
62E3A5C8"
00:18:06: RADIUS: Vendor, Cisco [26] 36
00:18:06: RADIUS: Cisco AVpair [1] 30 "h323-ivr-out=transactionID:3"
00:18:06: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:18:06: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:18:06: RADIUS: Vendor, Cisco [26] 19
00:18:06: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
00:18:06: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:18:06: RADIUS: Service-Type [6] 6 Login [1]
00:18:06: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:18:06: RADIUS: Received from id 3 10.6.20.70:1698, Access-Accept, len 200
00:18:06: RADIUS: authenticator 9C AA 9E 4C 64 02 13 3A - 72 8C 3F D9 72 D0 3B 06
00:18:06: RADIUS: Vendor, Cisco [26] 27
00:18:06: RADIUS: Cisco AVpair [1] 21 "h323-ivr-in=sanjose"
00:18:06: RADIUS: Vendor, Cisco [26] 34
00:18:06: RADIUS: Cisco AVpair [1] 28 "h323-credit-amount=7777.77"
00:18:06: RADIUS: Vendor, Cisco [26] 26
00:18:06: RADIUS: Cisco AVpair [1] 20 "h323-return-code=0"
00:18:06: RADIUS: Vendor, Cisco [26] 30
00:18:06: RADIUS: h323-credit-time [102] 24 "h323-credit-time=54329"
00:18:06: RADIUS: Vendor, Cisco [26] 33
00:18:06: RADIUS: h323-billing-model [109] 27 "h323-billing-model=prepay"
00:18:06: RADIUS: Vendor, Cisco [26] 24
00:18:06: RADIUS: h323-currency [110] 18 "h323-currency=US"
00:18:06: RADIUS: Idle-Timeout [28] 6 30
00:18:06: RADIUS: Received from id C
00:18:27: ISDN Se0:23: RX <- DISCONNECT pd = 8 callref = 0x009D
00:18:27: Cause i = 0x8290 - Normal call clearing
00:18:27: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4081234567 , call
lasted 32 seconds
00:18:27: ISDN Se0:23: TX -> RELEASE pd = 8 callref = 0x809D
00:18:27: ISDN Se0:23: RX <- RELEASE_COMP pd = 8 callref = 0x009D
00:18:27: RADIUS/ENCODE(0000000C): Unsupported AAA attribute timezone
00:18:27: RADIUS(0000000C): Encoding nas-port...Only port-type avlbl
00:18:27: RADIUS(0000000C): sending
00:18:27: RADIUS: Send to unknown id 5 10.6.20.70:1699, Accounting-Request, len 327
00:18:27: RADIUS: authenticator 2D 65 1C 38 6D 5B B3 DD - C8 57 D6 02 B4 4F E4 4E
00:18:27: RADIUS: Acct-Session-Id [44] 10 "0000000C"
00:18:27: RADIUS: Vendor, Cisco [26] 56
00:18:27: RADIUS: Conf-Id [24] 50 "h323-conf-id=B8FE8B7F BF1711D3 800CE483
89ADC43B"
00:18:27: RADIUS: Vendor, Cisco [26] 31

```

```

00:18:27: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
00:18:27: RADIUS: Vendor, Cisco [26] 65
00:18:27: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=B8FE8B7F BF1711D3
800CE483 89ADC43B"
00:18:27: RADIUS: Acct-Input-Octets [42] 6 0
00:18:27: RADIUS: Acct-Output-Octets [43] 6 148000
00:18:27: RADIUS: Acct-Input-Packets [47] 6 0
00:18:27: RADIUS: Acct-Output-Packets [48] 6 925
00:18:27: RADIUS: Acct-Session-Time [46] 6 32
00:18:27: RADIUS: Vendor, Cisco [26] 35
00:18:27: RADIUS: Cisco AVpair [1] 29 "h323-ivr-out=Tariff:Unknown"
00:18:27: RADIUS: User-Name [1] 12 "4081234567"
00:18:27: RADIUS: Acct-Status-Type [40] 6 Stop [2]
00:18:27: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:18:27: RADIUS: Vendor, Cisco [26] 19
00:18:27: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
00:18:27: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:18:27: RADIUS: Called-Station-Id [30] 7 "12345"
00:18:27: RADIUS: Service-Type [6] 6 Login [1]
00:18:27: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:18:27: RADIUS: Delay-Time [41] 6 0
00:18:27: RADIUS: Received from id 5 10.6.20.70:1699, Accounting-response, len 20
00:18:27: RADIUS: authenticator E5 B1 ED 3B AD A8 5B 5C - 49 83 63 BA DF 02 B2 00

```

An incoming call is set up using dial-peer voice 1001 pots. dial-peer voice 1001 has voice-class aaa 2 applied which should redirect AAA requests to the server specified for method list sanj_aaa6: 10.6.20.70 auth-port 1708 acct-port 1709.

```

00:30:05: ISDN Sel:23: RX <- SETUP pd = 8 callref = 0x0004
00:30:05: Bearer Capability i = 0x8090A2
00:30:05: Channel ID i = 0xE1808397
00:30:05: Calling Party Number i = 0x0080, '4081234567', Plan:Unknown,
Type:Unknown
00:30:05: Called Party Number i = 0xE9, '12346', Plan:Private, Type:Abbreviated
00:30:05: RADIUS/ENCODE(0000000E): Unsupported AAA attribute timezone
00:30:05: RADIUS(0000000E): Encoding nas-port...Only port-type avbl
00:30:05: RADIUS(0000000E): sending
00:30:05: RADIUS: Send to unknown id 6 10.6.20.70:1709, Accounting-Request, len 262
00:30:05: RADIUS: authenticator 2F 3A 09 3D 6B C4 10 D2 - F6 68 D6 F4 36 35 C3 DE
00:30:05: RADIUS: Acct-Session-Id [44] 10 "0000000E"
00:30:05: RADIUS: Vendor, Cisco [26] 56
00:30:05: RADIUS: Conf-Id [24] 50 "h323-conf-id=6C29BC16 BF1911D3 8010E483
89ADC43B"
00:30:05: RADIUS: Vendor, Cisco [26] 31
00:30:05: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
00:30:05: RADIUS: Vendor, Cisco [26] 65
00:30:05: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=6C29BC16 BF1911D3
8010E483 89ADC43B"
00:30:05: RADIUS: User-Name [1] 12 "4081234567"
00:30:05: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:30:05: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:30:05: RADIUS: Vendor, Cisco [26] 19
00:30:05: RADIUS: cisco-nas-port [2] 13 "ISDN 1:D:23"
00:30:05: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:30:05: RADIUS: Called-Station-Id [30] 7 "12346"
00:30:05: RADIUS: Service-Type [6] 6 Login [1]
00:30:05: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:30:05: RADIUS: Delay-Time [41] 6 0
00:30:05: ISDN Sel:23: TX -> CALL_PROC pd = 8 callref = 0x8004
00:30:05: Channel ID i = 0xA98397
00:30:05: ISDN Sel:23: TX -> CONNECT pd = 8 callref = 0x8004
00:30:05: ISDN Sel:23: RX <- CONNECT_ACK pd = 8 callref = 0x0004
00:30:05: ISDN Sel:23: CALL_PROGRESS: CALL_CONNECTED call id 0x64, bchan 22, dsl 1
00:30:05: %ISDN-6-CONNECT: Interface Serial1:22 is now connected to 4081234567

```

```

00:30:06: RADIUS: Received from id 6 10.6.20.70:1709, Accounting-response, len 20
00:30:06: RADIUS: authenticator E1 AD 70 9F DC 09 29 32 - 74 47 96 9F 3F 77 27 82
00:30:11: %ISDN-6-CONNECT: Interface Serial1:22 is now connected to 4081234567
00:30:19: RADIUS(0000000E): Encoding nas-port...Only port-type avlbl
00:30:19: RADIUS/ENCODE(0000000E): acct_session_id: 14
00:30:19: RADIUS(0000000E): sending
00:30:19: RADIUS: Send to unknown id 4 10.6.20.70:1708, Access-Request, len 199
00:30:19: RADIUS: authenticator CE 16 21 8D A5 59 56 9F - B7 E9 CA 5C EC C5 89 A0
00:30:19: RADIUS: User-Name [1] 8 "777777"
00:30:19: RADIUS: User-Password [2] 18 *
00:30:19: RADIUS: Vendor, Cisco [26] 56
00:30:19: RADIUS: Conf-Id [24] 50 "h323-conf-id=61A46F2C 00000003 62E66E40
634A0A64"
00:30:19: RADIUS: Vendor, Cisco [26] 36
00:30:19: RADIUS: Cisco AVpair [1] 30 "h323-ivr-out=transactionID:4"
00:30:19: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:30:19: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:30:19: RADIUS: Vendor, Cisco [26] 19
00:30:19: RADIUS: cisco-nas-port [2] 13 "ISDN 1:D:23"
00:30:19: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:30:19: RADIUS: Service-Type [6] 6 Login [1]
00:30:19: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:30:20: RADIUS: Received from id 4 10.6.20.70:1708, Access-Accept, len 173
00:30:20: RADIUS: authenticator FF 0D 40 72 0D 80 12 26 - 44 13 D5 0E C4 BB 71 BE
00:30:20: RADIUS: Vendor, Cisco [26] 34
00:30:20: RADIUS: Cisco AVpair [1] 28 "h323-credit-amount=7777.77"
00:30:20: RADIUS: Vendor, Cisco [26] 26
00:30:20: RADIUS: Cisco AVpair [1] 20 "h323-return-code=0"
00:30:20: RADIUS: Vendor, Cisco [26] 30
00:30:20: RADIUS: h323-credit-time [102] 24 "h323-credit-time=54329"
00:30:20: RADIUS: Vendor, Cisco [26] 33
00:30:20: RADIUS: h323-billing-model [109] 27 "h323-billing-model=prepay"
00:30:20: RADIUS: Vendor, Cisco [26] 24
00:30:20: RADIUS: h323-currency [110] 18 "h323-currency=US"
00:30:20: RADIUS: Idle-Timeout [28] 6 30
00:30:20: RADIUS: Received from id E
00:30:43: ISDN Sel:23: RX <- DISCONNECT pd = 8 callref = 0x0004
00:30:43: Cause i = 0x8290 - Normal call clearing
00:30:43: %ISDN-6-DISCONNECT: Interface Serial1:22 disconnected from 4081234567 , call
lasted 37 seconds
00:30:43: ISDN Sel:23: TX -> RELEASE pd = 8 callref = 0x8004
00:30:43: ISDN Sel:23: RX <- RELEASE_COMP pd = 8 callref = 0x0004
00:30:43: RADIUS/ENCODE(0000000E): Unsupported AAA attribute timezone
00:30:43: RADIUS(0000000E): Encoding nas-port...Only port-type avlbl
00:30:43: RADIUS(0000000E): sending
00:30:43: RADIUS: Send to unknown id 7 10.6.20.70:1709, Accounting-Request, len 327
00:30:43: RADIUS: authenticator 99 5A B4 45 67 C0 F4 91 - 9B 4B C3 1D 7E DE 7D D1
00:30:43: RADIUS: Acct-Session-Id [44] 10 "0000000E"
00:30:43: RADIUS: Vendor, Cisco [26] 56
00:30:43: RADIUS: Conf-Id [24] 50 "h323-conf-id=6C29BC16 BF1911D3 8010E483
89ADC43B"
00:30:43: RADIUS: Vendor, Cisco [26] 31
00:30:43: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
00:30:43: RADIUS: Vendor, Cisco [26] 65
00:30:43: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=6C29BC16 BF1911D3
8010E483 89ADC43B"
00:30:43: RADIUS: Acct-Input-Octets [42] 6 0
00:30:43: RADIUS: Acct-Output-Octets [43] 6 161920
00:30:43: RADIUS: Acct-Input-Packets [47] 6 0
00:30:43: RADIUS: Acct-Output-Packets [48] 6 1012
00:30:43: RADIUS: Acct-Session-Time [46] 6 37
00:30:43: RADIUS: Vendor, Cisco [26] 35
00:30:43: RADIUS: Cisco AVpair [1] 29 "h323-ivr-out=Tariff:Unknown"
00:30:43: RADIUS: User-Name [1] 12 "4081234567"

```

```

00:30:43: RADIUS: Acct-Status-Type [40] 6 Stop [2]
00:30:43: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:30:43: RADIUS: Vendor, Cisco [26] 19
00:30:43: RADIUS: cisco-nas-port [2] 13 "ISDN 1:D:23"
00:30:43: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:30:43: RADIUS: Called-Station-Id [30] 7 "12346"
00:30:43: RADIUS: Service-Type [6] 6 Login [1]
00:30:43: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:30:43: RADIUS: Delay-Time [41] 6 0
00:30:43: RADIUS: Received from id 7 10.6.20.70:1709, Accounting-response, len 20
00:30:43: RADIUS: authenticator 78 80 AB D1 82 75 ED ED - E4 1F 12 25 D8 83 F9 6

```

!voice class aaa 3 is applied to **dial-peer voice 1000 pots** and a call is made. **voice class aaa 3** uses server 10.6.20.70 with auth port 1720 and acct port 1721. The radius daemon has not started. AAA accounting and AAA authorization requests are sent to the appropriate server but no acknowledgement is received. Retries are attempted.

```

00:37:03: %SYS-5-CONFIG_I: Configured from console by console
00:37:11: ISDN Se0:23: RX <- SETUP pd = 8 callref = 0x009E
00:37:11: Bearer Capability i = 0x8090A2
00:37:11: Channel ID i = 0xE1808397
00:37:11: Calling Party Number i = 0x0080, '4081234567', Plan:Unknown,
Type:Unknown
00:37:11: Called Party Number i = 0xE9, '12345', Plan:Private, Type:Abbreviated
00:37:11: RADIUS/ENCODE(00000010): Unsupported AAA attribute timezone
00:37:11: RADIUS(00000010): Encoding nas-port...Only port-type avlbl
00:37:11: RADIUS(00000010): sending
00:37:11: RADIUS: Send to unknown id 8 10.6.20.70:1721, Accounting-Request, len 414
00:37:11: RADIUS: authenticator EC F7 FD AB ED 0D 26 BF - F0 A4 D2 88 91 1E D9 22
00:37:11: RADIUS: Acct-Session-Id [44] 10 "00000010"
00:37:11: RADIUS: Vendor, Cisco [26] 56
00:37:11: RADIUS: h323-setup-time [25] 50 "h323-setup-time=*00:37:09.095 UTC Sat
Jan 1 2000"
00:37:11: RADIUS: Vendor, Cisco [26] 34
00:37:11: RADIUS: h323-gw-id [33] 28 "h323-gw-id=router."
00:37:11: RADIUS: Vendor, Cisco [26] 56
00:37:11: RADIUS: Conf-Id [24] 50 "h323-conf-id=69EAABEB BF1A11D3 8014E483
89ADC43B"
00:37:11: RADIUS: Vendor, Cisco [26] 31
00:37:11: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
00:37:11: RADIUS: Vendor, Cisco [26] 32
00:37:11: RADIUS: h323-call-type [27] 26 "h323-call-type=Telephony"
00:37:11: RADIUS: Vendor, Cisco [26] 65
00:37:11: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=69EAABEB BF1A11D3
8014E483 89ADC43B"
00:37:11: RADIUS: Vendor, Cisco [26] 30
00:37:11: RADIUS: Cisco AVpair [1] 24 "subscriber=RegularLine"
00:37:11: RADIUS: User-Name [1] 12 "4081234567"
00:37:11: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:37:11: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:37:11: RADIUS: Vendor, Cisco [26] 19
00:37:11: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
00:37:11: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:37:11: RADIUS: Called-Station-Id [30] 7 "12345"
00:37:11: RADIUS: Service-Type [6] 6 Login [1]
00:37:11: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:37:11: RADIUS: Delay-Time [41] 6 0
00:37:11: ISDN Se0:23: TX -> CALL_PROC pd = 8 callref = 0x809E
00:37:11: Channel ID i = 0xA98397
00:37:11: ISDN Se0:23: TX -> CONNECT pd = 8 callref = 0x809E
00:37:11: ISDN Se0:23: RX <- CONNECT_ACK pd = 8 callref = 0x009E
00:37:11: ISDN Se0:23: CALL_PROGRESS: CALL_CONNECTED call id 0x65, bchan 22, dsl 0
00:37:11: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4081234567

```

```

00:37:16: RADIUS: Retransmit id 8
00:37:16: RADIUS: acct-delay-time for 4021D9EC (at 4021DB84) now 5
00:37:17: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4081234567
00:37:21: RADIUS: Retransmit id 1
00:37:21: RADIUS: acct-delay-time for 4021D9EC (at 4021DB84) now 10
00:37:26: RADIUS: Retransmit id 2
00:37:26: RADIUS: acct-delay-time for 4021D9EC (at 4021DB84) now 15
00:37:31: RADIUS: Tried all servers.
00:37:31: RADIUS: No valid server found. Trying any viable server
00:37:31: RADIUS: Tried all servers.
00:37:31: RADIUS: No response for id 3
00:37:31: RADIUS/DECODE: parse response no app start; FAIL
00:37:31: RADIUS/DECODE: parse response; FAIL
00:37:35: RADIUS(00000010): Encoding nas-port...Only port-type avlbl
00:37:35: RADIUS/ENCODE(00000010): acct_session_id: 16
00:37:35: RADIUS(00000010): sending
00:37:35: RADIUS: Send to unknown id 5 10.6.20.70:1720, Access-Request, len 199
00:37:35: RADIUS: authenticator 4B 6E 67 9F D4 1E 73 37 - 45 D3 CD 7C 70 FD C7 12
00:37:35: RADIUS: User-Name [1] 8 "777777"
00:37:35: RADIUS: User-Password [2] 18 *
00:37:35: RADIUS: Vendor, Cisco [26] 56
00:37:35: RADIUS: Conf-Id [24] 50 "h323-conf-id=61A46F2C 00000003 62E66E40
634A0A64"
00:37:35: RADIUS: Vendor, Cisco [26] 36
00:37:35: RADIUS: Cisco AVpair [1] 30 "h323-ivr-out=transactionID:5"
00:37:35: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:37:35: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:37:35: RADIUS: Vendor, Cisco [26] 19
00:37:35: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
00:37:35: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:37:35: RADIUS: Service-Type [6] 6 Login [1]
00:37:35: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:37:40: RADIUS: Retransmit id 5
00:37:45: RADIUS: Retransmit id 5
00:37:50: RADIUS: Retransmit id 5
00:37:55: RADIUS: Tried all servers.
00:37:55: RADIUS: No valid server found. Trying any viable server
00:37:55: RADIUS: Tried all servers.
00:37:55: RADIUS: No response for id 5
00:37:55: RADIUS/DECODE: parse response no app start; FAIL
00:37:55: RADIUS/DECODE: parse response; FAIL
00:38:00: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4081234567 , call
lasted 48 seconds
00:38:00: ISDN Se0:23: TX -> DISCONNECT pd = 8 callref = 0x809E
00:38:00: Cause i = 0x8090 - Normal call clearing
00:38:00: RADIUS/ENCODE(00000010): Unsupported AAA attribute timezone
00:38:00: RADIUS(00000010): Encoding nas-port...Only port-type avlbl
00:38:00: RADIUS(00000010): sending
00:38:00: RADIUS: Send to unknown id 9 10.6.20.70:1721, Accounting-Request, len 660
00:38:00: RADIUS: authenticator C5 79 B7 D3 92 75 37 D0 - E7 5C 5B 84 99 6E 97 17
00:38:00: RADIUS: Acct-Session-Id [44] 10 "00000010"
00:38:00: RADIUS: Vendor, Cisco [26] 56
00:38:00: RADIUS: h323-setup-time [25] 50 "h323-setup-time=*00:37:09.095 UTC Sat
Jan 1 2000"
00:38:00: RADIUS: Vendor, Cisco [26] 34
00:38:00: RADIUS: h323-gw-id [33] 28 "h323-gw-id=router."
00:38:00: RADIUS: Vendor, Cisco [26] 56
00:38:00: RADIUS: Conf-Id [24] 50 "h323-conf-id=69EAABEB BF1A11D3 8014E483
89ADC43B"
00:38:00: RADIUS: Vendor, Cisco [26] 31
00:38:00: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
00:38:00: RADIUS: Vendor, Cisco [26] 32
00:38:00: RADIUS: h323-call-type [27] 26 "h323-call-type=Telephony"
00:38:00: RADIUS: Vendor, Cisco [26] 65

```

```

00:38:00: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=69EAABEB BF1A11D3
8014E483 89ADC43B"
00:38:00: RADIUS: Vendor, Cisco [26] 30
00:38:00: RADIUS: Cisco AVpair [1] 24 "subscriber=RegularLine"
00:38:00: RADIUS: Acct-Input-Octets [42] 6 0
00:38:00: RADIUS: Acct-Output-Octets [43] 6 112160
00:38:00: RADIUS: Acct-Input-Packets [47] 6 0
00:38:00: RADIUS: Acct-Output-Packets [48] 6 701
00:38:00: RADIUS: Acct-Session-Time [46] 6 49
00:38:00: RADIUS: Vendor, Cisco [26] 58
00:38:00: RADIUS: h323-connect-time [28] 52 "h323-connect-time=*00:37:09.109 UTC Sat
Jan 1 2000"
00:38:00: RADIUS: Vendor, Cisco [26] 61
00:38:00: RADIUS: h323-disconnect-tim[29] 55 "h323-disconnect-time=*00:37:57.739 UTC
Sat Jan 1 2000"
00:38:00: RADIUS: Vendor, Cisco [26] 34
00:38:00: RADIUS: h323-disconnect-cau[30] 28 "h323-disconnect-cause=10 "
00:38:00: RADIUS: Vendor, Cisco [26] 35
00:38:00: RADIUS: Cisco AVpair [1] 29 "h323-ivr-out=Tariff:Unknown"
00:38:00: RADIUS: Vendor, Cisco [26] 28
00:38:00: RADIUS: h323-voice-quality [31] 22 "h323-voice-quality=0"
00:38:00: RADIUS: User-Name [1] 12 "4081234567"
00:38:00: RADIUS: Acct-Status-Type [40] 6 Stop [2]
00:38:00: RADIUS: NAS-Port-Type [61] 6 Async [0]
00:38:00: RADIUS: Vendor, Cisco [26] 19
00:38:00: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
00:38:00: RADIUS: Calling-Station-Id [31] 12 "4081234567"
00:38:00: RADIUS: Called-Station-Id [30] 7 "12345"
00:38:00: RADIUS: Service-Type [6] 6 Login [1]
00:38:00: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
00:38:00: RADIUS: Delay-Time [41] 6 0
00:38:00: ISDN Se0:23: RX <- RELEASE pd = 8 callref = 0x009E
00:38:00: ISDN Se0:23: TX -> RELEASE_COMP pd = 8 callref = 0x809E
00:38:05: RADIUS: Retransmit id 9
00:38:05: RADIUS: acct-delay-time for 4021D9EC (at 4021DC7A) now 5
00:38:10: RADIUS: Retransmit id 4
00:38:10: RADIUS: acct-delay-time for 4021D9EC (at 4021DC7A) now 10
00:38:15: RADIUS: Retransmit id 5
00:38:15: RADIUS: acct-delay-time for 4021D9EC (at 4021DC7A) now 15
00:38:20: RADIUS: Tried all servers.
00:38:20: RADIUS: No valid server found. Trying any viable server
00:38:20: RADIUS: Tried all servers.
00:38:20: RADIUS: No response for id 6
00:38:20: RADIUS/DECODE: parse response no app start; FAIL
00:38:20: RADIUS/DECODE: parse response; FAIL

```

Using Show Commands

show call accounting voice summary

Show call accounting voice summary shows the status of all accounting templates that are defined, loaded.

```

show call accounting voice summary
name          url                                     last_load  is_running
=====
cdr1          tftp://10.255.255.255/johndoe/sanjose/ success    is running
cdr2          tftp://10.255.255.255/johndoe/sanjose/ success    is running

```

show call accounting-template voice <template name>

show call accounting-template voice <template name> shows the VSAs that are contained in the accounting template.

```
show call accounting-template voice cdr1
CDR template cdr1 is running
  url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
The last load was successful.
```

```
  attr: h323-call-origin (56)
```

```
Totally 1 attrs defined.
```

```
show call accounting-template voice cdr2
CDR template cdr2 is running
  url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr2.cdr
The last load was successful.
```

```
  attr: h323-call-origin (56)
```

```
Totally 1 attrs defined.
```

!The output below results from defining a template that does not exist or that cannot be reached.

```
router(config)#$://10.255.255.255/johndoe/sanjose/cdr/cdr4000.cdr
Reading cdr template cdr10 fail, put it on retry queue.
```

```
01:15:46: hifs ifs could not open file
```

!The output below is for a template with an invalid VSA.

```
sh call accounting-template voice cdr1
CDR template cdr1 is running
  url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
  The last load was successful.
```

```
  attr: h323-call-origin (56)
```

```
Totally 1 attrs defined.
```

!Template cdr1.cdr is modified on the tftp server to enable an invalid VSA (for example h323-call-origin) to be put into the template.

```
call accounting-template voice reload cdr1
Loading johndoe/sanjose/cdr/cdr1.cdr from 10.255.255.255 (via Ethernet0): !
[OK - 88/4096 bytes]
cam: Fail to reload cdr template cdr1, unloading ...
```

```
02:27:29: hifs ifs file read succeeded. size=88,
url=tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
02:27:29: Error: attr name invalid-vsa-h323-call-origin (0) is not valid in line 3.
```

```
sh call accounting-template voice cdr1
CDR template cdr1 is running
  url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
Last load returned errno=8, Exec format error
```

```
attr: h323-call-origin (56)
```

```
Totally 1 attrs defined.
```

The template has been rejected, and previous template still applied.

show call aaa attributes

show call aaa attributes displays the VSAs that are supported. Mandatory VSAs that are sent to the accounting server are not displayed.

```
sh call aaa attributes
AAA ATTRIBUTE LIST:
  Name=disc-cause-ext           Format=Enum
  Name=Acct-Status-Type        Format=Enum
  Name=acl                      Format=Ulong
  Name=addr                    Format=IP v4 Address
  .....
  Name=gw-password             Format=Binary
  Name=h323-billing-model      Format=String
  Name=h323-call-origin        Format=String
  .....
  .....
```

!Use the **show call accounting-template voice summary** command to check if a template is loaded and running.

!The output below shows two templates successfully loaded and running, and a template that failed to load.

```
show call accounting-template voice summary
name          url                                     last_load  is_running
=====
cdr1          tftp://10.255.255.255/johndoe/sanjose/ success    is running
cdr2          tftp://10.255.255.255/johndoe/sanjose/ success    is running
cdr10        tftp://10.255.255.255/johndoe/sanjose/ fail       is not running
```

!The output below shows reloading template cdr1 after modifying it.

!Initially, the original template cdr1 is loaded as shown:

```
show call accounting-template voice cdr1
CDR template cdr1 is running
url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
The last load was successful.
```

```
attr: h323-call-origin (56)
```

```
Totally 1 attrs defined.
```

!Additional VSAs are added to modify cdr1 on the tftp server as shown:

```
call accounting
call accounting-template voice reload cdr1
Loading johndoe/sanjose/cdr/cdr1.cdr from 10.255.255.255 (via Ethernet0): !
[OK - 1848/3072 bytes]
```

```
cam: Reload cdr template cdr1 success.
01:35:58: hifs ifs file read succeeded. size=1848,
url=tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
show call accounting-template voice cdr1
CDR template cdr1 is running
url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
The last load was successful.
attr: h323-call-origin (56)
```

```
attr: h323-call-type (57)
attr: h323-connect-time (59)
attr: h323-disconnect-cause (63)
attr: h323-disconnect-time (64)
attr: h323-gw-id (65)
attr: h323-remote-address (73)
attr: h323-remote-id (74)
attr: h323-setup-time (76)
attr: h323-voice-quality (78)
attr: subscriber (79)
attr: in-portgrp-id (80)
attr: out-portgrp-id (81)
attr: charged-units (82)
attr: disconnect-text (83)
attr: info-type (84)
attr: logical-if-index (85)
attr: peer-address (86)
attr: peer-id (87)
attr: peer-if-index (88)
attr: acom-level (89)
attr: tx-duration (90)
attr: voice-tx-duration (91)
attr: fax-tx-duration (92)
attr: noise-level (94)
attr: codec-bytes (95)
attr: coder-type-rate (96)
attr: early-packets (97)
attr: late-packets (98)
attr: lost-packets (99)
attr: gapfill-with-interpolation (100)
attr: gapfill-with-prediction (101)
attr: gapfill-with-redundancy (102)
attr: gapfill-with-silence (103)
attr: lowater-playout-delay (104)
attr: hiwater-playout-delay (105)
attr: ontime-rv-playout (106)
attr: receive-delay (107)
attr: round-trip-delay (108)
attr: remote-udp-port (109)
attr: session-protocol (110)
attr: vad-enable (111)
```

Totally 42 attrs defined.

debug radius accounting

In the output below, cdr1 includes h323-call-origin but does not include VSA h323-gw-id. cdr2 includes h323-gw-id but does not include h323-call-origin.

```
show call accounting-template voice cdr1
CDR template cdr1 is running
url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr1.cdr
The last load was successful.

attr: h323-call-origin (56)
```

Totally 1 attrs defined.

```
show call accounting-template voice cdr2
```

```
CDR template cdr2 is running
url: tftp://10.255.255.255/johndoe/sanjose/cdr/cdr2.cdr
The last load was successful.
```

```
attr: h323-gw-id (65)
```

```
Totally 1 attrs defined.
```

```
!The output below is from a call that uses cdr1.cdr which allows only h323-call-origin.
```

```
debug radius accounting
```

```
Radius protocol debugging is on
```

```
Radius packet hex dump debugging is off
```

```
Radius packet protocol (authentication) debugging is off
```

```
Radius packet protocol (accounting) debugging is on
```

```
02:41:32: RADIUS/ENCODE(00000023): Unsupported AAA attribute timezone
02:41:32: RADIUS(00000023): Encoding nas-port...Only port-type avlbl
02:41:32: RADIUS(00000023): sending
02:41:32: RADIUS: Send to unknown id 26 10.6.20.70:1699, Accounting-Request, len
262
02:41:32: RADIUS: authenticator 84 6E A0 C0 0F 27 79 03 - 59 96 FC 6C F4 17 05
4D
02:41:32: RADIUS: Acct-Session-Id [44] 10 "00000023"
02:41:32: RADIUS: Vendor, Cisco [26] 56
02:41:32: RADIUS: Conf-Id [24] 50 "h323-conf-id=C925CD59 BF2B11D3
8038E483 89ADC43B"
02:41:32: RADIUS: Vendor, Cisco [26] 31
02:41:32: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
02:41:32: RADIUS: Vendor, Cisco [26] 65
02:41:32: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=C925CD59
BF2B11D3 8038E483 89ADC43B"
02:41:32: RADIUS: User-Name [1] 12 "4081234567"
02:41:32: RADIUS: Acct-Status-Type [40] 6 Start [1]
02:41:32: RADIUS: NAS-Port-Type [61] 6 Async [0]
02:41:32: RADIUS: Vendor, Cisco [26] 19
02:41:32: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
02:41:32: RADIUS: Calling-Station-Id [31] 12 "4081234567"
02:41:32: RADIUS: Called-Station-Id [30] 7 "12345"
02:41:32: RADIUS: Service-Type [6] 6 Login [1]
02:41:32: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
02:41:32: RADIUS: Delay-Time [41] 6 0
02:41:32: RADIUS: Received from id 26 10.6.20.70:1699, Accounting-response, len
20
02:41:32: RADIUS: authenticator 90 AD C8 09 60 D7 26 01 - DE E0 BC DC C1 F8 CA
2F
02:41:32: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4081234567
02:41:38: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4081234567
02:41:52: RADIUS(00000023): Encoding nas-port...Only port-type avlbl
02:41:59: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4081234567
, call lasted 26 seconds
02:41:59: RADIUS/ENCODE(00000023): Unsupported AAA attribute timezone
02:41:59: RADIUS(00000023): Encoding nas-port...Only port-type avlbl
02:41:59: RADIUS(00000023): sending
02:41:59: RADIUS: Send to unknown id 27 10.6.20.70:1699, Accounting-Request, len
327
02:41:59: RADIUS: authenticator 13 B7 10 EE 1C 55 7A D2 - 0F 4A A5 2F 1F 85 0E
3A
02:41:59: RADIUS: Acct-Session-Id [44] 10 "00000023"
02:41:59: RADIUS: Vendor, Cisco [26] 56
02:41:59: RADIUS: Conf-Id [24] 50 "h323-conf-id=C925CD59 BF2B11D3
8038E483 89ADC43B"
02:41:59: RADIUS: Vendor, Cisco [26] 31
02:41:59: RADIUS: h323-call-origin [26] 25 "h323-call-origin=answer"
02:41:59: RADIUS: Vendor, Cisco [26] 65
```

```

02:41:59: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=C925CD59
BF2B11D3 8038E483 89ADC43B"
02:41:59: RADIUS: Acct-Input-Octets [42] 6 0
02:41:59: RADIUS: Acct-Output-Octets [43] 6 121600
02:41:59: RADIUS: Acct-Input-Packets [47] 6 0
02:41:59: RADIUS: Acct-Output-Packets [48] 6 760
02:41:59: RADIUS: Acct-Session-Time [46] 6 27
02:41:59: RADIUS: Vendor, Cisco [26] 35
02:41:59: RADIUS: Cisco AVpair [1] 29 "h323-ivr-out=Tariff:Unknown"
02:41:59: RADIUS: User-Name [1] 12 "4081234567"
02:41:59: RADIUS: Acct-Status-Type [40] 6 Stop [2]
02:41:59: RADIUS: NAS-Port-Type [61] 6 Async [0]
02:41:59: RADIUS: Vendor, Cisco [26] 19
02:41:59: RADIUS: cisco-nas-port [2] 13 "ISDN 0:D:23"
02:41:59: RADIUS: Calling-Station-Id [31] 12 "4081234567"
02:41:59: RADIUS: Called-Station-Id [30] 7 "12345"
02:41:59: RADIUS: Service-Type [6] 6 Login [1]
02:41:59: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
02:41:59: RADIUS: Delay-Time [41] 6 0
02:41:59: RADIUS: Received from id 27 10.6.20.70:1699, Accounting-response, len
20
02:41:59: RADIUS: authenticator 7F B2 88 3A 4A 96 05 C6 - D5 81 19 D8 25 3B 4D CB

```

!The output below is from the **show debug** command.

show debug

Radius protocol debugging is on

Radius packet protocol (accounting) debugging is on

!The output below is from a call that uses cdr2 which allows h323-gw-id, but does not allow h323-call-origin.

```

RADIUS/ENCODE(00000025): Unsupported AAA attribute timezone
02:51:35: RADIUS(00000025): Encoding nas-port...Only port-type avlbl
02:51:35: RADIUS(00000025): sending
02:51:35: RADIUS: Send to unknown id 28 10.6.20.70:1709, Accounting-Request, len
265
02:51:35: RADIUS: authenticator 15 F0 7E AB 75 07 10 70 - 5E 3C 54 78 09 18 83
E5
02:51:35: RADIUS: Acct-Session-Id [44] 10 "00000025"
02:51:35: RADIUS: Vendor, Cisco [26] 34
02:51:35: RADIUS: h323-gw-id [33] 28 "h323-gw-id=router."
02:51:35: RADIUS: Vendor, Cisco [26] 56
02:51:35: RADIUS: Conf-Id [24] 50 "h323-conf-id=306F55DD BF2D11D3
803CE483 89ADC43B"
02:51:35: RADIUS: Vendor, Cisco [26] 65
02:51:35: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=306F55DD
BF2D11D3 803CE483 89ADC43B"
02:51:35: RADIUS: User-Name [1] 12 "4081234567"
02:51:35: RADIUS: Acct-Status-Type [40] 6 Start [1]
02:51:35: RADIUS: NAS-Port-Type [61] 6 Async [0]
02:51:35: RADIUS: Vendor, Cisco [26] 19
02:51:35: RADIUS: cisco-nas-port [2] 13 "ISDN 1:D:23"
02:51:35: RADIUS: Calling-Station-Id [31] 12 "4081234567"
02:51:35: RADIUS: Called-Station-Id [30] 7 "12346"
02:51:35: RADIUS: Service-Type [6] 6 Login [1]
02:51:35: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
02:51:35: RADIUS: Delay-Time [41] 6 0
02:51:35: %ISDN-6-CONNECT: Interface Serial1:22 is now connected to 4081234567
02:51:35: RADIUS: Received from id 28 10.6.20.70:1709, Accounting-response, len
20
02:51:35: RADIUS: authenticator D3 D8 59 42 2B 48 96 8D - 5E 2E D8 61 9A 9D 0D
5F
02:51:41: %ISDN-6-CONNECT: Interface Serial1:22 is now connected to 4081234567
02:51:43: %ISDN-6-DISCONNECT: Interface Serial1:22 disconnected from 4081234567

```

```

, call lasted 8 seconds
02:51:43: RADIUS/ENCODE(00000025): Unsupported AAA attribute timezone
02:51:43: RADIUS(00000025): Encoding nas-port...Only port-type avlbl
02:51:43: RADIUS(00000025): sending
02:51:43: RADIUS: Send to unknown id 29 10.6.20.70:1709, Accounting-Request, len
330
02:51:43: RADIUS: authenticator 55 35 AB CC 20 64 69 4B - 3F EE 79 04 11 E8 AE
4F
02:51:43: RADIUS: Acct-Session-Id [44] 10 "00000025"
02:51:43: RADIUS: Vendor, Cisco [26] 34
02:51:43: RADIUS: h323-gw-id [33] 28 "h323-gw-id=router."
02:51:43: RADIUS: Vendor, Cisco [26] 56
02:51:43: RADIUS: Conf-Id [24] 50 "h323-conf-id=306F55DD BF2D11D3
803CE483 89ADC43B"
02:51:43: RADIUS: Vendor, Cisco [26] 65
02:51:43: RADIUS: Cisco AVpair [1] 59 "h323-incoming-conf-id=306F55DD
BF2D11D3 803CE483 89ADC43B"
02:51:43: RADIUS: Acct-Input-Octets [42] 6 0
02:51:43: RADIUS: Acct-Output-Octets [43] 6 50240
02:51:43: RADIUS: Acct-Input-Packets [47] 6 0
02:51:43: RADIUS: Acct-Output-Packets [48] 6 314
02:51:43: RADIUS: Acct-Session-Time [46] 6 8
02:51:43: RADIUS: Vendor, Cisco [26] 35
02:51:43: RADIUS: Cisco AVpair [1] 29 "h323-ivr-out=Tariff:Unknown"
02:51:43: RADIUS: User-Name [1] 12 "4081234567"
02:51:43: RADIUS: Acct-Status-Type [40] 6 Stop [2]
02:51:43: RADIUS: NAS-Port-Type [61] 6 Async [0]
02:51:43: RADIUS: Vendor, Cisco [26] 19
02:51:43: RADIUS: cisco-nas-port [2] 13 "ISDN 1:D:23"
02:51:43: RADIUS: Calling-Station-Id [31] 12 "4081234567"
02:51:43: RADIUS: Called-Station-Id [30] 7 "12346"
02:51:43: RADIUS: Service-Type [6] 6 Login [1]
02:51:43: RADIUS: NAS-IP-Address [4] 6 10.5.20.100
02:51:43: RADIUS: Delay-Time [41] 6 0
02:51:43: RADIUS: Received from id 29 10.6.20.70:1709, Accounting-response, len
20
02:51:43: RADIUS: authenticator 45 31 ED 45 F4 06 ED 54 - 5E 6F 83 64 4D 2D 34
90

```

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.



ASCII Table

ASCII Table

Table 1 Prompt Name for ASCII Characters

Value (Hex)	Character	Name	Value (Hex)	Character	Name
20		Space	21	!	Exclamation mark
22	“	Double quote	23	#	Pound
24	\$	Dollar	25	%	Percent
26	&	Ampersand	27	‘	Right single quote
28	(Left parenthesis	29)	Right parenthesis
2A	*	Astrick	2B	+	Plus
2C	,	Comma	2D	-	Hyphen
2E	.	Dot	2F	/	Slash
30	0	Zero	31	1	One
32	2	Two	33	3	Three
34	4	Four	35	5	Five
36	6	Six	37	7	Seven
38	8	Eight	39	9	Nine
3A	:	Colon	3B	;	Semi-colon
3C	<	Less than	3D	=	Equal
3E	>	Greater than	3F	?	Question mark
40	@	at	41	A	a
42	B	b	43	C	c
44	D	d	45	E	e



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

© 2007 Cisco Systems, Inc. All rights reserved.

Table 1 Prompt Name for ASCII Characters (continued)

Value (Hex)	Character	Name	Value (Hex)	Character	Name
46	F	f	47	G	g
48	H	h	49	I	i
4A	J	j	4B	K	k
4C	L	l	4D	M	m
4E	N	n	4F	O	o
50	P	p	51	Q	q
52	R	r	53	S	s
54	T	t	55	U	u
56	V	v	57	W	w
58	X	x	59	Y	y
5A	Z	z	5B	[Left bracket
5C	\	Backslash	5D]	Right bracket
5E	^	Caret	5F	_	Underscore
60	'	Left single quote	61	a	a
62	b	b	63	c	c
64	d	d	65	e	e
66	f	f	67	g	g
68	h	h	69	i	i
6A	j	j	6B	k	k
6C	l	l	6D	m	m
6E	n	n	6F	o	o
70	p	p	71	q	q
72	r	r	73	s	s
74	t	t	75	u	u
76	v	v	77	w	w
78	x	x	79	y	y
7A	z	z	7B	{	Left brace
7C		Pipe	7D	}	Right brace
7E	~	Tilde			

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.



GLOSSARY

A

- AAA** Authentication, Authorization, and Accounting. AAA is a suite of network security services that provides the primary framework through which you can set up access control on your Cisco router or gateway.
- ANI** Automatic number identification. Same as calling party.

D

- DNIS** Dialed number identification service. Same as the called number.

G

- gatekeeper** A gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper. An H.323 gateway is an endpoint on the LAN that provides real-time, two-way communications between H.323 terminals on the LAN and other ITU-T terminals in the WAN or to another H.323 gateway.
- gateway** A gateway allows H.323 terminals to communicate with non-H.323 terminals by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

I

- IFS** Cisco IOS file system.
- IVR** Interactive voice response. When someone dials in, IVR responds with a prompt to get a personal identification number (PIN), and so on.



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

© 2007 Cisco Systems, Inc. All rights reserved.

P

POTS Plain old telephone service. Basic telephone service supplying standard single line telephones, telephone lines, and access to the PSTN.

PSTN Public Switched Telephone Network. PSTN refers to the local telephone company.

V

VoIP Voice over IP. The ability to carry normal telephone-style voice signals over an IP-based network with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco open standards-based (for example, H.323) approach to IP voice traffic.

For a list of networking terms and acronyms, refer to *Internetworking Terms and Acronyms*.

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.