Cisco IOS XE Access Node Control Protocol Configuration Guide

Release 2

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

Cisco IOS XE Access Node Control Protocol Configuration Guide

About Cisco IOS XE Software Documentation

Last Updated: December 1, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS XE software 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

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

Audience

The Cisco IOS XE 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 XE documentation set is also intended for those users experienced with Cisco IOS XE software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS XE release.

Documentation Conventions

In Cisco IOS XE 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 XE 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 contains the following topics:

Typographic Conventions

Cisco IOS XE 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.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS XE documentation uses the following command syntax conventions:

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

Software Conventions

Cisco IOS XE software uses the following conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold 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 the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Cisco IOS XE documentation 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 XE documentation set, how it is organized, and how to access it on Cisco.com. Listed are configuration guides, command references, and supplementary references and resources that comprise the documentation set.

Cisco IOS XE Documentation Set

The Cisco IOS XE documentation set 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 XE software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS XE release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS XE features.
  - Command references—Alphabetical compilations of command pages that provide detailed information about the commands used in the Cisco IOS XE features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS XE releases and that is updated at each standard release.
- Command reference book for **debug** commands.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Reference book for system messages for all Cisco IOS XE releases.

Cisco IOS XE 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 Cisco IOS XE 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.

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

Cisco IOS XE Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page x.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The command references contain commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The command references support many different software releases and platforms. Your Cisco IOS XE software release or platform may not support all these technologies.

Table 2 lists documents and resources that supplement the Cisco IOS XE 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.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

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

Table 1 Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide*	Configuration and troubleshooting of SPA interface processors (SIPs) and shared port adapters (SPAs) that are supported on the Cisco ASR 1000 Series Router.
• *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*	Overview of software functionality that is specific to the Cisco ASR 1000 Series Aggregation Services Routers.
• *Cisco IOS XE Access Node Control Protocol Configuration Guide* • *Cisco IOS Access Node Control Protocol Command Reference*	Communication protocol between digital subscriber line access multiplexers (DSLAMs) and a broadband remote access server (BRAS).
• *Cisco IOS XE Asynchronous Transfer Mode Configuration Guide* • *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
• *Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over Ethernet (PPPoE).
• *Cisco IOS XE Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	IEEE 802.3ad Link Bundling; Link Aggregation Control Protocol (LACP) support for Ethernet and Gigabit Ethernet links and EtherChannel bundles; LACP support for stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles; and IEEE 802.3ad Link Aggregation MIB.
• *Cisco IOS XE Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	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.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS XE DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS XE Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS XE High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	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.
• *Cisco IOS XE Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS XE Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS XE IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	IP addressing, Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
• *Cisco IOS XE IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
• *Cisco IOS XE IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	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).
• *Cisco IOS XE IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS XE IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS XE IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS XE IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS XE IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS XE IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS XE IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS XE IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS XE IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS XE IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding.
• *Cisco IOS XE IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For a list of IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-roadmap_xe.html
• *Cisco IOS XE ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).
• *Cisco IOS XE LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs and multilayer switching (MLS).
• *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
• *Cisco IOS XE NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.
• *Cisco IOS XE Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	Basic system management, system monitoring and logging, Cisco IOS Scripting with Tool Control Language (Tcl), Cisco networking services (CNS), Embedded Event Manager (EEM), Embedded Syslog Manager (ESM), HTTP, Remote Monitoring (RMON), and SNMP.
• *Cisco IOS XE Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS XE Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), Network-Based Application Recognition (NBAR), priority queueing, Multilink PPP (MLP) for QoS, header compression, Resource Reservation Protocol (RSVP), weighted fair queueing (WFQ), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; public key infrastructure (PKI); RADIUS; and TACACS+.
• *Cisco IOS XE Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; security for VPNs with IPsec; VPN availability features (reverse route injection, IPsec preferred peer, and real-time resolution for the IPsec tunnel peer); IPsec data plane features; IPsec management plane features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; and Cisco Group Encrypted Transport VPN (GET VPN).
• *Cisco IOS XE Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS XE Security Configuration Guide: Securing User Services*	AAA (includes Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS XE Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS XE VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	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, and tunnel authentication via RADIUS on tunnel terminator.
• *Cisco IOS XE Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; L2VPN Pseudowire Redundancy; and Media-Independent PPP and Multilink PPP.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco Unified Border Element (Enterprise) Configuration Guide* • *Cisco IOS Voice Command Reference*	The Cisco Unified Border Element (Enterprise) on the Cisco ASR 1000 brings a scalable option for enterprise customers. Running as a process on the Cisco ASR 1000 and utilizing the high-speed RTP packet processing path, the Cisco Unified Border Element (Enterprise) is used as an IP-to-IP gateway by enterprises and commercial customers to interconnect SIP and H.323 voice and video networks. The Cisco UBE (Enterprise) provides a network-to-network demarcation interface for signaling interworking, media interworking, address and port translations, billing, security, quality of service (QoS), and bandwidth management.
• *Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model* • *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model*	The Cisco Unified Border Element (SP Edition) is a session border controller (SBC) that is VoIP-enabled and deployed at the edge of networks. For Cisco IOS XE Release 2.3 and earlier releases, Cisco Unified Border Element (SP Edition) is supported only in the distributed mode. Operating in the distributed mode, the SBC is a toolkit of functions that can be used to deploy and manage VoIP services, such as signaling interworking, network hiding, security, and quality of service.
• *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* • *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*	The Cisco Unified Border Element (SP Edition) is a highly scalable, carrier-grade session border controller (SBC) that is designed for service providers and that is generally deployed at the border of the enterprise or SP networks to enable the easy deployment and management of VoIP services. Cisco Unified Border Element (SP Edition) is integrated into Cisco routing platforms and can use a large number of router functions to provide a very feature-rich and intelligent SBC application. Formerly known as Integrated Session Border Controller, Cisco Unified Border Element (SP Edition) provides a network-to-network demarcation interface for signaling interworking, media interworking, address and port translations, billing, security, quality of service, call admission control, and bandwidth management. For Cisco IOS XE Release 2.4 and later releases, Cisco Unified Border Element (SP Edition) can operate in two modes or deployment models: unified and distributed. The configuration guide documents the features in the unified mode.

Table 2 lists documents and resources that supplement the Cisco IOS XE software configuration guides and command references.

Table 2 Cisco IOS XE Software Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS XE software releases.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Cisco IOS XE system messages	List of Cisco IOS XE system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or the system software.
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 XE software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS XE software 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 XE 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 updated 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 XE software technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Using the Command-Line Interface in Cisco IOS XE Software

Last Updated: December 1, 2009

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

For more information about using the CLI, see "Part 1: Using the Cisco IOS Command-Line Interface (CLI)" of the *Cisco IOS XE Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About 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/go/techdocs.

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 settings that you can change on a console port or 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 ASR 1000 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

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.	• 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.	• 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.	• 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	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS XE process or processes fail, in most scenarios the router will reload. • 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)#`	If a Cisco IOS XE process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS XE CLI. 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.	• Inspect various states on the router, including the Cisco IOS XE state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS XE software or other processes. • Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or 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.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	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
```

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 command history feature saves the commands that 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 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 **vrrp** as a keyword in addition to **version**.

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** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

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 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. You can use output modifiers to filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **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 *System Messages for Cisco IOS XE* document.

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

- "Part 1: Using the Cisco IOS Command-Line Interface (CLI)" of the *Cisco IOS XE Configuration Fundamentals Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/ios_xe/fundamentals/configuration/guide/2_xe/cf_xe_book.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html
- Cisco Product Support Resources

  http://www.cisco.com/go/techdocs
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS XE software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS XE 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\

Access Node Control Protocol

First Published: June 25, 2009
Last Updated: June 25, 2009

The Access Node Control Protocol feature enhances communication between Digital Subscriber Line Access Multiplexers (DSLAMs) and a broadband remote access server (BRAS), enabling the exchange of events, actions, and information requests between the multiplexer end and the server end. As a result, either end can implement appropriate actions.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Access Node Control Protocol" section on page 15.

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

Contents

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

Prerequisites for Access Node Control Protocol

To run Access Node Control Protocol (ANCP) over Transmission Control Protocol (TCP), IP must be enabled on broadband remote access servers (BRAS). Interactions from RADIUS to the BRAS are not required for ANCP and are dependent on the RADIUS server.

For information about release and platform support, see the "Feature Information for Access Node Control Protocol" section on page 15.

Restrictions for Access Node Control Protocol

Cisco IOS XE Release 2.4 supports interactions with the RADIUS server from the broadband remote access server (BRAS). Interactions from RADIUS to the BRAS are not required for ANCP and are dependent on the RADIUS server.

Information About Access Node Control Protocol

The Access Node Control Protocol (ANCP) is used to aggregate traffic from multiple subscribers and deliver information for any application, while remaining independent from the application. Currently, ANCP is used in the application between DSLAMs and the broadband remote access server in a digital subscriber line (DSL) broadband environment.

The ANCP feature enables close communication between DSL aggregation multiplexers (DSLAMs) and network edge devices. Using ANCP between DSLAMs and a BRAS enables exchange of events, actions, and information requests so that the appropriate actions occur at the DSLAM and BRAS.

The ANCP architecture supports the following uses of ANCP:

Rate Adaptive Mode

Rate adaptive mode helps to maximize the line bit rate for a given line, and the rate is dependent on the quality of the signal achieved on the line. Rate adaptive mode conveys DSL modem line rate from a DSLAM to a broadband remote access server.

A BRAS running ANCP listens for TCP requests from its ANCP neighbors (DSLAMs).

- After a TCP session is established—ANCP begins exchanging messages to establish adjacency between the BRAS and its neighbors.
- After adjacency is established—ANCP event messages can be sent from the DSLAM to the BRAS.

Rate adaptive DSL uses signal quality to adjust line speeds. A BRAS typically sets the subscriber interfaces to the maximum bandwidth agreed to in the service license agreement (SLA).

When customer premises equipment (CPE) is synchronized to a data rate that is lower than the line speed, cell or packet loss occurs on the DSLAM. To prevent this, the DSLAM can use ANCP to notify the BRAS of newly adjusted circuit rates.

When a customer-facing port:

- Activates — The DSLAM sends a Port Up message to the BRAS. The appropriate quality of service (QoS) takes effect in accordance with the ANCP-delivered information.
- Deactivates — The DSLAM sends a Port Down message to the BRAS. ANCP reports the DSL state sent by the DSLAM, which is typically Silent or Idle. If the broadband remote access server receives another Port Up message, the subscriber sessions either time out or are renewed with a new shaping rate. The shaping rate on the interface does not change until the router receives a new Port Up message.

RADIUS Interaction

Interactions between the broadband remote access server and the RADIUS server are from the router to RADIUS.

The BRAS sends the following attributes and attribute-value pairs (AVPs) to the RADIUS server:

ANCP Line Rates	Upstream Data Rate	Downstream Data Rate	Output Policy Name
VSA 39	Attribute 197, Ascend-Data-Rate	Attribute 255, Ascend-Xmit-Rate	Attribute 77, Connect-Speed-Info
	Attribute Type 38, Rx Connect Speed AVP	Attribute Type 24, Tx Connect Speed AVP	

The BRAS uses Point-to-Point Protocol (PPPoE) to interact with the authentication, authorization, and accounting (AAA) module. RADIUS processes the information and then takes appropriate action.

Port Mapping

Port mapping associates customer premises equipment (CPE) clients of a DSLAM with VLAN subinterfaces on the BRAS. The VLANs include 802.1Q or queue-in-queue (Q-in-Q) hierarchical VLANs. Port mapping is configured in global configuration mode on the BRAS by grouping CPE client IDs with a specific DSLAM neighbor.

There are two methods you can use to map ports: configure all VLAN subinterfaces first, and the ANCP neighbor mappings next. Or, you can configure the mappings directly under the interface.

For example, the following commands configure port mapping for Q-in-Q VLAN subinterfaces:

```
ancp neighbor name dslam-name id dslam-id
    dot1q outer-vlanid second-dot1q inner-vlanid [interface type number] client-id
    “client-id”
```

or

```
ancp neighbor name dslam-name id dslam-id
    dot1q outer-vlanid client-id “client-id”
```

The *client-id* is a unique access-loop-circuit-id that the DSLAM sends to the BRAS for each unique port. The DSLAM sends this ID in the ANCP Port Up event message. The access-loop-circuit-id uses a defined format consisting of an access node identifier and digital subscriber line (DSL) information as mentioned below:

ATM/DSL

“*access-node-identifier* **atm** *slot/module/port*.*subinterface*:*vpi*.*vci***”**

Ethernet/DSL

"*access-node-identifier* **ethernet** *slot/module/port.subinterface*[**:***vlan-id*]**"**

The BRAS sets the default state as Down, on all ports of the router, until the DSLAM sends a Port Up message.

Noninteractive Operation, Administration, and Maintenance

ANCP provides an out-of-band control channel for performing noninteractive operation, administration, and maintenance (OAM) operations from the broadband remote access server. This channel enables router operators to view the ANCP port state of specific DSLAM ports. ANCP port state information is stored in the ANCP dynamic database on the BRAS.

Interactive OAM

The Interactive OAM and Scaling Improvements feature adds on-demand ping capability to ANCP for operations and troubleshooting.

Note This feature is enabled by default and requires no configuration.

General Switch Management Protocol and ANCP

ANCP is an extension of the General Switch Management Protocol (GSMP). GSMP defines a master-slave neighbor relationship in which the master initiates a connection to a slave. In ANCP, this master-slave relationship is reversed—the BRAS (master) listens and accepts incoming ANCP connections from the DSLAM (slave). The DSLAM uses event messages to communicate asynchronous events to the BRAS, such as topology changes and Port Down or Port Up events.

GSMP connectivity between the BRAS and the DSLAM occurs over TCP/IP (RFC 3293). The DSLAM initiates the connection to the router and the router accepts the connection if the appropriate interface is ANCP enabled.

The GSMP Adjacency Protocol establishes GSMP neighbor relationships.

1. During the adjacency-building:
   a. The DSLAM and router negotiate their capabilities and determine the synchronization state between the two ends.
   b. GSMP detects whether the router and the DSLAM have retained a local information database state in case of a transport failure, or whether both devices require a state update.
   c. If GSMP determines that it must resynchronize the adjacency, it restarts the adjacency synchronization process, which includes the capability negotiation defined in the ANCP extension draft available at:

http://www.ietf.org/internet-drafts/draft-wadhwa-gsmp-l2control-configuration-00.txt

2. In an ANCP, if a neighbor (neighbor1) contains capabilities that its neighbor (neighbor2) does not support, neighbor1 turns off the capabilities and recommunicates the packets to neighbor2 with the same set of capabilities as neighbor2.
3. After both the neighbors agree to the same set of capabilities, adjacency is established.

How to Configure Access Node Control Protocol

To configure ANCP, perform the following global or subinterface configuration tasks:

Enabling ANCP on an Ethernet Interface

Use the following procedure to enable ANCP on an Ethernet interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **interface** *type number.subinterface*
6. **encapsulation dot1q** [*vlanid*] [**second-dot1q** *second-vlanid*]
7. **ancp enable**
8. **end**
9. **ancp adjacency timer** *interval*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface type number`
	
	Example:
	`Router(config)# interface FastEthernet1/0/0`
		Creates or modifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 10.16.1.2 255.255.0.0`	Assigns an IP address and subnet mask to the interface.
Step 5	**interface** *type number.subinterface* **Example:** `Router(config-if)# interface FastEthernet1/0/0.1`	Creates or modifies a subinterface. Enters subinterface configuration mode.
Step 6	**encapsulation dot1q** [*vlanid*] [**second-dot1q** *second-vlanid*] **Example:** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	Enables dot1q VLAN encapsulation on the subinterface for a single-queue 802.1Q VLAN or for Q-in-Q hierarchical VLANs.
Step 7	**ancp enable** **Example:** `Router(config-subif)# ancp enable`	Enables ANCP on the interface where IP is configured.
Step 8	**end** **Example:** `Router(config-subif)# end`	Exits subinterface configuration mode.
Step 9	**ancp adjacency timer** *interval* **Example:** `Router(config)# ancp adjacency timer 100`	Sets the ANCP adjacency timer interval, which specifies the amount of time to wait before sending an ANCP hello packet to the DSLAM. Valid values are defined in units of 100 milliseconds (ms). Default: 100 (10 seconds)
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Enabling ANCP on an ATM Interface

The **ancp enable** command should be configured only for the control VCs on which the ancp message is sent from the DSLAM. Use the following procedure to enable ANCP on ATM interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface atm** *slot/subslot/port.subinterface*
5. **ip address** *ip-address mask*

6. **pvc** *vpi/vci*
7. **ancp enable**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ancp adjacency timer** *interval* **Example:** `Router(config)# ancp adjacency timer 100`	Sets the ANCP adjacency timer interval, which specifies the amount of time to wait before sending an ANCP hello packet to the DSLAM. • Valid values are defined in units of 100 milliseconds (ms). Default: 100 (10 seconds).
Step 4	**interface atm** *slot/subslot/port.subinterface* **Example:** `Router(config)# interface atm 2/0/1.1`	Creates or modifies a subinterface and enters subinterface configuration mode.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-subif)# ip address 10.16.1.2 255.255.0.0`	Assigns an IP address and subnet mask to the subinterface.
Step 6	**pvc** *vpi/vci* **Example:** `Router(config-subif)# pvc 2/100`	Enables an ANCP connection over ATM PVC and enters ATM virtual circuit configuration mode.
Step 7	**ancp enable** **Example:** `Router(config-if-atm-vc)# ancp enable`	Enables ANCP on the interface where IP is configured.
Step 8	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode.

Mapping DSLAM Ports to VLAN Interfaces on Broadband Remote Access Servers

Use the following procedure to map DSLAM ports to VLAN interfaces on the BRAS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface** *type number*
5. **encapsulation dot1q** *vlan-id*
6. **ancp neighbor name** *dslam-name* **id** *dslam-id* **client-id** *client-id*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ancp atm shaper percent-factor** *factor* **Example:** `Router(config)# ancp shaper percent-factor 95`	Enables ANCP cell tax accounting for ATM U-interface connections
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/0.1`	Enters interface configuration mode for the specified subinterface.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if)# encapsulation dot1q 411`	Enables IEEE 802.1Q encapsulation of traffic on a specified VLAN.

	Command or Action	Purpose
Step 6	**ancp neighbor name** *dslam-name* **id** *dslam-id* **client-id** *client-id* **Example:** `Router(config-if)# ancp neighbor name dslam1 id 1.2.3.4 client-id “1.2.3.4. eth 0/0.1“`	Specifies the ANCP access DSLAM to which VLAN subinterfaces are mapped.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Mapping DSLAM Ports to PVC Interfaces on Broadband Remote Access Servers

The **ancp neighbor name** command is available under **pvc** and **pvc-in-range** command modes. This command creates a one-to-one mapping between a PVC and a DSLAM port. Use the following procedure to map DSLAM ports to PVC interfaces on the BRAS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface atm** *slot/subslot/port.subinterface*
5. **pvc** *vpi/vci*
   or
   range pvc *start-vpi/start-vci end-vpi/end-vci*
6. (Optional) **pvc-in-range** *vpi/vci*
7. **ancp neighbor name** *dslam-name* **id** *dslam-id* **client-id** *client-id*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your **password**.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ancp atm shaper percent-factor** *factor* **Example:** `Router(config)# ancp shaper percent-factor 95`	Enables ANCP cell tax accounting for ATM U-interface connections
Step 4	**interface atm** *slot/subslot/port.subinterface* **Example:** `Router(config)# interface atm 2/0/1.1`	Enters interface configuration mode for the specified ATM subinterface.

Step 5	**pvc** *vpi/vci*
	
	or
	
	range pvc *start-vpi/start-vci end-vpi/end-vci*
	
	Example:
	`Router(config-subif)# pvc 1/101`
	
	or
	
	Example:
	`Router(config-subif)# range pvc 9/100 9/102`
		Creates a one-to-one mapping between a PVC and DSLAM port and enters ATM virtual circuit configuration mode.
		
		or
		
		Defines a range of ATM PVCs and enters PVC range configuration mode.
		
		• If a range of ATM PVCs are defined, use the **pvc-in-range** command to configure an individual PVC.

Step 6	**pvc-in-range** *vpi/vci* **Example:** `Router(config-if-atm-range-pvc)# pvc-in-range 9/100`	(Optional) Configures an individual PVC within a range in PVC range configuration mode.
Step 7	**ancp neighbor name** *dslam-name* **id** *dslam-id* **client-id** *client-id* **Example:** `Router(config-if-atm-range-pvc)# ancp neighbor name dslam1 id 1.2.3.4 client-id “1.2.3.4. atm0/0.1“`	Specifies the ANCP access DSLAM to which PVC subinterfaces are mapped. • This command is available under PVC range and ATM virtual circuit configuration modes.
Step 8	**end** **Example:** `Router(config-if-atm-range-pvc)# end`	Exits PVC range configuration mode.

Configuration Examples for Access Node Control Protocol

This section provides the following configuration examples:

- Enabling Access Node Control Protocol on Ethernet Interfaces: Example, page 11
- Enabling Access Node Control Protocol on ATM Interfaces: Example, page 11
- Mapping DSLAM Ports to VLAN Interfaces on the BRAS: Example, page 11

- Mapping DSLAM Ports to PVC Interfaces on the BRAS: Example, page 12

Enabling Access Node Control Protocol on Ethernet Interfaces: Example

The following example shows how to enable ANCP on an Ethernet subinterface. In the example, ANCP is enabled on Gigabit Ethernet subinterface 2/0/1.1.

```
interface GigabitEthernet 2/0/1
    ip address 192.168.64.16 255.255.255.0
    ancp enable
!
interface GigabitEthernet 2/0/1.1
    encapsulation dot1q 100 second-dot1q 200

ancp adjacency timer 100
```

Enabling Access Node Control Protocol on ATM Interfaces: Example

The following example shows how to enable ANCP on an ATM subinterface. In the example, ANCP is enabled on ATM subinterface 2/0/1.1.

```
interface ATM2/0/0.1 point-to-point
          description ANCP Link to one DSLAM
          no ip mroute-cache
          ip address 192.168.0.2 255.255.255.252
          pvc 254/32
                protocol ip 192.168.0.1
                ancp enable
                no snmp trap link-status
          !
```

Mapping DSLAM Ports to VLAN Interfaces on the BRAS: Example

The following example shows how to map CPE client ports of a DSLAM to Q-in-Q VLAN subinterfaces on the BRAS. In the example, the DSLAM neighbor named dslam1 with an IP address of 192.68.10.5 has a CPE client port mapped to Q-in-Q VLANs 100 and 200 configured on Ethernet interface 1/0/0.2. Another CPE client port is mapped to Q-in-Q VLANs 100 and 100 configured on Ethernet interface 1/0/0.1.

```
interface GigabitEthernet1/0/0.1
     encapsulation dot1q 100 second-dot1q 100
    ancp neighbor name dslam1 id 192.168.10.5 192.168.10.5 ethernet1/0/0.2

!
interface GigabitEthernet1/0/0.2
     encapsulation dot1q 100 second-dot1q 200
    ancp neighbor name dslam1 id 192.168.10.5 192.168.10.5 ethernet1/0/0.1
!
ancp atm shaper percent-factor 95
!
```

The example shown above maps the ports directly at the subinterface level. You can also configure all VLAN subinterfaces first, and perform the mappings under ANCP neighbor next. The following example shows this configuration:

```
interface GigabitEthernet1/0/0.1
     encapsulation dot1q 100 second-dot1q 100
```

```
!
interface GigabitEthernet1/0/0.2
     encapsulation dot1q 100 second-dot1q 200
!
ancp atm shaper percent-factor 95
!
ancp neighbor name dslam1 id 192.168.10.5
    dot1q 100 second-dot1q 200 interface GigabitEthernet1/0/0.1 client-id “192.168.10.5
    ethernet1/0/0.2”
!
ancp neighbor name dslam1 id 192.168.10.5
    dot1q 100 second-dot1q 200 interface GigabitEthernet1/0/0.2 client-id “192.168.10.5
    ethernet1/0/0.2”
```

Mapping DSLAM Ports to PVC Interfaces on the BRAS: Example

The **ancp neighbor name** command specifies how to map CPE client ports of a DSLAM to PVC interfaces on the BRAS. This command can be configured either globally or under PVC/PVC-in-Range mode.

In PVC or PVC-in-Range Configuration Mode

In this example, the router interfaces with one DSLAM which has 2 ports or clients, namely, port *x* and port *y*.

```
interface ATM2/0/0.1 point-to-point
          description ANCP Link to one DSLAM
          no ip mroute-cache
          ip address 192.168.0.2 255.255.255.252
          pvc 254/32
                protocol ip 192.168.0.1 255.255.255.252
                ancp neighbor name <dslam name1> id <dslam 1 id> client-id
       “dslam-port-x-identifier”
                no snmp trap link-status
          !
interface ATM1/0/0.1 multipoint
           description TDSL clients - default TDSL 1024
           class-int speed:ubr:1184:160:10
           range pvc 10/41 10/160
                 service-policy input SET-PRECEDENCE-0
                 service-policy output premium-plus:l2c:25088
                 pvc-in-range 10/103
                   description TDSL client 16 Mbps with ANCP
                   class-vc speed:ubr:17696:1184:05
                   ancp neighbor name <dslam name1> id <dslam 1 id> client-id
       “dslam-port-x-identifier”
              !
range pvc 11/41 11/160
            service-policy input SET-PRECEDENCE-0
            service-policy output premium-plus:l2c:25088
                 pvc-in-range 11/108
                   description TDSL client 16 Mbps with ANCP
                   class-vc speed:ubr:17696:1184:05
                   ancp neighbor name <dslam name1> id <dslam 1 id> client-id
       “dslam-port-y-identifier”
                !
          !
!
```

In Global Configuration Mode

When the **ancp neighbor** command is configured globally, the PVC information for the ATM interface must also be specified. The following is an example of the CLI when the **ancp neighbor** command is globally configured:

```
interface ATM1/0/0.1 multipoint
    description TDSL clients - default TDSL 1024
    class-int speed:ubr:1184:160:10
    range pvc 10/41 10/160
        service-policy input SET-PRECEDENCE-0
        service-policy output premium-plus:l2c:25088
        pvc-in-range 10/103
    description TDSL client 16 Mbps with ANCP
    class-vc speed:ubr:17696:1184:05
!
    range pvc 11/41 11/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 11/108
        description TDSL client 16 Mbps with ANCP
        class-vc speed:ubr:17696:1184:05
        !
    !
    ancp neighbor name <dslam name1> id <dslam 1 id>
        atm 10/103 interface ATM1/0/0.1 client-id “dslam-port-x-identifier”
        atm 11/108 interface ATM1/0/0.1 client-id “dslam-port-y-identifier”
```

Additional References

The following sections provide references related to the Access Node Control Protocol feature.

Related Documents

Related Topic	Document Title
IEEE 802.1Q VLAN	*Cisco IOS IEEE 802.1Q Support*, Release 12.0(1)T
Access Node Control Protocol	*Metro Ethernet WAN Services and Architectures* (white paper), Access Node Control Protocol
Queue-in-Queue VLAN Tags	*IEEE 802.1Q-in-Q VLAN Tag Termination*, Release 12.3T
ANCP Commands	Cisco IOS Access Node Control Protocol Command Reference

RFCs

RFC	Title
ANCP extension draft	GSMP Extensions for Access Node Control Mechanism, Internet draft

RFC	Title
RFC 3292	*General Switch Management Protocol (GSMP) V3*
RFC 3293	*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Access Node Control Protocol

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for Access Node Control Protocol

Feature Name	Releases	Feature Information
Access Node Control Protocol	Cisco IOS XE Release 2.4	In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000. The following sections provide information about this feature: • Information About Access Node Control Protocol, page 2 • How to Configure Access Node Control Protocol, page 5 The following command was introduced: **ancp vdsl ethernet shaper**.
Interactive OAM and Scaling Improvements	Cisco IOS XE Release 2.4	The Interactive OAM and Scaling Improvements feature adds on demand ping capability to ANCP for operations and troubleshooting. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000. The following commands were introduced or modified: **ping ancp**, **show ancp neighbor port**, **show ancp port**, **show ancp session**, **show ancp session adjacency**, **show ancp session event**, and **show ancp statistics**.

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

Multiservice Activation in Access-Accept Message

First Published: June 19, 2009
Last Updated: June 25, 2009

The Multiservice Activation in Access-Accept Message feature is part of Access Node Control Protocol (ANCP) and allows multiple services to be included in a single RADIUS Access-Accept message.This feature is similar to the Multiservice Activation and Deactivation in a Change of Authorization (CoA) Message feature, but in this case all requested service activations are processed automatically. This means that if a service activation fails, no further service activations are processed, and any service that has already been activated by the Access-Accept message is deactivated.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Multiservice Activation in Access-Accept Message" section on page 6.

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

Contents

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

Restrictions for Multiservice Activation in Access-Accept Message

- If one of the service activations fails, all unprocessed services from the Access-Accept message will be ignored, and any services from the Access-Accept message that have been activated will be deactivated.
- A two-stage application process exists when applying a quality of service (QoS) policy via a service in an Access-Accept message. The first stage involves parsing the policy and sending the policy value to the dataplane. The second stage involves the application of the QoS policy on the dataplane. In the instance where stage one is completed successfully, but stage two fails, the relevant service can indicate that the activation was successful.

Information About Multiservice Activation in Access-Accept Message

To configure multiservice activation in Access-Accept messages, you must understand the following concepts:

- Multiservice Activation in Access-Accept Message Overview, page 2
- QoS Policy for VSA 250, page 3

Multiservice Activation in Access-Accept Message Overview

An Access-Request message is sent by a RADIUS client to a RADIUS server to authenticate the user or subscriber profile included in the message. If the user or subscriber profile is:

- Acceptable—The RADIUS server may return an Access-Accept message
- Unacceptable—The RADIUS server may return an access-reject message

To enable multiservice activation, the Access-Accept message may include multiple Cisco generic VSA 250 (SSG_ACCOUNT_INFO) entries, with each VSA specifying a service name to be activated.

RSIM Format

```
vsa cisco generic 250 string "Aservice-name1"
vsa cisco generic 250 string "Aservice-name2"
vsa cisco generic 250 string "Aservice-name3"
```

RADIUS Format

```
07:06:23.234: RADIUS: Received from id 1645/36 11.12.13.2:1645, Access-Accept, len 112
07:06:23.238: RADIUS:  authenticator 92 C5 A2 F2 24 56 37 1E - 74 F4 C6 92 B0 E8 92 4C
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-1"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-2"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-3"
```

Upon receipt of the Access-Accept message, the specified services are extracted and each service is activated serially. If a service activation fails, all unprocessed services from the Access-Accept message are ignored, and any services from the Access-Accept message that have been activated are deactivated.

Note The RSIM format for Access-Accept multiple services requests for QoS services is not applicable for multiple service activation or deactivation requests in a CoA message. The format for CoA messages is VSA 252. For more information see Multiservice Activation and Deactivation in a CoA Message module

QoS Policy for VSA 250

You can use VSA 250 concatenated QoS syntax with the RADIUS Access-Accept message while establishing a session. The syntax parses the VSA concatenated string and activates the QoS and Intelligent Services Gateway (ISG) policy.

Note ISG manages multiple QoS services in one Access-Accept message and applies the message to activate static and parameterized QoS.

How to Configure Multiservice Activation in Access-Accept Message

This section contains the following procedures:

- Activating a Session Service Using Access-Accept, page 3 (optional)

Activating a Session Service Using Access-Accept

Configure Cisco VSA 250 in the service profile on RADIUS to dynamically activate a session service with Access-Accept. RADIUS uses VSA 250 in Access-Accept messages with the following syntax:

RSIM Format

```
vsa cisco generic 250 string
"Aservice-name-1"
```

Configuration Examples for Multiservice in Access-Accept Message

This section provides the following configuration example:

- Activating QoS Services Using VSA 250: Example, page 4

Activating QoS Services Using VSA 250: Example

To activate QoS Services, use the qos:vc-qos-policy-out syntax with the RADIUS Access-Accept message. The concatenated string is parsed and the QoS and ISG policy is activated.

The following example defines VSA 250 concatenated string parsing, and the activation of the ISG service and QoS policies:

qos:<qos-attribute-name>=<attribute value>[;qos:<qos-attribute-name>=<attribute value>…]

qos-attribute-name	Displays the QoS attribute name. The accepted attributes for the QoS attribute name in this special concatenated format are: vc-qos-policy-in vc-qos-policy-out vc-weight vc-watermark-min vc-watermark-max
attribute value	Displays the value to be assigned to the QoS attribute. The acceptable range of values are determined by the platform.

If the target session is an ATM VC, the vc-weight, vc-watermark-min, and vc-watermark-max attributes are interpreted.

The following example displays the concatenated QoS syntax for VSA 250:

```
vsa cisco generic 250 string
"Aqos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in”
```

Additional References

The following sections provide references related to the Multiservice Activation in Access-Accept Message feature.

Related Documents

Related Topic	Document Title
IEEE 802.1Q VLAN	*Cisco IOS IEEE 802.1Q Support*, Release 12.0(1)T feature module
Access-Node Control Protocol	*Metro Ethernet WAN Services and Architectures* (white paper), Access Node Control Protocol
Queue-in-Queue VLAN Tags	*IEEE 802.1Q-in-Q VLAN Tag Termination*, Release 12.3T
ANCP commands	*Cisco IOS Access Node Control Protocol Command Reference*

RFCs

RFC	Title
ANCP extension draft	GSMP Extensions for Access Node Control Mechanism, Internet draft
RFC 3292	*General Switch Management Protocol (GSMP) V3*
RFC 3293	*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Multiservice Activation in Access-Accept Message

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for Multiservice Activation in Access-Accept Message

Feature Name	Releases	Feature Information
Multiservice Activation in Access-Accept Message	Cisco IOS XE Release 2.4	The Multiservice Activation in Access-Accept Message feature supports dynamic activation of multiple services using RADIUS Access-Accept messages. In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Routers. The following command was modified by this feature: **subscriber service multiple-accept**.

Multiservice Activation and Deactivation in a CoA Message

First Published: June 25, 2009
Last Updated: June 25, 2009

This feature allows multiple services to be activated or deactivated by a single Change of Authorization (CoA) message sent from the policy server. This feature is similar to the Multiservice Activation in Access-Accept Message feature, but in this case it is assumed that the user session is already active.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Multiservice Activation and Deactivation in a CoA Message" section on page 7.

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

Contents

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

Restrictions for Multiservice Activation and Deactivation in a CoA Message

- All service names included in the multiservice activation or deactivation message must be Intelligent Services Gateway (ISG) aware. For example, they must be of type class-map type service "service1."
- If one of the services activation or deactivation messages fails, the broadband remote access server (BRAS) rolls back only the previous successfully activated or deactivated services and those that were included in the same multiservice activation or deactivation CoA message.
- However, the current ISG implementation has limitations in the process of reestablishing the state of previously activated or deactivated services. For example, if a feature that can overlap is enabled in the same session, the new, successfully activated or deactivated feature parameters delete the old parameters of the same feature, which was already activated in that session. Attempts to reestablish old parameters of that feature fail.
- If a valid CLI-configured ISG service is forwarded through CoA to a new session and fails (ISG service is unable to find an accounting list):
  - BRAS does not wait for the hardware to be provisioned.
  - An ACK message is relayed.
  - ISG services are not applied.
  - Tracebacks are observed.

Information About Multiservice Activation and Deactivation in a CoA Message

To configure multiservice activation or deactivation in a CoA message, you must understand the following concepts:

- Multiservice Activation and Deactivation in a CoA Message Overview, page 2
- QoS Policy for VSA 252, page 3

Multiservice Activation and Deactivation in a CoA Message Overview

The CoA multiservice activation or deactivation message contains a list of services. Multiple services are listed in the form of multiple lines in a VSA 252.

For the case of multiservice deactivation within one CoA message, the RADIUS server sends the request to deactivate multiple services within one CoA multiservice deactivation message. For each service listed in the multiservice deactivation message, the BRAS deactivates the service. Successful deactivation of the service is followed by an accounting-stop message.

If a service cannot be successfully deactivated, the BRAS aborts the deactivation of all subsequent services contained in the multiservice activation message. The BRAS activates all the services within the same multiservice activation message that were successfully deactivated before the failed service activated.

An existing VSA 252 is used to form one multiservice activation or deactivation CoA message. To form one multiservice activate or deactivate CoA message, multiple lines of VSA 252 are included in the message. The following example shows mixed multiservice activation or deactivation in one CoA message:

RADIUS Format

```
ISG#
00:41:15: RADIUS: CoA  received from id 76 10.168.1.6:1700, CoA Request, len 67
00:41:15: CoA: 10.168.1.6 request queued
00:41:15: RADIUS:  authenticator C4 AC 5D 50 6A BE D7 00 - F9 1D FA 38 15 32 25 3A
00:41:15: RADIUS:  Vendor, Cisco       [26]  18
00:41:15: RADIUS:   ssg-account-info   [250] 12  "S151.1.1.2"
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 31           [Service-Log-On service1]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 32           [Service-Log-On service2]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0C 73 65 72 76 69 63 65 33        [Service-Log-Off service3]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 34           [Service-Log-On service4]
```

QoS Policy for VSA 252

You can use VSA 252 concatenated quality of service (QoS) syntax in a RADIUS CoA message. The syntax is used to activate or deactivate ISG service and the QoS policy by parsing the VSA 252 concatenated string.

Note ISG manages multiple QoS services in one CoA message and applies the message to activate static and parameterized QoS.

How to Configure Multiservice Activation and Deactivation in a CoA Message

This section contains the following procedures:

- Activating a Session Service Using CoA, page 3 (optional)
- Deactivating a Session Service Using CoA, page 4 (optional)

Activating a Session Service Using CoA

Configure Cisco VSA 252 in the service profile on RADIUS to dynamically activate a session service with CoA. RADIUS uses VSA 252 in CoA messages with the following syntax:

```
vsa cisco generic 252 binary 0b suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

The CoA command in this example performs the following actions:

- Initiates an ISG service "qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;".
- Replaces the default QoS output child policy on virtual template IPOne_out and installs the IPOne_out policy if there is no default output child policy on the virtual template.
- Replaces the default QoS input child policy on virtual template IPOne_in and installs the IPOne_in policy if there is no default input child policy configured on the virtual template.

Deactivating a Session Service Using CoA

To dynamically activate a session service using CoA and default QoS policy on a virtual template, configure Cisco VSA 252 in the RADIUS service profile. RADIUS uses VSA 252 in CoA messages with the following syntax:

```
vsa cisco generic 252 binary 0c suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

The CoA command in this example performs the following actions:

- Terminates an ISG service "qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in".
- Replaces the QoS output child policy IPOne_out with the default child policy configured on the appropriate virtual template interface.
- Replaces the QoS input child policy IPOne_in with the default child policy configured on the appropriate virtual template interface.

Configuration Examples for Multiservice Activation and Deactivation in a CoA Message

This section provides the following configuration example:

- Activating and Deactivating QoS Services Using VSA 252: Example, page 4

Activating and Deactivating QoS Services Using VSA 252: Example

To activate QoS services, RADIUS adds one or more multiple QoS classes to the parent and child policy in one VSA 252 string and relays the following syntax:

```
CoA VSA 252 0b <new service>
```

In addition to the existing services, the new service should be installed and should not have overlapping classes with the current services.

The following example defines QoS activation and adds the QoS classes in the parameterized QoS service RADIUS form:

```
VSA252 0b
q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

To deactivate the second service, RADIUS relays the same VSA 252 string that was used for service activation, replacing “0b” with “0c”.

The following example defines QoS deactivation and deletes the QoS classes in the parameterized QoS service RADIUS form:

```
VSA252 0c
q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

Additional References

The following sections provide references related to the Multiservice Activation and Deactivation in a CoA Message feature.

Related Documents

Related Topic	Document Title
IEEE 802.1Q VLAN	*Cisco IOS IEEE 802.1Q Support*, Release 12.0(1)T feature module
Access Node Control Protocol	*Metro Ethernet WAN Services and Architectures* (white paper), Access Node Control Protocol
Queue-in-Queue VLAN Tags	*IEEE 802.1Q-in-Q VLAN Tag Termination*, Release 12.3T
ANCP Commands	Cisco IOS Access Node Control Protocol Command Reference

RFCs

RFC	Title
ANCP extension draft	GSMP Extensions for Access Node Control Mechanism, Internet draft
RFC 3292	*General Switch Management Protocol (GSMP) V3*
RFC 3293	*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Multiservice Activation and Deactivation in a CoA Message

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for Multiservice Activation and Deactivation in a CoA Message

Feature Name	Releases	Feature Information
ANCP Phase 2.5	Cisco IOS XE Release 2.4	The Multiservice Activation and Deactivation in a CoA Message feature supports dynamic activation and deactivation of multiple services using RADIUS CoA messages. In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Routers.
Multiservice Activation and Deactivation in a CoA Message	Cisco IOS XE Release 2.4	The Multiservice Activation and Deactivation in a CoA Message feature supports dynamic activation and deactivation of multiple services using RADIUS CoA messages. In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Routers.