



## **Cisco IOS XE Configuration Fundamentals 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

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

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

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

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

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynx, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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.

*Cisco IOS XE Configuration Fundamentals Configuration Guide*  
© 2009 Cisco Systems, Inc. All rights reserved.



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

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

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

## Command Syntax Conventions

Cisco IOS XE documentation uses the following command syntax conventions:

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

## Software Conventions

Cisco IOS 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.
<b>Bold Courier font</b>	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by 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, page iv](#)
- [Cisco IOS XE Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

## 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](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
<ul style="list-style-type: none"> <li><i>Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide</i></li> </ul>	Configuration and troubleshooting of SPA interface processors (SIPs) and shared port adapters (SPAs) that are supported on the Cisco ASR 1000 Series Router.
<ul style="list-style-type: none"> <li><i>Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</i></li> </ul>	Overview of software functionality that is specific to the Cisco ASR 1000 Series Aggregation Services Routers.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Access Node Control Protocol Configuration Guide</i></li> <li><i>Cisco IOS Access Node Control Protocol Command Reference</i></li> </ul>	Communication protocol between digital subscriber line access multiplexers (DSLAMs) and a broadband remote access server (BRAS).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Asynchronous Transfer Mode Configuration Guide</i></li> <li><i>Cisco IOS Asynchronous Transfer Mode Command Reference</i></li> </ul>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide</i></li> <li><i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i></li> </ul>	PPP over Ethernet (PPPoE).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Carrier Ethernet Configuration Guide</i></li> <li><i>Cisco IOS Carrier Ethernet Command Reference</i></li> </ul>	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.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i></li> <li><i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li><i>Cisco IOS XE DECnet Configuration Guide</i></li> <li><i>Cisco IOS DECnet Command Reference</i></li> </ul>	DECnet protocol.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Dial Technologies Configuration Guide</i></li> <li><i>Cisco IOS Dial Technologies Command Reference</i></li> </ul>	Asynchronous communications, dial backup, dialer technology, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE High Availability Configuration Guide</i></li> <li><i>Cisco IOS High Availability Command Reference</i></li> </ul>	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.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Intelligent Services Gateway Configuration Guide</i></li> <li><i>Cisco IOS Intelligent Services Gateway Command Reference</i></li> </ul>	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.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i></li> <li><i>Cisco IOS Interface and Hardware Component Command Reference</i></li> </ul>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Addressing Services Configuration Guide</i></li> <li><i>Cisco IOS IP Addressing Services Command Reference</i></li> </ul>	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).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Application Services Configuration Guide</i></li> <li><i>Cisco IOS IP Application Services Command Reference</i></li> </ul>	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).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Multicast Configuration Guide</i></li> <li><i>Cisco IOS IP Multicast Command Reference</i></li> </ul>	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).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Routing: BFD Configuration Guide</i></li> </ul>	Bidirectional forwarding detection (BFD).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Routing: BGP Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: BGP Command Reference</i></li> </ul>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Routing: EIGRP Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: EIGRP Command Reference</i></li> </ul>	Enhanced Interior Gateway Routing Protocol (EIGRP).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE IP Routing: ISIS Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: ISIS Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IP Routing: ODR Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: ODR Command Reference</i></li> </ul>	On-Demand Routing (ODR).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IP Routing: OSPF Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: OSPF Command Reference</i></li> </ul>	Open Shortest Path First (OSPF).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IP Routing: Protocol-Independent Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i></li> </ul>	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IP Routing: RIP Configuration Guide</i></li> <li>• <i>Cisco IOS IP Routing: RIP Command Reference</i></li> </ul>	Routing Information Protocol (RIP).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IP SLAs Configuration Guide</i></li> <li>• <i>Cisco IOS IP SLAs Command Reference</i></li> </ul>	Cisco IOS IP Service Level Agreements (IP SLAs).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IP Switching Configuration Guide</i></li> <li>• <i>Cisco IOS IP Switching Command Reference</i></li> </ul>	Cisco Express Forwarding.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE IPv6 Configuration Guide</i></li> <li>• <i>Cisco IOS IPv6 Command Reference</i></li> </ul>	For a list of IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: <a href="http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-roadmap_xe.html">http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-roadmap_xe.html</a>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE ISO CLNS Configuration Guide</i></li> <li>• <i>Cisco IOS ISO CLNS Command Reference</i></li> </ul>	ISO Connectionless Network Service (CLNS).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE LAN Switching Configuration Guide</i></li> <li>• <i>Cisco IOS LAN Switching Command Reference</i></li> </ul>	VLANs and multilayer switching (MLS).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i></li> <li>• <i>Cisco IOS Multiprotocol Label Switching Command Reference</i></li> </ul>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE NetFlow Configuration Guide</i></li> <li>• <i>Cisco IOS NetFlow Command Reference</i></li> </ul>	Network traffic data analysis, aggregation caches, and export features.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE Network Management Configuration Guide</i></li> <li>• <i>Cisco IOS Network Management Command Reference</i></li> </ul>	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.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS XE Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS Novell IPX Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i></li> <li><i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	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).
<ul style="list-style-type: none"> <li><i>Cisco IOS Security Command Reference</i></li> </ul>	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+.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Security Configuration Guide: Secure Connectivity</i></li> </ul>	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).
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Security Configuration Guide: Securing the Data Plane</i></li> </ul>	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.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Security Configuration Guide: Securing User Services</i></li> </ul>	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.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Service Advertisement Framework Configuration Guide</i></li> <li><i>Cisco IOS Service Advertisement Framework Command Reference</i></li> </ul>	Cisco Service Advertisement Framework.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE VPDN Configuration Guide</i></li> <li><i>Cisco IOS VPDN Command Reference</i></li> </ul>	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.
<ul style="list-style-type: none"> <li><i>Cisco IOS XE Wide-Area Networking Configuration Guide</i></li> <li><i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li>• <i>Cisco Unified Border Element (Enterprise) Configuration Guide</i></li> <li>• <i>Cisco IOS Voice Command Reference</i></li> </ul>	<p>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.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model</i></li> <li>• <i>Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model</i></li> </ul>	<p>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.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model</i></li> <li>• <i>Cisco Unified Border Element (SP Edition) Command Reference: Unified Model</i></li> </ul>	<p>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.</p> <p>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.</p>

[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
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS XE software releases.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of <b>debug</b> 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS XE documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>

## Additional Resources and Documentation Feedback

*What's New in Cisco Product Documentation* is 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

© 2009 Cisco Systems, Inc. All rights reserved.





# 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:

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

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

## Understanding Command Modes

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

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



**Table 1**     *CLI Command Modes*

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

**Table 1** CLI Command Modes (continued)

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

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

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

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

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

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



**Note**

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

## Using the Interactive Help Feature

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

**Table 2** CLI Interactive Help Commands

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

The following examples show how to use the help commands:

### **help**

```
Router> help
```

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

Two styles of help are provided:

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

### **?**

```
Router# ?
```

Exec commands:

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

<snip>

### ***partial command?***

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

zone zone-pair

### ***partial command<Tab>***

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

### ***command ?***

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

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

### ***command keyword ?***

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

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

<cr>

## Understanding Command Syntax

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

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

**Table 3**     *CLI Syntax Conventions*

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

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
WORD    domain name
```

```
Router(config)# ethernet cfm domain dname ?
level
```

```
Router(config)# ethernet cfm domain dname level ?
<0-7>   maintenance level number
```

```
Router(config)# ethernet cfm domain dname level 7 ?
<cr>
```

```
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>
```

```
Router(config)# logging host ?
Hostname or A.B.C.D  IP address of the syslog server
ipv6                 Configure IPv6 syslog server
```

## Understanding Enable and Enable Secret Passwords

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

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

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

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



### Note

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

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

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

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

## Using the Command History Feature

The 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 **vrp** 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
<b>h</b>	help
<b>lo</b>	logout
<b>p</b>	ping
<b>s</b>	show
<b>u</b> or <b>un</b>	undebug
<b>w</b>	where

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

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

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

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

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

## Using the no and default Forms of Commands

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

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

The **no** 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](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](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](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/cgi-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

<http://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

© 2009 Cisco Systems, Inc. All rights reserved.





## **Using the Cisco IOS Command-Line Interface (CLI)**





# Show Command Output Redirection

---

**Last Updated: May 4, 2009**

This feature adds the capability to redirect output from Cisco IOS XE command-line interface (CLI) **show** commands and **more** commands to a file.

## 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 Show Command Output Redirection” section on page 4](#).

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

- [Information About Show Command Output Redirection, page 1](#)
- [Configuration Examples for Show Command Output Redirection, page 2](#)
- [Feature Information for Show Command Output Redirection, page 4](#)

## Information About Show Command Output Redirection

This feature enhances the **show** commands in the Cisco IOS XE CLI to allow large amounts of data output to be written directly to a file for later reference. This file can be saved on local or remote storage devices such as Flash, a SAN Disk, or an external memory device.



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

For each **show** command issued, a new file can be created, or the output can be appended to an existing file. Command output can optionally be displayed on-screen while being redirected to a file by using the **tee** keyword. Redirection is available using a pipe (|) character after any **show** command, combined with the **redirect**, **append**, or **tee** keywords.

These extensions can also be added to **more** commands.

## Configuration Examples for Show Command Output Redirection

This section provides the following configuration examples:

- [Redirecting a show interface output to a device attached to a USB port: Example, page 2](#)

### Redirecting a show interface output to a device attached to a USB port: Example

This task will show how to redirect a **show platform software configuration access policy** output to a device attached to a *templ.txt* file in the bootflash of an ASR1000 series router.

```
router#show platform software configuration access policy | redirect bootflash:templ.txt
```

```
router#more bootflash:templ.txt  
The current access-policies
```

```
Method : telnet  
Rule : wait  
Shell banner:  
Wait banner :
```

```
Method : ssh  
Rule : wait  
Shell banner:  
Wait banner :
```

```
Method : console  
Rule : wait with interrupt  
Shell banner:  
Wait banner :
```

```
===
```

## Additional References

No standards, MIBs, or RFCs are applicable to this feature.



## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for Show Command Output Redirection

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 Show Command Output Redirection

Feature Name	Releases	Feature Information
Show Command Output Redirection	Cisco IOS XE Release 2.1	This feature was introduced.

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

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

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

© 2009 Cisco Systems, Inc. All rights reserved.



## **Configuration Using Setup and Autoinstall**





# Overview: Basic Configuration of a Cisco Networking Device

---

**First published:** August 9, 2005  
**Last updated:** May 4, 2009

Cisco IOS XE software provides two features, AutoInstall and Setup mode, to simplify configuring a Cisco IOS XE-based networking device. AutoInstall enables automatic loading of device configuration files from a remote location and can be used to configure several devices concurrently. Setup is an interactive Cisco IOS XE software command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration but limits you to configuring a single device at a time. AutoInstall is an automatic process for the device that is being configured; Setup is a manual process for the device that is being configured.

This module provides an introduction to each feature and directs you to modules that describe the features in detail and explain how to use them.

The terms *initial configuration* and *startup configuration* are used interchangeably.

## Contents

- [Prerequisites for Basic Configuration of a Cisco Networking Device, page 2](#)
- [Restrictions for Basic Configuration of a Cisco Networking Device, page 3](#)
- [Information About Basic Configuration of a Cisco Networking Device, page 1](#)
- [Additional References, page 3](#)

## Information About Basic Configuration of a Cisco Networking Device

Before you configure a networking device with a basic configuration, you should understand the following concepts and decide whether AutoInstall or Setup mode is the best method, based on your requirements.



---

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

© 2005-2009 Cisco Systems, Inc. All rights reserved.

- [Comparison of Cisco IOS XE AutoInstall and Cisco IOS XE Setup Mode, page 2](#)
- [Cisco IOS XE AutoInstall, page 2](#)
- [Cisco IOS XE Setup Mode, page 2](#)

## Comparison of Cisco IOS XE AutoInstall and Cisco IOS XE Setup Mode

Cisco IOS XE AutoInstall enables automatic loading of device configuration files from a remote location and can be used to configure several devices concurrently. Setup is an interactive Cisco IOS XE software CLI mode that guides you through a basic (also called a startup) configuration but limits you to configuring a single device at a time. AutoInstall is an automatic process; Setup is a manual process.

### Cisco IOS XE AutoInstall

AutoInstall is the Cisco IOS XE software feature that enables the configuration of a remote networking device from a central location. The configuration files must be stored on a TFTP server that is accessible by the devices that you are using AutoInstall to setup.

AutoInstall is supported over Ethernet, Token Ring, and FDDI interfaces for LANs, serial interfaces using High-Level Data Link Control (HDLC) encapsulation, and serial interfaces using Frame Relay encapsulation for WANs.

AutoInstall is designed to facilitate central management of installations at remote sites. The AutoInstall process begins when a Cisco IOS XE software-based device is turned on and a valid configuration file is not found in NVRAM. AutoInstall may not start if the networking device has Cisco Router and Security Device Manager (SDM) or Cisco Network Assistant already installed. In this case, to enable AutoInstall you need to disable SDM.

[Using AutoInstall to Remotely Configure Cisco Networking Devices](#) describes how AutoInstall functions, how to disable SDM, and how to configure devices to use AutoInstall.

### Cisco IOS XE Setup Mode

Cisco IOS XE Setup mode enables you to build an initial configuration file using the Cisco IOS XE CLI or System Configuration Dialog. The dialog guides you through initial configuration and is useful when you are unfamiliar with Cisco products or the CLI and when configuration changes do not require the level of detail the CLI provides.

Setup starts automatically when a device has no configuration file in NVRAM and is not preconfigured from the factory to use Cisco SDM. When setup completes, it presents the System Configuration Dialog. This dialog guides you through an initial configuration with prompts for basic information about your device and network and then creates an initial configuration file. After the file is created, you can use the CLI to perform additional configuration.

[Using Setup Mode to Configure a Cisco Networking Device](#) describes how to use Setup to build a basic configuration and to make configuration changes.

## Where to Go Next

Proceed to either [Using AutoInstall to Remotely Configure Cisco Networking Devices](#) module or [Using Setup Mode to Configure a Cisco Networking Device](#).

# Additional References

This section provides references related to the basic configuration of a Cisco networking device.

## Related Documents

Related Topic	Document Title
Configuring a networking device for the first time using the Cisco IOS XE software feature AutoInstall.	<a href="#">Using AutoInstall to Remotely Configure Cisco Networking Devices</a>
Configuring a networking device using Cisco IOS XE Setup mode	<a href="#">Using Setup Mode to Configure a Cisco Networking Device</a>
Configuration fundamentals and associated commands	<i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i> for your release and the release-independent <a href="#">Cisco IOS Configuration Fundamentals Command Reference</a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Overview: Basic Configuration of a Cisco Networking Device

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 Overview: Basic Configuration of a Cisco Networking Device

Feature Name	Releases	Feature Information
Overview: Basic Configuration of a Cisco Networking Device	Cisco IOS XE Release 2.1	This feature was introduced.

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

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

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

© 2005-2009 Cisco Systems, Inc. All rights reserved.





# Using AutoInstall to Remotely Configure Cisco Networking Devices

---

**First Published: November 28, 2005**

**Last Updated: May 4, 2009**

AutoInstall enables remote, automatic configuration of networking devices. AutoInstall is typically used to set up new networking devices remotely. You can, however, use AutoInstall to configure existing networking devices after you remove the configuration file from their NVRAM. The AutoInstall process uses pre-existing configuration files that are stored on a TFTP server.

In this module the term *networking device* means a router that runs Cisco IOS XE software. Also, the following terms are used interchangeably:

- *initial configuration* and *startup configuration*
- *set up* and *configure*

## 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 Using AutoInstall to Remotely Configure a Cisco Networking Device”](#) section on page 34.

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

- [Information About Using AutoInstall to Remotely Configure Cisco Networking Devices, page 2](#)
- [How to Use AutoInstall to Remotely Configure Cisco Networking Devices, page 13](#)



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Using AutoInstall to Remotely Configure Cisco Networking Devices, page 14](#)
- [Additional References, page 33](#)
- [Feature Information for Using AutoInstall to Remotely Configure a Cisco Networking Device, page 34](#)

## Information About Using AutoInstall to Remotely Configure Cisco Networking Devices

Before you configure or use AutoInstall, you should understand the following information:

- [AutoInstall, page 2](#)
- [Benefits of Using AutoInstall to Remotely Configure a Cisco Networking Device, page 12](#)

### AutoInstall

AutoInstall can be used to load a final full configuration, or a partial temporary configuration, on to a networking device that is being configured with AutoInstall.



**Tip**

When you use AutoInstall to load a partial temporary configuration, you must finish configuring the device manually.

The requirements for provisioning your network for AutoInstall, and the configuration options for provisioning AutoInstall are explained in these sections:

- [Services and Servers Used By AutoInstall: Dynamic Assignment of IP Addresses, page 2](#)
- [Services and Servers Used By AutoInstall: IP-to-Hostname Mapping, page 6](#)
- [Services and Servers Used By AutoInstall: Storage and Transmission of Configuration Files, page 6](#)
- [Networking Devices Used by AutoInstall, page 7](#)
- [Configuration Files Used by AutoInstall, page 8](#)
- [Configuration Options for AutoInstall, page 11](#)
- [The AutoInstall Process, page 11](#)

### Services and Servers Used By AutoInstall: Dynamic Assignment of IP Addresses

The network must be able to provide the dynamic assignment of an IP address to the networking device that is being configured with AutoInstall. The type of IP address assignment server that is used depends on the type of connection that the networking that is being configured with AutoInstall has to the network.

AutoInstall uses these types of IP address servers:

- [DHCP Servers, page 3](#)
- [SLARP Servers, page 4](#)
- [BOOTP Servers, page 5](#)

## DHCP Servers

Networking devices using AutoInstall over a LAN connection require a DHCP server to provide an IP address dynamically. This requirement applies to Fast Ethernet, Token Ring, and FDDI interfaces. The network must be configured to provide IP connectivity between the DHCP server and any devices that are using AutoInstall over LAN connections.

DHCP (defined in RFC 2131) is an extension of the functionality provided by the Bootstrap Protocol (defined in RFC 951). DHCP provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options such as a router (gateway) IP address, a TFTP server IP address, the name of a boot file to load, and the domain name to use. DHCP servers can be configured on routers, UNIX servers, Microsoft Windows-based servers, and other platforms.

DHCP servers typically assign IP addresses from a pool of IP addresses randomly. It is possible for a device that uses DHCP to obtain its IP address to have a different IP address every time it is connected to the network. This creates a problem for the AutoInstall process when you want to ensure that a particular device is assigned a specific hostname during the AutoInstall process. For example, if you are installing routers on different floors in a remote site and each router is supposed to be assigned a name that indicates its location, such as **ChicagoHQ-1st** and **ChicagoHQ-2nd**, you need to ensure that each device gets the IP address that will be mapped to its correct hostname.

The process of ensuring that a device is assigned a specific IP address is referred to as *creating a reservation*. A reservation is a manually configured relationship between an IP address and a physical layer address of a LAN interface on the device. Many Cisco IOS XE-based devices do not use their MAC address when they request an IP address via DHCP. They use a much longer client identifier instead. Due to the complexity of identifying the client identifier so that you can preconfigure a reservation, and the complexity of finding out if the new device uses its MAC address or the client identifier, we recommend that you allow a new device to obtain an IP address without using a DHCP reservation first in order to discover if the device is using its MAC address or a client identifier. When you have learned how the new device is identifying itself to the DHCP server, you can make a note of the format and create a reservation for it. The next time the new device is rebooted it should obtain the IP address that you reserved to ensure that the new device is assigned the correct hostname. Refer to the information on creating DHCP reservations that was provided with your DHCP server software. The process for creating reservations using Cisco IOS XE based DHCP servers is explained in the “[Using AutoInstall to Set Up Devices Connected to LANs: Example](#)” section on page 14. This section includes instructions for identifying the client identifier before the device is connected to the network so that you can preconfigure the DHCP reservations.

**Note**

This document uses a Cisco router as the DHCP server for using AutoInstall to configure LAN-connected networking devices. If you are using a different device as your DHCP server ensure that you have the user documentation for it available in the event that you need help configuring it.

**Note**

There are several configuration parameters such as TFTP server addresses, DNS server addresses, domain names and so on, that can be provided to LAN-connected clients by DHCP servers during the process of assigning IP addresses to clients. These parameters are not required by AutoInstall, therefore they are not included in this document. If you know how to use these parameters you can include them in your DHCP server configuration when you are using AutoInstall to setup your networking devices.

For more information on DHCP services visit the IETF RFC site (<http://www.ietf.org/rfc.html>) and look for RFCs about DHCP. Most server operating systems support DHCP servers. Refer to the documentation that was provided with your operating system for more information.

## SLARP Servers

A router that is being configured with AutoInstall over a serial interface using HDLC encapsulation will send a Serial Line ARP (SLARP) request for an IP address over the serial interface that is connected to the staging router.

The serial interface of the staging router must be configured with an IP address in which the host portion is 1 or 2, such as 192.168.10.1 or 192.168.10.2. The staging router will send a SLARP response to the router that is being configured with AutoInstall that contains the value that the staging router is not using. For example, if the interface on the staging router that is connected to the router that is being configured with AutoInstall is using 192.168.10.1 as its IP address, the staging router will send a SLARP response with a value of 192.168.10.2 to the router that is being configured with AutoInstall.



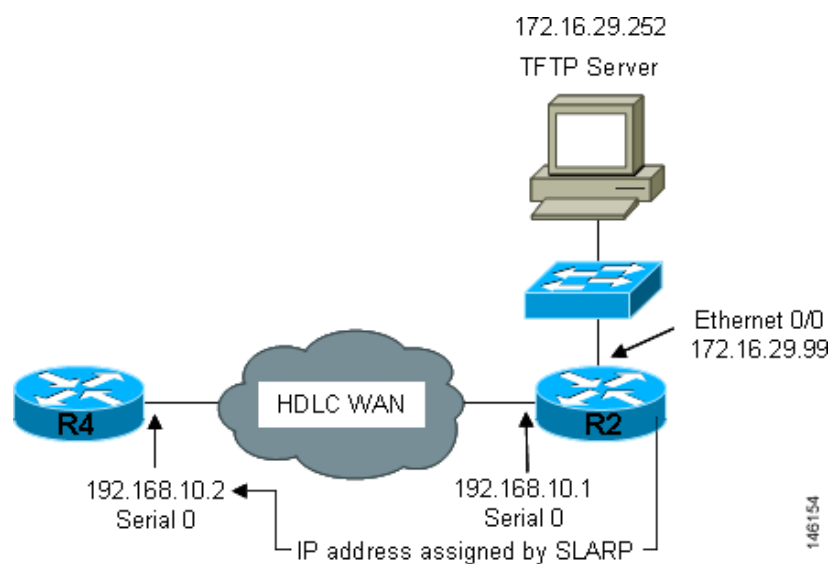
### Tip

If you are using a mask of 255.255.255.252 on the serial interface of the staging router SLARP will assign the available IP host address to the new device. For example, if you assign IP address 198.162.10.5 255.255.255.252 to serial 0 on the staging router, SLARP will assign 198.162.10.6 to the new device. If you assign IP addresses 198.162.10.6 255.255.255.252 to serial 0 on the staging router SLARP will assign 198.162.10.5 to the new device.

Figure 2 shows an example of SLARP.

In Figure 1, the IP address of serial interface 0 on the staging router (R2) is 192.168.10.1. SLARP therefore assigns the IP address 192.168.10.2 to serial interface 0 on the new device.

**Figure 1** Using SLARP to Assign an IP Address to a New Device



### Note

AutoInstall over a serial interface using HDLC can be performed only over the first serial port on a new device (serial interface 0 or serial interface x/0). The staging router and new device must be directly connected using the first serial interface port on the new device; for example, serial 0/0 or if the first serial port is in the second slot of the device, serial 2/0.

**Tip**

The IP address that is assigned to the router that is being configured with AutoInstall by SLARP from the staging router is the IP address that you must use in the **ip host hostname ip-address** command in the AutoInstall network-confg or cisco.net.cfg file to ensure that the router that is being configured with AutoInstall is assigned the correct hostname so that it can request its host-specific configuration file.

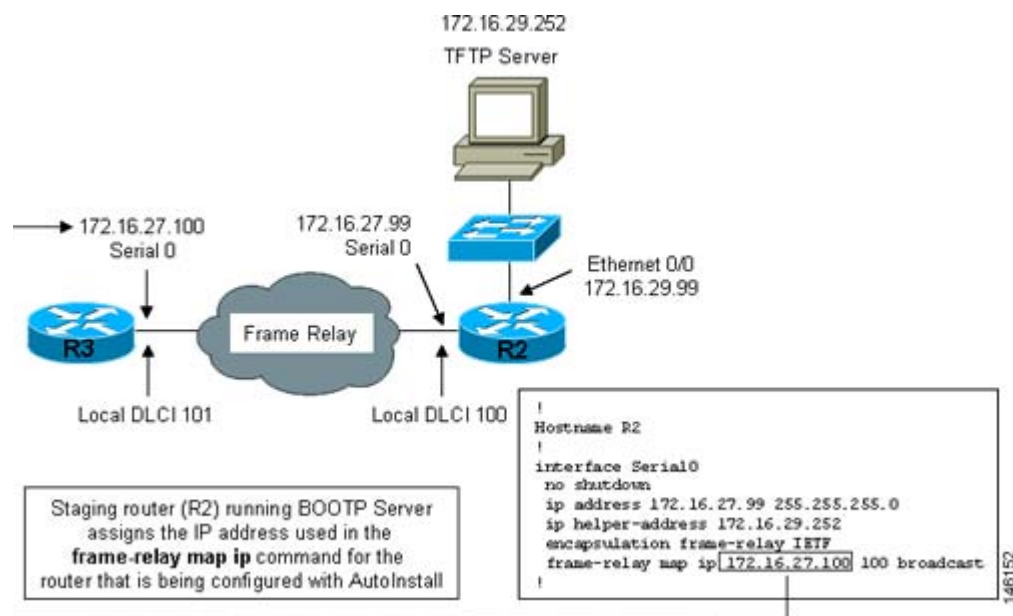
## BOOTP Servers

A router that is being configured with AutoInstall over a serial interface using Frame Relay encapsulation will send a BOOTP request for an IP address over the serial interface that is connected to the staging router.

The staging router learns the correct IP address to provide in its BOOTP response to the router that is being configured with AutoInstall by examining the **frame-relay map ip ip-address dlci** command that is configured on the interface that it is using to connect to the router that is being configured with AutoInstall.

In [Figure 2](#) R2 is the staging router. R2 has the **frame-relay map ip 172.16.27.100 100** broadcast command configured on interface serial 0. When R2 receives the BOOTP request for an IP address from R3 during the AutoInstall process, R3 will reply with 172.16.27.100.

**Figure 2** Example of Using BOOTP for Autoinstall Over a Frame Relay Network

**Tip**

The limitation imposed by SLARP in which the IP addresses for the new device and the staging router must end in either .1 or .2 does not apply to BOOTP. BOOTP for AutoInstall over Frame Relay supports all host addresses for the IP address subnet that is assigned to the Frame Relay circuit between the router that is being configured with AutoInstall and the staging router.

**Tip**

The IP address that is assigned to the router that is being configured with AutoInstall by BOOTP from the staging router is the IP address that you must use in the **ip host *hostname ip-address*** command in the AutoInstall network-conf or cisco.net.cfg file to ensure that the router that is being configured with AutoInstall is assigned the correct hostname so that it can request its host-specific configuration file.

**Note**

AutoInstall over a serial interface using Frame Relay encapsulation can be performed only over the first serial port on a new device (serial interface 0 or serial interface x/0). The staging router and new device must be directly connected using the first serial interface port on the new device; for example, serial 0/0 or if the first serial port is in the second slot of the device, serial 2/0.

## Services and Servers Used By AutoInstall: IP-to-Hostname Mapping

If you want the networking device to load a full configuration file during the AutoInstall process, the networking device must be able to determine its hostname so that it can request the configuration file that you created specifically for it.

The following caveats apply to the provisioning of IP address to hostname mapping for AutoInstall:

- Any networking device that is being configured with AutoInstall can determine its hostname by loading one of the AutoInstall network configuration files (network-conf or cisco.net.cfg) from the TFTP server that contain the **ip host *hostname ip-address*** commands. For example, to map host R3 to IP address 198.162.100.3, the network-conf or cisco.net.cfg file must contain the **ip host r3 198.162.100.3** command.
- A networking device that is being configured with AutoInstall over a LAN interface can also determine its hostname by querying a DNS server. If the DNS server is not connected to the same LAN the device must learn the IP address of the DNS server from the DHCP server during the process of obtaining its dynamically assigned IP address from the DHCP server.

### DNS Servers

DNS servers are used to provide a network service that maps hostnames to IP addresses and IP addresses to hostnames (reverse DNS lookups). Anytime that you use a hostname to initiate an IP connection to a host, your PC must determine the IP address that is assigned to the hostname that you want to contact. For example, when you visit Cisco's website (<http://www.cisco.com/>) your PC sends a DNS query to a DNS server to discover the current IP address that can be used to contact Cisco's website.

For more information on DNS services visit the IETF RFC site (<http://www.ietf.org/rfc.html>) and look for RFCs about DNS. The Name Server LookUp tool (nslookup) is very useful for learning more about DNS. There are several excellent websites available about nslookup that you can find by searching for them.

## Services and Servers Used By AutoInstall: Storage and Transmission of Configuration Files

TFTP is a protocol used to transfer files between devices on a network. A TFTP server is a device that uses TFTP to transfer files to devices. TFTP servers can be configured on UNIX servers, Microsoft Windows-based PCs and servers, and other platforms.

**Tip**

If you do not have a TFTP server available you can configure a Cisco IOS XE-based router as a TFTP server using the **tftp-server file-system:filename** command. Refer to the [Configuring Basic File Transfer Services](#) guide

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun\\_c/ffcppt2/fcf011.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcppt2/fcf011.htm) for more information on configuring your router as a TFTP server.

Cisco routers use TFTP to load the configuration files that are required for AutoInstall. You must have a TFTP server deployed in your network to provide file storage and file transmission services to the devices that will be using AutoInstall.

For more information on TFTP services visit the IETF RFC site (<http://www.ietf.org/rfc.html>) and look for RFCs about TFTP. There are several excellent websites available about TFTP that you can find by searching for them. Several freeware and shareware versions of TFTP servers for various operating systems and hardware platforms are available from the Internet.

The following caveats apply to the provisioning of TFTP servers for AutoInstall:

- Devices using AutoInstall over a LAN—If the TFTP server and the devices using AutoInstall are on different LAN segments, you must either configure the **ip helper-address address** command on all of the interfaces that will receive TFTP session initialization requests from the devices that are using AutoInstall.
- Devices using AutoInstall over a WAN—If the devices using AutoInstall are connected to a WAN, you must configure the **ip helper-address address** command on all of the interfaces that will receive TFTP session initialization requests from devices that are using AutoInstall.

**ip helper-address**

If the new device does not learn the IP address of the TFTP server via DHCP option 150, it will transmit the TFTP session initialization requests as network layer broadcasts using the IP destination broadcast address of 255.255.255.255. Routers block network layer broadcast datagrams which prevents the TFTP session initialization requests from reaching the TFTP server, and AutoInstall will fail. The solution to this problem is to use the **ip helper-address address** command. The **ip helper-address address** command changes the broadcast address of TFTP session initialization request from 255.255.255.255 to the address that is configured with the *address* argument. For example, the **ip helper-address 172.16.29.252** command will change IP destination broadcast address of 255.255.255.255 to 172.16.29.252.

## Networking Devices Used by AutoInstall

These networking devices are used by AutoInstall:

- [Device That Is Being Configured with AutoInstall, page 7](#)
- [Staging Router, page 8](#)
- [Intermediate Frame Relay-ATM Switching Device \(Optional\), page 9](#)

### Device That Is Being Configured with AutoInstall

A device that is being configured with AutoInstall can be any Cisco IOS XE-based router that supports AutoInstall and does not have a configuration file in its NVRAM.



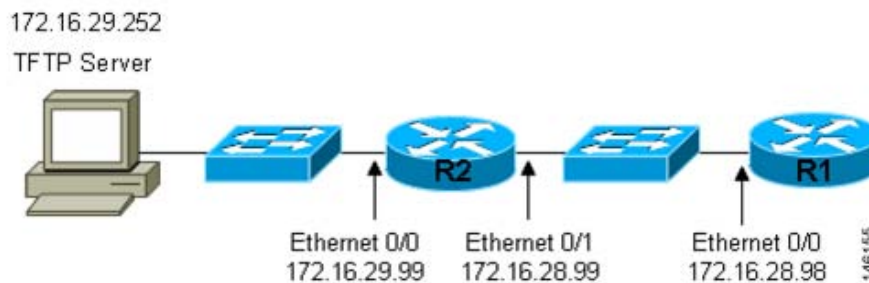
## Staging Router

A staging router acts as an intermediary between the TFTP server (to which it must have IP connectivity) and a device that is being configured with AutoInstall when the new device and the TFTP server are connected to different networks. In [Figure 3](#) R1 requires a staging router because it is connected to a different LAN segment than the TFTP server.

Staging routers are required in the following situations:

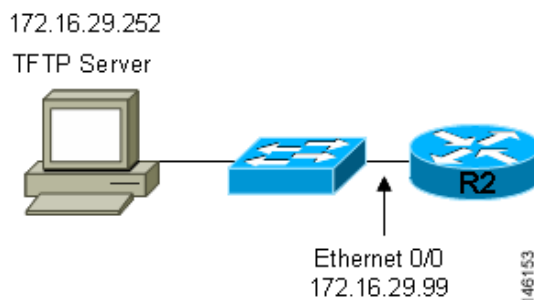
- Devices using AutoInstall over a LAN—If the TFTP and/or DHCP servers and the devices using AutoInstall are on different LAN segments you must use a staging router.
- Devices using AutoInstall over a WAN—If the devices using AutoInstall are connected to a WAN, you must configure the **ip helper-address** *address* command on all of the directly connected interfaces that will receive TFTP session initialization requests from the devices that are using AutoInstall.

**Figure 3** Example of AutoInstall That Requires a Staging Router



Staging routers are not required when the new device that is being configured with AutoInstall is connected to the same LAN segment as the TFTP and DHCP servers. In [Figure 4](#) R2 does not require a staging server to use AutoInstall because it is on the same LAN segment as the TFTP server.

**Figure 4** Example of AutoInstall That Does Not Require a Staging Router



## Configuration Files Used by AutoInstall

A configuration file executes predefined commands and settings that enable a device to function in a network. The type of configuration file you choose determines many aspects of how you set up the network for AutoInstall.

These types of files are used by AutoInstall:

- [Network Configuration File, page 9](#)



- [Host-Specific Configuration File, page 9](#)
- [Default Configuration File \(Optional\), page 10](#)

## Network Configuration File

This is the first file that the AutoInstall process attempts to use. After the device has obtained an IP address it will try to discover its hostname by attempting to download a network configuration file that contains IP address to host name mappings.

If you want the device to learn its hostname from the network-config file so that it can download a host-specific configuration file, you must add an entry for the device in the network-config network configuration file. The syntax for the entry is **ip host *hostname* *ip-address*** where *hostname* is the name that you want the host to use and *ip-address* is the address that the host will receive from the IP address server. For example, if you want the new device to use the name Australia, and the IP address that was dynamically assigned the new device is 172.16.29.103, you need to create an entry in the network configuration file that contains the **ip host australia 172.16.29.103** command.

The file names used for the network configuration file are network-config or cisco.net.cfg. Routers running AutoInstall will try to load the network-config from the TFTP server first. If the network-config is not found on the TFTP server, the AutoInstall process will attempt to load the cisco.net.cfg file. The cisco.net.cfg filename was used by DOS-based TFTP servers that only supported the old 8.3 file naming convention. We recommend that you use the network-config filename to avoid the delay that is created when AutoInstall has to timeout attempting to load the network-config before it attempts to load the cisco.net.cfg file.

If you using autoinstall to setup multiple devices you can create one network configuration file that contains an entry for each of the devices.

## Host-Specific Configuration File

Host-specific configuration files are a full configuration for each new device. If you decide to use host-specific files, you must create a separate file for each new device that you are using AutoInstall to setup.

The filenames used for the host-specific configuration files are *name-config* or *name.cfg* where the word name is replaced by the hostname of the router. For example, the filename for a router named hqrouter is hqrouter-config or hqrouter.cfg.

Routers running AutoInstall will try to load the host-specific configuration filename using the format *name-config* from the TFTP server first. If the *name-config* file is not found on the TFTP server, the AutoInstall process will attempt to load the *name.cfg* file. The *name.cfg* file name format was used by DOS based TFTP servers that only supported the old 8.3 file naming convention. We recommend that you use the *name-config* filename to avoid the delay that is created when AutoInstall has to timeout attempting to load the *name-config* before it attempts to load the *name.cfg* file.



### Tip

If you use the *name.cfg* format for host-specific configuration files the filenames for hostnames that are longer than 8 characters must be truncated to the first eight characters. For example, the filename for a device with the hostname australia must be truncated to australi.cfg. When AutoInstall maps the IP address assigned to the new router to its hostname of australia in the network configuration file, AutoInstall will attempt to download a host-specific file with the name australi.cfg after it fails to load the host-specific filename australia-config.

**Tip**

Cisco recommends that you use the host-specific file option for setting up new devices to ensure that each new device is set up properly.

## Default Configuration File (Optional)

A default configuration file, which includes minimum configuration information allows you to telnet to the new device and configure it manually.

**Tip**

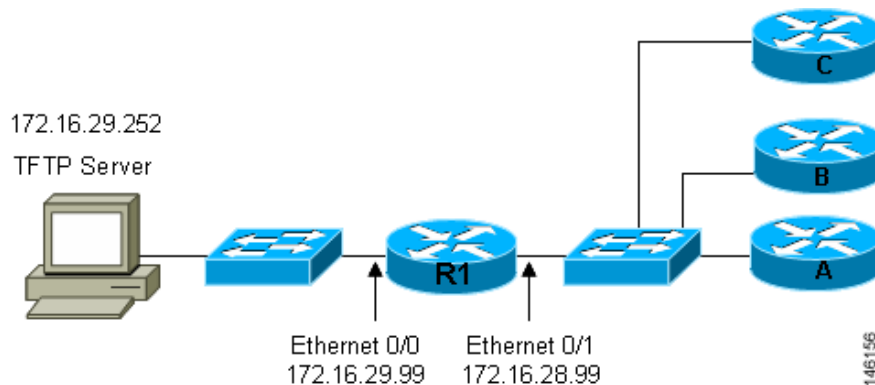
If the new device has learned its hostname after it loaded the network configuration file the default configuration file is not used. You must use the host-specific file instead to configure features such as passwords for remote CLI sessions.

Figure 5 is an example of using the default configuration file to stage new routers for remote manual configuration. Routers A, B, and C are new routers that will be added to the network one at a time. You connect the first router and wait for it to load the default configuration file. The default configuration file must have enough information in it to allow the new router to communicate with the PC that you will be using to finish its configuration using a Telnet session. After the default configuration file is loaded on the new router, you can use Telnet to connect to the router to complete its configuration. You must assign a new, unique IP address to its interfaces so that the default configuration file can be used for configuring the next router.

**Caution**

Failure to change the IP addresses in the router that you are configuring remotely with Telnet will result in duplicate IP addresses on the LAN when the next router loads the default configuration file. In this situation you will not be able to use Telnet to connect to either router. You must disconnect one of the routers before you can resolve this problem.

**Figure 5** *Example of Using the Default Configuration File To Stage Routers For Remote Manual Configuration*

**Tip**

You must include the commands for configuring passwords for remote Telnet access and access to privileged EXEC mode if you are going to access the routers remotely to complete their configurations save their configuration files to NVRAM.

The filenames used for the default network configuration file are `router-conf` or `router.cfg`. Routers running AutoInstall will try to load the `router-conf` from the TFTP server first. If the `router-conf` is not found on the TFTP server the AutoInstall process will attempt to load the `router.cfg` file. The `router.cfg` file name was used by DOS-based TFTP servers that only supported the old 8.3 file naming convention. We recommend that you use the `router-conf` filename to avoid the delay that is created when AutoInstall has to timeout while attempting to load the `router-conf` before it attempts to load the `router.cfg` file.

If you are using AutoInstall to configure LAN-attached devices, you can specify a different default boot filename in DHCP Option 067.

## Configuration Options for AutoInstall

You can provision your network to support AutoInstall using several different combinations of devices and services. For example:

- You can provision all of the services required for AutoInstall (except dynamic IP address assignment using SLARP or BOOTP that must be preformed by a Cisco router) on one network server, or you can provision each service on a different network server.
- You can provision the DHCP service on a Cisco router.
- The device using AutoInstall can determine its IP address from a DNS server, or you can use one of the AutoInstall network configuration files (`network-conf` or `cisconet.cfg`) that contain the `ip host hostname ip-address` commands.
- You can use provision AutoInstall to load a full configuration or a partial configuration onto a device that is using AutoInstall.

This module focuses on some of the most common methods for provisioning AutoInstall. Refer to the [“How to Use AutoInstall to Remotely Configure Cisco Networking Devices” section on page 13](#) for information on the most common methods for provisioning AutoInstall.

## The AutoInstall Process

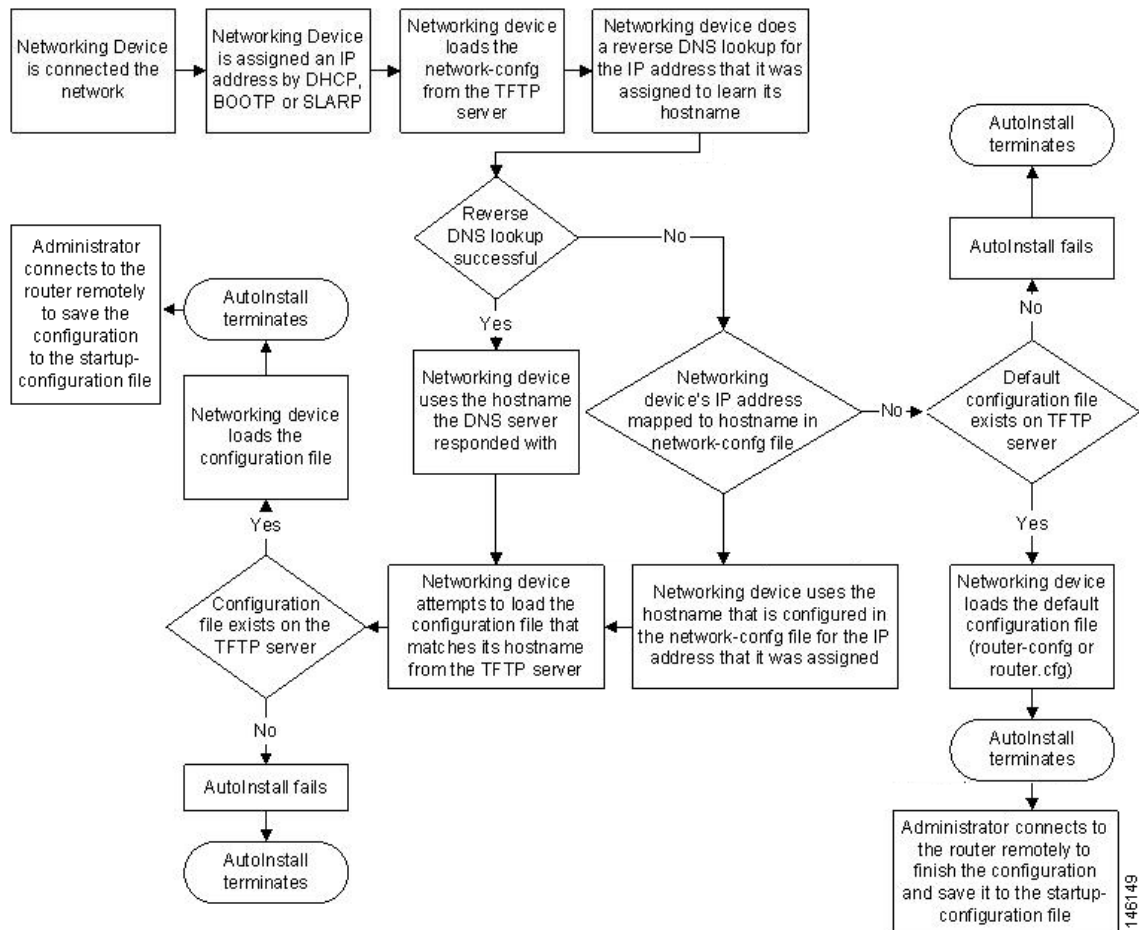
The AutoInstall process begins when a networking device that does not have any files in its NVRAM is connected to the network.



### Timesaver

You can decrease the time that the AutoInstall process takes to complete by only connecting the interface on the networking device that you want to use for AutoInstall until the AutoInstall process has finished. For example, if you want the networking device to perform AutoInstall over a WAN interface and you connect its LAN interfaces and its WAN interfaces the networking device will attempt to perform AutoInstall over the LAN interfaces before it attempts to use the WAN interfaces. Leaving the LAN interfaces disconnected until the AutoInstall process is finished causes the networking device to initiate the AutoInstall process over its WAN interface immediately.

[Figure 6](#) shows the basic flow of the AutoInstall process.

**Figure 6** *AutoInstall Process Flowchart*

## Benefits of Using AutoInstall to Remotely Configure a Cisco Networking Device

AutoInstall facilitates the deployment of Cisco routers by allowing you to manage the setup procedure for routers from a central location. The person responsible for physically installing the router does not require specific networking skills. The ability to physically install the router, connect the power and networking cables, and power it on are the only skills required by the installer. The configuration files are stored and managed on a central TFTP server. By using AutoInstall one skilled network technician based at a central site can manage the deployment of several routers in a short period of time.

Two enhancements to AutoInstall:

- [AutoInstall Using DHCP for LAN Interfaces](#)
- [How to Use AutoInstall to Remotely Configure Cisco Networking Devices](#)

### AutoInstall Using DHCP for LAN Interfaces

The AutoInstall Using DHCP for LAN Interfaces feature enhances the benefits of AutoInstall by replacing the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces (specifically Fast Ethernet, Token Ring, and FDDI interfaces).

DHCP (defined in RFC 2131) is an extension of the functionality provided by the BOOTP (defined in RFC 951). DHCP provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options. The IP address procurement phase of the AutoInstall process is accomplished using DHCP for Fast Ethernet, Token Ring, and FDDI interfaces. Uploading of configuration files using unicast TFTP is also allowed.

## How to Use AutoInstall to Remotely Configure Cisco Networking Devices

This section describes the how to prepare a router for AutoInstall. Additional examples for using AutoInstall for new routers connected to LANs, HDLC WANs, and Frame Relay networks, are provided in the [“Configuration Examples for Using AutoInstall to Remotely Configure Cisco Networking Devices”](#) section on page 14.

In most cases you need to configure a staging router through which a new device running AutoInstall sends TFTP, BOOTP, and DNS requests.

**Tip**

In all cases, you must verify and save the configuration on the networking device after the AutoInstall process is complete. If you do not save the configuration, you must repeat the entire process.

- [Disabling the SDM Default Configuration File, page 13](#)

## Disabling the SDM Default Configuration File

Perform this task if SDM was pre installed on your device and you want to use AutoInstall to configure the device instead. SDM remains on the device.

### SUMMARY STEPS

1. Connect the console cable from the console port on the device to the serial port on the PC.
2. Connect the power supply to the device, plug the power supply into a power outlet, and turn on the device.
3. Connect to the device using a terminal emulation program.
4. **enable**
5. **erase startup-config**
6. **reload**

### DETAILED STEPS

- |               |   |
|---------------|---|
| <b>Step 1</b> | Connect the console cable, shipped with your device, from the console port on the device to a serial port on your PC. Refer to the hardware installation guide for the device for instructions. |
| <b>Step 2</b> | Connect the power supply to the device, plug the power supply into a power outlet, and turn on the device. Refer to the quick start guide for the device for instructions.                      |

- Step 3** Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:
- 9600 baud
  - 8 data bits, no parity, 1 stop bit
  - No flow control
- Step 4** **enable**  
Enter privileged EXEC mode.
- enable**  
Router> enable  
Router#
- Step 5** **erase startup-config**  
Erases the existing configuration in NVRAM.
- Router# erase startup-config
- Step 6** **reload**  
Initiates the reload process. The router will initiate the AutoInstall process after it finishes the reload process.
- Router# reload
- 

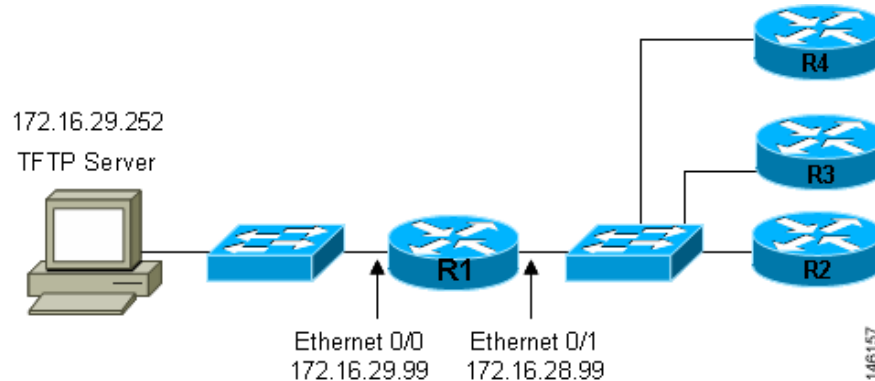
## Configuration Examples for Using AutoInstall to Remotely Configure Cisco Networking Devices

This section provides the following configuration examples:

- [Using AutoInstall to Set Up Devices Connected to LANs: Example, page 14](#)
- [Using AutoInstall to Set Up Devices Connected to WANs: Example, page 26](#)

### Using AutoInstall to Set Up Devices Connected to LANs: Example

This task uses the network in [Figure 7](#). This task will show how to use AutoInstall to setup routers R2, R3, and R4. Router R1 is the DHCP server that will be used to assign the IP address for Fast Ethernet 0/0 on the new routers during the AutoInstall process.

**Figure 7** Network Topology for Assigning AutoInstall Configuration Files For Specific Devices

Every DHCP client has a unique DHCP client identifier. The DHCP client identifier is used by DHCP servers to keep track of IP address leases and for configuring IP address reservations. You need to know the DHCP client identifier for each of the networking devices that you want to configure with AutoInstall so that you can configure the DHCP IP address reservations which will ensure that each device is provided with the correct IP address, and subsequently its unique configuration file. You can determine the DHCP client identifier manually or automatically.

To use AutoInstall to setup routers R2, R3, and R4, perform following tasks:

- [Determining the Value for the DHCP Client Identifier Manually, page 15](#)
- [Determining the Value for the DHCP Client Identifier Automatically, page 18](#)
- [Creating a Private DHCP Pool for Each of The Routers, page 21](#)
- [Creating Configuration Files for Each Router, page 22](#)
- [Creating the network-config file, page 23](#)
- [Setting Up the Routers with AutoInstall, page 24](#)
- [Saving the Configuration Files on The Routers, page 25](#)
- [Removing the Private DHCP Address Pools from R1, page 26](#)

## Determining the Value for the DHCP Client Identifier Manually

If you want to determine the value for the client identifiers automatically, you do not need to perform this task. Proceed to the [“Determining the Value for the DHCP Client Identifier Automatically” section on page 18](#).

You must know the MAC address of the Fast Ethernet interface that will be used to connect the router to the LAN during the AutoInstall process to determine the client identifier manually. This requires connecting a terminal to the router, and powering it on, so that you can enter the **show interface interface-type interface-number** command.

The client-identifier looks like this:

```
0063.6973.636f.2d30.3030.362e.3533.6237.2e38.6537.312d.4661.332f.30
```

The format is *nullcisco-0006.53b7.8e71-fa3/0* where *0006.53b7.8e71* is the MAC address and *fa3/0* is the short interface name for the interface that the IP address request is made for.

The values for the short-if-name field can be obtained from an SNMP workstation with the Cisco MIBs installed. This is an example of how to map ifIndex to an interface on Cisco IOS:

```
snmpwalk -c public ponch ifName
```

```
IF-MIB::ifName.1 = STRING: AT2/0
IF-MIB::ifName.2 = STRING: Et0/0
IF-MIB::ifName.3 = STRING: Se0/0
IF-MIB::ifName.4 = STRING: BR0/0
```

Use the **show interface interface-type interface-number** command to display the information and statistics for a Fast Ethernet interface.

```
R6> show interface fastethernet 3/0
FastEthernet3/0 is up, line protocol is up
  Hardware is AmdFE, address is 0006.53b7.8e71 (bia 0006.53b7.8e71)
.
.
.
R6>
```

The MAC address for FastEthernet 3/0 on R6 is 0006.53b7.8e71. The format of the client identifier for this interface is nullcisco-0006.53b7.8e71-fa3/0.



#### Note

The short interface name for Fast Ethernet interfaces is fa.

[Table 1](#) shows the values for converting characters to their hexadecimal equivalents. The last row in [Table 2](#) shows the client identifier for Fast Ethernet 3/0 on R6 (nullcisco-0006.53b7.8e71-fa3/0).

**Table 1**      **Hexadecimal to Character Conversion Chart**

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
00	NUL	1a	SUB	34	4	4e	N	68	h
01	SOH	1b	ESC	35	5	4f	O	69	I
02	STX	1c	FS	36	6	50	P	6a	j
03	ETX	1d	GS	37	7	51	Q	6b	k
04	EOT	1e	RS	38	8	52	R	6c	l
05	ENQ	1f	US	39	9	53	S	6d	m
06	ACK	20		3a	:	54	T	6e	n
07	BEL	21	!	3b	;	55	U	6f	o
08	BS	22	"	3c	<	56	V	70	p
09	TAB	23	#	3d	=	57	W	71	q
0A	LF	24	\$	3e	>	58	X	72	r
0B	VT	25	%	3f	?	59	Y	73	s
0C	FF	26	&	40	@	5a	Z	74	t
0D	CR	27	'	41	A	5b	[	75	u
0E	SO	28	(	42	B	5c	\	76	v
0F	SI	29	)	43	C	5d	]	77	w
10	DLE	2a	*	44	D	5e	^	78	x
11	DC1	2b	+	45	E	5f	_	79	y
12	DC2	2c	,	46	F	60	`	7a	z



**Table 1** Hexadecimal to Character Conversion Chart (continued)

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
13	DC3	2d	-	47	G	61	a	7b	{
14	DC4	2e	.	48	H	62	b	7c	
15	NAK	2f	/	49	I	63	c	7D	}
16	SYN	30	0	4a	J	64	d	7e	~
17	ETB	31	1	4b	K	65	e	7f	D
18	CAN	32	2	4c	L	66	f		
19	EM	33	3	4d	M	67	g		

**Table 2** Conversion of nullcisco-0006.53b7.8e71-fa3/0 To A Client Identifier

00	c	i	s	c	o	-	0	0	0	6	.	5	3	b	7	.	8	e	7	1	-	f	a	3	/	0
00	63	69	73	63	6f	2d	30	30	30	36	2e	35	33	62	37	2e	38	65	37	31	2d	46	61	33	2f	30

**R4**

Use the **show interface interface-type interface-number** command to display the information and statistics for Fast Ethernet 0/0 on R4.

```
R4> show interface FastEthernet 0/0
FastEthernet0 is up, line protocol is up
Hardware is Lance, address is 00e0.1eb8.eb0e (bia 00e0.1eb8.eb0e)
```

The MAC address for Fast Ethernet 0/0 on R4 is 00e0.1eb8.eb0e. The format of the client identifier for this interface is nullcisco-00e0.1eb8.eb0e-et0.

**Note**

The short interface name for Fast Ethernet interfaces is et.

Using the values for converting characters to their hexadecimal equivalents in [Table 1](#), the client identifier for Fast Ethernet 0/0 on R4 is shown in the last row of [Table 3](#).

**Table 3** Conversion of null.cisco-00e0.1eb8.eb0e-et0 To A Client Identifier for R4

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	0	e	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	30	65	2d	45	74	30

**R3**

Use the **show interface interface-type interface-number** command to display the information and statistics for Fast Ethernet 0/0 on R3.

```
R3> show interface FastEthernet 0/0
FastEthernet0 is up, line protocol is up
Hardware is Lance, address is 00e0.1eb8.eb73 (bia 00e0.1eb8.eb73)
```

The MAC address for Fast Ethernet 0/0 on R3 is 00e0.1eb8.eb73. The format of the client identifier for this interface is: nullcisco-00e0.1eb8.eb73-et0.

Using the values for converting characters to their hexadecimal equivalents in [Table 1](#), the client identifier for Fast Ethernet 0/0 on R3 is shown in the last row of [Table 4](#).

**Table 4** Conversion of null.cisco-00e0.1eb8.eb73-et0 To A Client Identifier for R3

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	7	3	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	37	33	2d	45	74	30

## R2

Use the **show interface interface-type interface-number** command to display the information and statistics for Fast Ethernet 0/0 on R2.

```
R2> show interface Fast Ethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb09 (bia 00e0.1eb8.eb09)
```

The MAC address for Fast Ethernet 0/0 on R2 is 00e0.1eb8.eb09. The format of the client identifier for this interface is nullcisco-00e0.1eb8.eb09-et0.

Using the values for converting characters to their hexadecimal equivalents in [Table 1](#), the client identifier for Fast Ethernet 0/0 on R2 is shown in the last row of [Table 5](#)

**Table 5** Conversion of null.cisco-00e0.1eb8.eb09-et0 To A Client Identifier for R2

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	0	9	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	30	39	2d	45	74	30

You have now determined the values for the client identifiers on each router. The final step is to add a period after each group of four characters working from the left to the right as shown below:

- R4–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
- R3–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
- R2–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

## What to Do Next

Save the values in a text file and proceed to the [“Creating a Private DHCP Pool for Each of The Routers” section on page 21](#).

## Determining the Value for the DHCP Client Identifier Automatically

If you determined the value for the client identifiers manually, you do not need to perform this task. Proceed to the [“Creating a Private DHCP Pool for Each of The Routers” section on page 21](#).

This task will create a DHCP server on R1 that will provide only one IP address. This IP address will be used by each new router in sequence while you determine the value of the router’s client identifier. By limiting the IP address scope to a single IP address you avoid any possible confusion about which router you are working on. If somebody powers up another router that attempts to start the AutoInstall process, it will not be able to obtain an IP address.

**Tip**

Do not place the network-config or router configuration files (r4-config, r3-config, or r2-config) in the root directory of the TFTP server yet. You do not want any of the routers to load these files until you have ensured that each router will obtain the correct IP address from the DHCP server so that the router will load the correct configuration file.

This task is broken down into sub-tasks to make it easier to follow (all sub-tasks are required):

- [Configuring IP on the Interfaces on R1, page 19](#)
- [Configuring a DHCP Pool on R1, page 19](#)
- [Excluding All But One of the IP Addresses from the DHCP Pool on R1, page 19](#)
- [Verifying The Configuration on R1, page 20](#)
- [Enabling debug ip dhcp server events on R1, page 20](#)
- [Identifying the Value for the Client Identifier on Each of the Routers, page 20](#)
- [Removing the DHCP Pool on R1 for Network 172.16.28.0/24, page 21](#)
- [Removing the DHCP Pool on R1 for Network 172.16.28.0/24, page 21](#)
- [Removing the Excluded Address Range From R1, page 21](#)

## Configuring IP on the Interfaces on R1

Configure IP addresses on the Fast Ethernet interfaces. Configure the **ip helper-address** *ip-address* command on Fast Ethernet 0/1.

```
!  
interface FastEthernet0/0  
  ip address 172.16.29.99 255.255.255.0  
!  
interface FastEthernet0/1  
  ip address 172.16.28.99 255.255.255.0  
  ip helper-address 172.16.29.252  
!
```

## Configuring a DHCP Pool on R1

Configure these commands to setup the temporary DHCP server on R1.

**Note**

This should be the only DHCP server in operation on R1. This should be the only DHCP server that is accessible by the routers that you will be using AutoInstall to setup.

```
!  
ip dhcp pool get-client-id  
  network 172.16.28.0 255.255.255.0  
!
```

## Excluding All But One of the IP Addresses from the DHCP Pool on R1

You need to ensure that there is only one IP address available from the DHCP server at any time. Configure the following command to exclude every IP address except 172.16.28.1 from the DHCP pool.

```
!  
ip dhcp excluded-address 172.16.28.2 172.16.28.255  
!
```

## Verifying The Configuration on R1

Verify that the configuration file for R1 has a DHCP server pool configured to provide a single IP address (172.16.28.1) to a DHCP client.

Verify that the configuration file has the IP addresses for the Fast Ethernet interfaces and the **ip helper-address** *ip-address* command.

```
!
ip dhcp excluded-address 172.16.28.2 172.16.28.255
!
ip dhcp pool get-client-id
    network 172.16.28.0 255.255.255.0
!
interface FastEthernet0/0
    ip address 172.16.29.99 255.255.255.0
!
interface FastEthernet0/1
    ip address 172.16.28.99 255.255.255.0
    ip helper-address 172.16.29.252
!
```

## Enabling debug ip dhcp server events on R1

You use the display output from the **debug ip dhcp server events** command on the terminal connected to R1 to identify the value of the client identifier for each router.

Enable the **debug ip dhcp server events** command on R1.

```
R1# debug ip dhcp server events
```

## Identifying the Value for the Client Identifier on Each of the Routers

This step is repeated for each of the routers. You should only have one of the routers powered-on at any time. When you have identified the value of the client identifier field for the router, you will turn the router off and proceed to the next router.

### R4

Connect R4 to the Fast Ethernet network and power it on. The following message will be displayed on the terminal connected to R1 when R4 is assigned the IP address 172.16.28.1.

```
DHCPD: assigned IP address 172.16.28.1 to client
0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30.
```

Copy the client identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30 to a text file and save it. Keep the text file open for the next two routers.

Turn off R4

Release the IP address binding for R4 from the DHCP pool on R1 using the **clear ip dhcp binding \*** command on R1.

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

### R3

Connect R3 to the Fast Ethernet network and power it on. The following message will be displayed on the terminal connected to R1 when R3 is assigned the IP address 172.16.28.1.

```
DHCPD: assigned IP address 172.16.28.1 to client  
0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30.
```

Copy the client identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30 to the text file and save it. Keep the text file open for the final router.

Turn off R3.

Release the IP address binding for R3 from the DHCP pool on R1 using the **clear ip dhcp binding \*** command on R1.

```
R1# clear ip dhcp binding *  
R1#  
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

## R2

Connect R2 to the Fast Ethernet network and power it on. The following message will be displayed on the terminal connected to R1 when R2 is assigned the IP address 172.16.28.1.

```
DHCPD: assigned IP address 172.16.28.1 to client  
0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30.
```

Copy the client identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30 to the text file and save it.

Turn off R2

Release the IP address binding for R2 from the DHCP pool on R1 using the **clear ip dhcp binding \*** command on R1.

```
R1# clear ip dhcp binding *  
R1#  
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

## Client Identifiers for R4, R3, and R2

You have determined the values for the client identifiers on each router.

- R4–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
- R3–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
- R2–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

## Removing the DHCP Pool on R1 for Network 172.16.28.0/24

The temporary DHCP pool on the router is no longer required, and must be removed.

```
R1(config)# no ip dhcp pool get-client-id
```

## Removing the Excluded Address Range From R1

The command for excluding all of the IP addresses except 172.16.28.1 from the DHCP pool on the router is no longer required, and must be removed.

```
R1(config)# no ip dhcp excluded-address 172.16.28.2 172.16.28.255
```

## Creating a Private DHCP Pool for Each of The Routers

You need to create the private DHCP address pools for each router to ensure that each router is assigned the IP address that maps to its host name in the network-conf file.

```

!
ip dhcp pool r4
  host 172.16.28.100 255.255.255.0
  client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30

!
ip dhcp pool r3
  host 172.16.28.101 255.255.255.0
  client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30

!
ip dhcp pool r2
  host 172.16.28.102 255.255.255.0
  client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

```

## Creating Configuration Files for Each Router

Create the configuration files for each router and place them in the root directory of the TFTP server.



### Tip

You must include the commands for configuring passwords for remote Telnet access and access to privileged EXEC mode if you are going to access the routers remotely to save their configuration files to NVRAM.

#### r2-config

```

!
hostname R2
!
enable secret 7gD2A0
!
interface FastEthernet0/0
  ip address 172.16.28.102 255.255.255.0
!
interface Serial0/0
  ip address 192.168.100.1 255.255.255.252
  no shutdown
!
interface Serial0/1
  ip address 192.168.100.5 255.255.255.252
  no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
line vty 0 4
  password 5Rf1k9
  login
!
end

```

#### r3-config

```

!
hostname R3
!
enable secret 7gD2A0
!

```

```
interface FastEthernet0/0
 ip address 172.16.28.101 255.255.255.0
!
interface Serial0/0
 ip address 192.168.100.9 255.255.255.252
 no shutdown
!
interface Serial0/1
 ip address 192.168.100.13 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 FastEthernet0
!
line vty 0 4
 password 5Rflk9
 login
!
end
```

#### **r4-config**

```
!
hostname R3
!
enable secret 7gD2A0
!
interface FastEthernet0/0
 ip address 172.16.28.101 255.255.255.0
!
interface Serial0/0
 ip address 192.168.100.9 255.255.255.252
 no shutdown
!
interface Serial0/1
 ip address 192.168.100.13 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
line vty 0 4
 password 5Rflk9
 login
!
end
```

## Creating the network-config file

Create the network-config file with the **ip host** *hostname ip-address* commands that map the IP addresses that you will be assigning with the DHCP server to the hostname.

```
ip host r4 172.16.28.100
ip host r3 172.16.28.101
ip host r2 172.16.28.102
```

## Setting Up the Routers with AutoInstall

You are now ready to set up the three routers (R4, R3, and R2) using AutoInstall.

Connect a terminal to the routers if you want to monitor the progress of AutoInstall. Use Hyperterminal or a similar terminal emulation program on your PC, with the following terminal emulation settings, to connect to the device:

- 9600 baud
- 8 data bits, no parity, 1 stop bit
- No flow control

You should have the following files in the root directory of the TFTP server.

- network-config
- r4-config
- r3-config
- r2-config

The TFTP server must be running.

Power on each router.



### Timesaver

---

You can set up all three routers concurrently.

---

### R4

The following is an excerpt of the messages that are displayed on R4's console terminal during the AutoInstall process:

```
Loading network-config from 172.16.29.252 (via FastEthernet0/0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.100 to r4
Loading r4-config from 172.16.29.252 (via FastEthernet0/0): !
[OK - 687 bytes]
```

### R3

The following is an excerpt of the messages that are displayed on R3's console terminal during the AutoInstall process:

```
Loading network-config from 172.16.29.252 (via FastEthernet0/0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.101 to r3
Loading r3-config from 172.16.29.252 (via FastEthernet0/0): !
[OK - 687 bytes]
```

### R2

The following is an excerpt of the messages that are displayed on R2's console terminal during the AutoInstall process:

```
Loading network-config from 172.16.29.252 (via FastEthernet0/0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.102 to r2
Loading r2-config from 172.16.29.252 (via FastEthernet0/0): !
[OK - 687 bytes]
```



### TFTP Server Log

The TFTP server log should contain messages similar to the following text.

```
Sent network-config to (172.16.28.100), 76 bytes
Sent r4-config to (172.16.28.100),687 bytes
Sent network-config to (172.16.28.101), 76 bytes
Sent r3-config to (172.16.28.101),687 bytes
Sent network-config to (172.16.28.102), 76 bytes
Sent r2-config to (172.16.28.102),687 bytes
```

## Saving the Configuration Files on The Routers

You must save the running configurations on each router to the startup configuration to ensure that the routers retain their configurations if they are ever power cycled.

### R4

```
R1# telnet 172.16.28.100
Trying 172.16.28.100 ... Open
```

User Access Verification

Password:

R4> enable

Password:

```
R4# copy running-config startup-config
```

Destination filename [startup-config]?

Building configuration...

[OK]

```
R4# exit
```

[Connection to 172.16.28.100 closed by foreign host]

```
R1#
```

### R3

```
R1# telnet 172.16.28.101
Trying 172.16.28.101 ... Open
```

User Access Verification

Password:

R3> enable

Password:

```
R3# copy running-config startup-config
```

Destination filename [startup-config]?

Building configuration...

[OK]

```
R3# exit
```

[Connection to 172.16.28.101 closed by foreign host]

```
R1#
```

### R2

```
R1# telnet 172.16.28.102
Trying 172.16.28.102 ... Open
```

```
User Access Verification

Password:
R2> enable
Password:

R2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2# exit

[Connection to 172.16.28.102 closed by foreign host]
R1#
```

## Removing the Private DHCP Address Pools from R1

The final step in the AutoInstall process is to remove the private DHCP address pools from R1.

```
R1(config)# no ip dhcp pool r4
R1(config)# no ip dhcp pool r3
R1(config)# no ip dhcp pool r2
```

This is the final task, and step for Using AutoInstall to Setup Devices Connected to LANs.

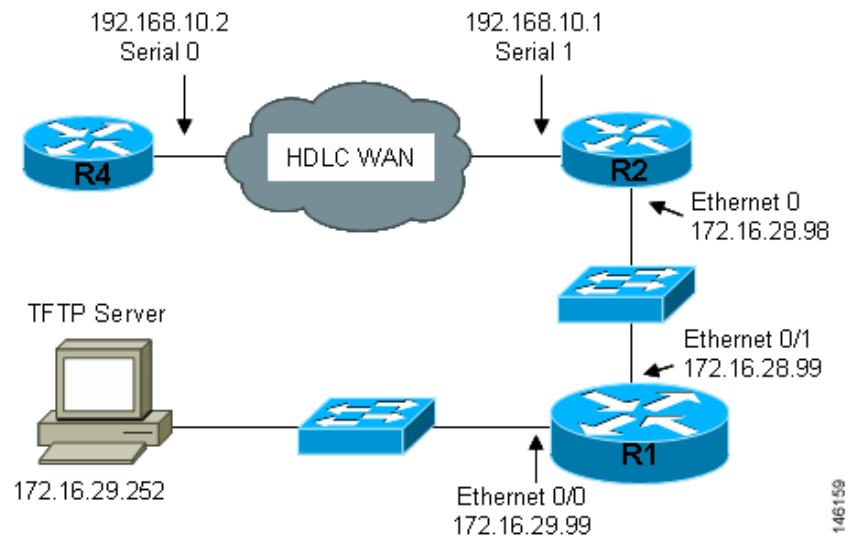
## Using AutoInstall to Set Up Devices Connected to WANs: Example

This section contains the following examples:

- [HDLC WAN Connections, page 26](#)
- [Frame-Relay WAN Connections, page 29](#)

### HDLC WAN Connections

This section uses the network in [Figure 8](#). The section shows how to use AutoInstall to setup R4. R2 will use SLARP to provide R4 the IP address (192.168.20.2) required for AutoInstall.

**Figure 8** Network Topology Using AutoInstall to Configure Routers Connected to HDLC WANs

The process for using AutoInstall to set up router R2 requires the following tasks:

- [Creating the Configuration for R4, page 27](#)
- [Creating the network-config File, page 28](#)
- [Configuring R1 and R2, page 28](#)
- [Setting Up R4 using AutoInstall, page 29](#)
- [Save the Configuration File on R4, page 29](#)

## Creating the Configuration for R4

Create the configuration file for R4 and save it on the TFTP server as r4-config:

```
!
hostname R4
!
enable secret 7gD2A0
!
interface FastEthernet0/0
 ip address 10.89.45.1 255.255.255.0
 no shutdown
!
interface Serial0/0
 ip address 192.168.10.2 255.255.255.0
 no fair-queue
!
router rip
 version 2
 network 168.192.0.0
 no auto-summary
!
ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
line vty 0 4
 password 6T2daX9
```

```
!
end
```

## Creating the network-config File

Create the network configuration file for R4 and save it on the TFTP server as network-config:

```
ip host r4 192.168.10.2
```

## Configuring R1 and R2

Configure R1 and R2 using the following configurations:

### R1

```
!
hostname R1
!
enable secret 7gD2A0
!
interface FastEthernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.16.28.99 255.255.255.0
 ip helper-address 172.16.29.252
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
ip classless
ip http server
!
line vty 0 4
 password 67F2SaB
!
end
```

### R2

```
!
hostname R2
!
enable secret 7gD2A0
!
interface FastEthernet0/0
 ip address 172.16.28.98 255.255.255.0
!
interface Serial0/1
 ip address 192.168.10.1 255.255.255.0
 clockrate 64000
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.10.0
 no auto-summary
!
ip http server
ip classless
```

```
!  
line vty 0 4  
  password u58Hg1  
!  
end
```

## Setting Up R4 using AutoInstall

The network is now ready to use AutoInstall to setup R4. perform the following steps to setup R4.

Connect R4 to the HDLC WAN network.

Power R4 on.

The AutoInstall process should be complete in approximately 5 minutes.

### TFTP Server Log

The TFTP server log should contain messages similar to the following text:

```
Sent network-config to (192.168.10.2), 76 bytes  
Sent r4-config to (192.168.10.2), 687 bytes
```

## Save the Configuration File on R4

You must save the running configurations on R4 to the startup configuration to ensure that R4 retains its configuration if it is ever power cycled.

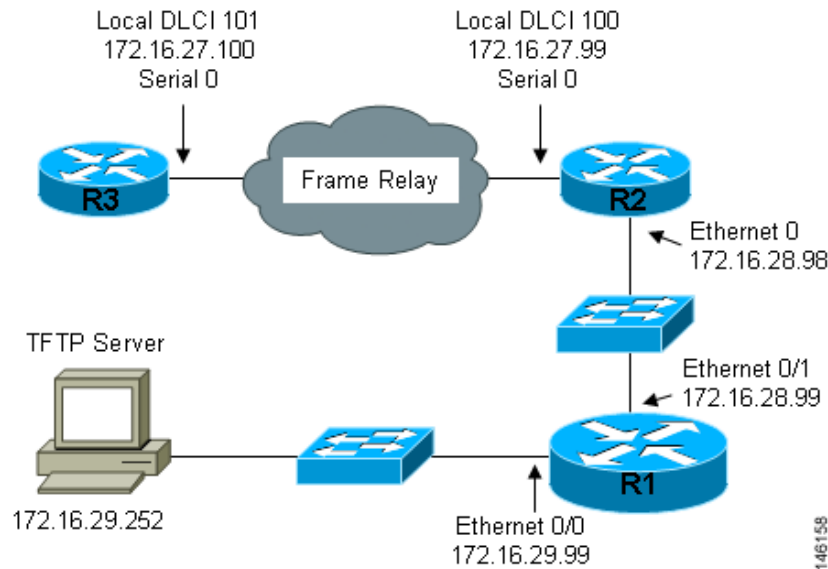
```
R1# telnet 192.168.10.2  
Trying 192.168.10.2 ... Open  
  
User Access Verification  
  
Password:  
R4> enable  
Password:  
  
R4# copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
R4# exit  
  
[Connection to 192.168.10.2 closed by foreign host]  
R1#
```

## Frame-Relay WAN Connections

This section uses the network in [Figure 9](#). The section shows how to use AutoInstall to setup R4. R2 will use BOOTP to provide R4 the IP address (172.16.27.100) required for AutoInstall.

R2 uses 172.16.27.100 as the IP address to provide to R3 using BOOTP because this is the IP address in the **frame-relay map ip 172.16.27.100 100 broadcast** command on serial 0 that points to serial 0 on R3.

**Figure 9** *Network Topology for Using AutoInstall to Configure Routers Connected to Frame Relay WANs*



The process for using AutoInstall to set up router R3 requires the following tasks:

- [Creating the Configuration for R3](#)
- [Creating the network-config File](#)
- [Configuring R1 and R2](#)
- [Setting Up R3 using AutoInstall](#)
- [Saving the Configuration File on R3](#)

### Creating the Configuration for R3

Create the configuration file for R4 and save it on the TFTP server as r3-config:

```
!
hostname R3
!
enable secret 8Hg5Zc20
!
interface FastEthernet0/0
  no ip address
  shutdown
!
interface Serial0/0
  ip address 172.16.27.100 255.255.255.0
  encapsulation frame-relay IETF
  no fair-queue
  frame-relay map ip 172.16.27.99 101 broadcast
  frame-relay interface-dlci 101
!
interface Serial0/1
  no ip address
  shutdown
!
router rip
```

```
version 2
network 172.16.0.0
no auto-summary
!
line vty 0 4
password 67Td3a
login
!
end
```

## Creating the network-config File

Create the network configuration file for R3 and save in on the TFTP server as network-config:

```
ip host r3 172.16.27.100
```

## Configuring R1 and R2

Configure R1 and R2 using the following configurations:

### R1

```
!
hostname R1
!
enable secret 86vC7Z
!
interface FastEthernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.16.28.99 255.255.255.0
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 6Gu8z0s
!
!
end
```

### R2

```
!
hostname R2
!
enable secret 67Hfc5z2
!
interface FastEthernet0/0
 ip address 172.16.28.98 255.255.255.0
 ip helper-address 172.16.29.252
!
interface Serial0/0
 ip address 172.16.27.99 255.255.255.0
 ip helper-address 172.16.29.252
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay map ip 172.16.27.100 100 broadcast
```

```

frame-relay interface-dlci 100
!
interface Serial1
  no ip address
!
router rip
  version 2
  network 172.16.0.0
  no auto-summary
!
line vty 0 4
  password 9Jb6Z3g
!
end

```

## Setting Up R3 using AutoInstall

The network is now ready to use AutoInstall to set up R3. perform the following steps to setup R4.

Connect R3 to the Frame Relay network.

Power R3 on.

The AutoInstall process should be complete in approximately 5 minutes.

### TFTP Server Log

The TFTP server log should contain messages similar to the following text:

```

Sent network-config to (172.16.27.100), 76 bytes
Sent r3-config to (172.16.27.100), 687 bytes

```

## Saving the Configuration File on R3

You must save the running configurations on R3 to the startup configuration to ensure that R3 retains its configuration if it is ever power cycled.

```

R1# telnet 172.16.27.100
Trying 172.16.27.100 ... Open

User Access Verification

Password:
R3> enable
Password:

R3# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit

[Connection to 192.168.10.2 closed by foreign host]
R1#

```



# Additional References

The following sections provide references related to Using AutoInstall to Remotely Configure Cisco Networking Devices.

## Related Documents

Related Topic	Document Title
Overview of Cisco IOS Setup Mode and AutoInstall for configuring Cisco networking devices	<a href="#">Overview: Basic Configuration of a Cisco Networking Device</a>
Using Setup Mode to Configure a Cisco Networking Device	<a href="#">Using Setup Mode to Configure a Cisco Networking Device</a>

## MIBs

MIB	MIBs Link
IF-MIB	<p>The IFNAME object in the IF-MIB can be used to identify the values for the short interface names used in the DHCP Client Identifier for Cisco IOS devices when they are configured as DHCP clients.</p> <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Using AutoInstall to Remotely Configure a Cisco Networking Device

Table 6 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 6 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 6** Feature Information for Using AutoInstall to Remotely Set Up a Cisco Networking Device

Feature Name	Releases	Feature Configuration Information
AutoInstall Using DHCP for LAN Interfaces	Cisco IOS XE Release 2.1	<p>The AutoInstall Using DHCP for LAN Interfaces feature enhances the benefits of AutoInstall by replacing the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces (specifically Fast Ethernet, Token Ring, and FDDI interfaces).</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">AutoInstall Using DHCP for LAN Interfaces</a></li> </ul>

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

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

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

coincidental.

© 2005-2009 Cisco Systems, Inc. All rights reserved.





## **SNMP Support**





# Configuring SNMP Support

---

**First Published: December 20, 2006**

**Last Updated: May 4, 2009**

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

This document discusses how to enable an SNMP agent on a Cisco device and how to control the sending of SNMP notifications from the agent. For information about using SNMP management systems, see the appropriate documentation for your network management system (NMS) application.

## 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 Configuring SNMP Support” section on page 49](#).

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

- [Information About Configuring SNMP Support, page 2](#)
- [How to Configure SNMP Support, page 11](#)
- [Configuration Examples for SNMP Support, page 43](#)
- [Additional References, page 46](#)
- [Feature Information for Configuring SNMP Support, page 49](#)
- [Glossary, page 51](#)



---

**Americas Headquarters:**

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

# Information About Configuring SNMP Support

To configure SNMP support on your network, you should understand the following concepts:

- [Components of SNMP, page 2](#)
- [SNMP Operations, page 3](#)
- [MIBs and RFCs, page 6](#)
- [Versions of SNMP, page 6](#)
- [Detailed Interface Registration Information, page 8](#)
- [SNMP Support for VPNs, page 9](#)
- [Interface Index Persistence, page 9](#)
- [Event MIB, page 10](#)
- [SNMP Notification Logging, page 11](#)

## Components of SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework is made up of three parts:

- SNMP manager
- SNMP agent
- MIB

## SNMP Manager

The SNMP manager is a system that controls and monitors the activities of network hosts using SNMP. The most common managing system is an NMS. The term NMS can be applied either to a dedicated device used for network management or to the applications used on such a device. Several network management applications are available for use with SNMP and range from simple command-line applications to applications that use GUIs, such as the CiscoWorks2000 products.

## SNMP Agent

The SNMP agent is the software component within a managed device that maintains the data for the device and reports this data, as needed, to managing systems. The agent resides on the routing device (router, access server, or switch). To enable an SNMP agent on a Cisco routing device, you must define the relationship between the manager and the agent.

**Note**

---

Commands that an SNMP agent needs to control the SNMP process are available through the Cisco IOS command-line interface (CLI) without additional configuration.

---



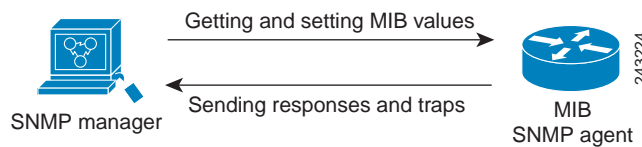
## MIB

A MIB is a virtual information storage area for network management information and consists of collections of managed objects. Within a MIB are collections of related objects defined in MIB modules. MIB modules are written in the SNMP MIB module language, as defined in STD 58, RFC 2578, RFC 2579, and RFC 2580 (see the “[MIBs and RFCs](#)” section for an explanation of RFC and STD documents). Individual MIB modules are also referred to as MIBs; for example, the Interfaces Group MIB (IF-MIB) is a MIB module within the MIB on your system.

An SNMP agent contains MIB variables whose values the SNMP manager can request or change through Get or Set operations. A manager can get a value from an agent or store a value in that agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to manager requests to get or set data.

[Figure 1](#) illustrates the communications between the SNMP manager and agent. A manager sends an agent requests to get and set MIB values. The agent responds to these requests. Independent of this interaction, the agent can send the manager unsolicited notifications (traps or informs) to notify the manager about network conditions.

**Figure 1**      **Communication Between an SNMP Agent and Manager**



## SNMP Operations

SNMP applications perform the following operations to retrieve data, modify SNMP object variables, and send notifications:

- Get
- Set
- Send notifications

### SNMP Get

The SNMP get operation is performed by an NMS to retrieve SNMP object variables. There are three types of get operations:

- get—Retrieves the exact object instance from the SNMP agent.
- getNext—Retrieves the next object variable, which is a lexicographical successor to the specified variable.
- getBulk—Retrieves a large amount of object variable data, without the need for repeated getNext operations.

### SNMP Set

The SNMP set operation is performed by an NMS to modify the value of an object variable.

## SNMP Notifications

A key feature of SNMP is its capability to generate unsolicited notifications from an SNMP agent.

### Traps and Informs

Unsolicited (asynchronous) notifications can be generated as traps or inform requests (informs). Traps are messages alerting the SNMP manager to a condition on the network. Informs are traps that include a request for confirmation of receipt from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

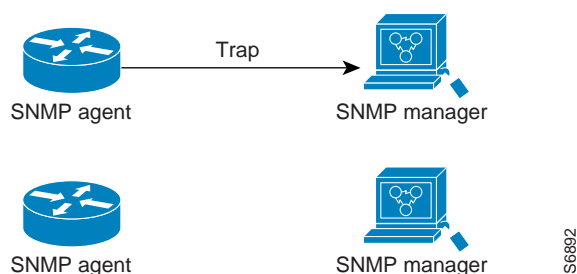
Traps are less reliable than informs because the receiver does not send an acknowledgment when it receives a trap. The sender does not know if the trap was received. An SNMP manager that receives an inform acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives a response, the inform can be sent again. Thus, informs are more likely to reach their intended destination.

Traps are often preferred even though they are less reliable because informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform must be held in memory until a response is received or the request times out. Also, traps are sent only once, whereas an inform may be resent several times. The retries increase traffic and contribute to higher overhead on the network. Use of traps and informs requires a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use informs, but if traffic volume or memory usage are concerns and receipt of every notification is not required, use traps.

Figure 2 through Figure 5 illustrate the differences between traps and informs.

Figure 2 shows that an agent successfully sends a trap to an SNMP manager. Although the manager receives the trap, it does not send an acknowledgment. The agent has no way of knowing that the trap reached its destination.

**Figure 2** *Trap Successfully Sent to SNMP Manager*



In Figure 3, the agent successfully sends an inform to the manager. When the manager receives the inform, a response is sent to the agent and the agent knows that the inform reached its destination. Notice that in this example the traffic generated is twice as much as in the interaction shown in Figure 2.

**Figure 3** Inform Request Successfully Sent to SNMP Manager

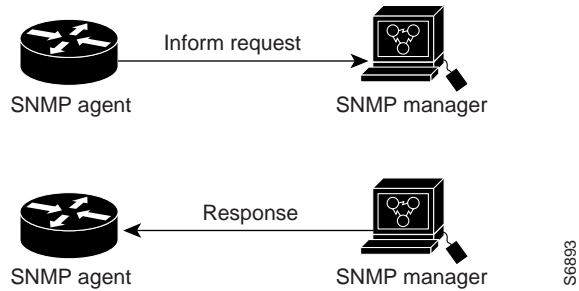


Figure 4 shows an agent sending a trap to a manager that the manager does not receive. The agent has no way of knowing that the trap did not reach its destination. The manager never receives the trap because traps are not resent.

**Figure 4** Trap Unsuccessfully Sent to SNMP Manager

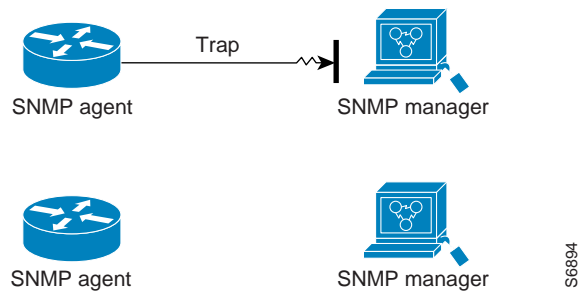
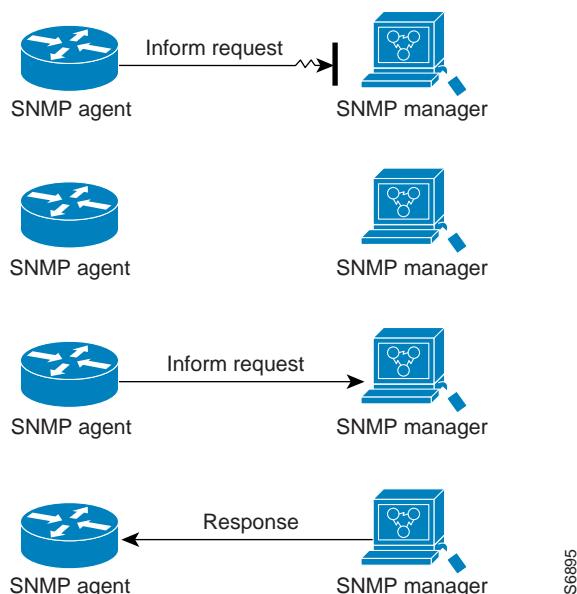


Figure 5 shows an agent sending an inform to a manager that does not reach the manager. Because the manager did not receive the inform, it does not send a response. After a period of time, the agent resends the inform. The manager receives the inform from the second transmission and replies. In this example, more traffic is generated than in the scenario shown in Figure 4 but the notification reaches the SNMP manager.

**Figure 5** *Inform Unsuccessfully Sent to SNMP Manager*

## MIBs and RFCs

MIB modules typically are defined in RFC documents submitted to the Internet Engineering Task Force (IETF), an international standards body. RFCs are written by individuals or groups for consideration by the Internet Society and the Internet community as a whole, usually with the intention of establishing a recommended Internet standard. Before being given RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. You can learn about the standards process and the activities of the IETF at the Internet Society website at <http://www.isoc.org>. You can read the full text of all RFCs, I-Ds, and STDs referenced in Cisco documentation at the IETF website at <http://www.ietf.org>.

The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213 and definitions of SNMP traps described in RFC 1215.

Cisco provides its own private MIB extensions with every system. Cisco enterprise MIBs comply with the guidelines described in the relevant RFCs unless otherwise noted in the documentation. You can find the MIB module definition files and list of MIBs supported on each Cisco platform on the Cisco MIB website on [Cisco.com](http://www.cisco.com).

## Versions of SNMP

Cisco IOS XE software supports the following versions of SNMP:

- **SNMPv1**—Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- **SNMPv2c**—The community string-based Administrative Framework for SNMPv2. SNMPv2c (the “c” is for “community”) is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.

- **SNMPv3**—Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 3413 to 3415. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are as follows:

- **Message integrity**—Ensuring that a packet has not been tampered with in transit.
- **Authentication**—Determining that the message is from a valid source.
- **Encryption**—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by a community string.

SNMPv2c support includes a bulk retrieval mechanism and detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round trips required. The SNMPv2c improved error handling support includes expanded error codes that distinguish different types of errors; these conditions are reported through a single error code in SNMPv1. The following three types of exceptions are also reported: no such object, no such instance, and end of MIB view.

SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. [Table 1](#) lists the combinations of security models and levels and their meanings.

**Table 1** *SNMP Security Models and Levels*

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

You must configure an SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers, however, and you can configure Cisco IOS XE software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

SNMPv3 supports RFCs 1901 to 1908, 2104, 2206, 2213, 2214, and 2271 to 2275. For additional information about SNMPv3, see RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework* (this is not a standards document).

## Detailed Interface Registration Information

The Interface Index Display for SNMP feature introduces new commands and command modifications that allow advanced users of SNMP to view information about the interface registrations directly on the managed agent. You can display MIB information from the agent without using an external NMS.



### Note

---

For the purposes of this document, the agent is a routing device running Cisco IOS XE software.

---

This feature addresses three objects in the Interfaces MIB: ifIndex, ifAlias, and ifName. For a complete definition of these objects, see the IF-MIB.my file available from the Cisco SNMPv2 MIB website at <ftp://ftp.cisco.com/pub/mibs/v2/>.

## Interface Index

The ifIndex object (ifEntry 1) is called the Interface Index. The Interface Index is a unique value greater than zero that identifies each interface or subinterface on the managed device. This value becomes the interface index identification number.

The CLI command **show snmp mib ifmib ifindex** allows you to view the SNMP Interface Index Identification numbers assigned to interfaces and subinterfaces. An NMS is not required.

## Interface Alias

The ifAlias object (ifXEntry 18) is called the Interface Alias. The Interface Alias is a user-specified description of an interface used for SNMP network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB) that can be set by a network manager to “name” an interface. The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode or subinterface configuration mode or by using a Set operation from an NMS. Previously, ifAlias descriptions for subinterfaces were limited to 64 characters. (The OLD-CISCO-INTERFACES-MIB allows up to 255 characters for the locIfDescr MIB variable, but this MIB does not support subinterfaces.) A new CLI command, **snmp ifmib ifalias long**, configures the system to handle IfAlias descriptions of up to 256 characters. IfAlias descriptions appear in the output of the CLI **show interfaces** command.

## Interface Name

The ifName object (ifXEntry 1) is the textual name of the interface. The purpose of the ifName object is to cross reference the CLI representation of a given interface. The value of this object is the name of the interface as assigned by the local device and is generally suitable for use in CLI commands. If there

is no local name or this object is otherwise not applicable, this object contains a zero-length string. No commands introduced by this feature affect the ifName object, but it is discussed here to show its relation to the ifIndex and ifAlias objects.

The **show snmp mib** command shows all objects in the MIB on a Cisco device (similar to a mibwalk). The objects in the MIB tree are sorted using lexical ordering, meaning that object identifiers are sorted in sequential, numerical order. Lexical ordering is important when using the GetNext operation from an NMS because these operations take an object identifier (OID) or a partial OID as input and return the next object from the MIB tree based on the lexical ordering of the tree.

## SNMP Support for VPNs

The SNMP Support for VPNs feature allows SNMP traps and informs to be sent and received using virtual private network (VPN) routing/forwarding (VRF) tables. In particular, this feature adds support to Cisco IOS XE software for the sending and receiving of SNMP traps and informs specific to individual VPNs.

A VPN is a network that provides high connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet over IP, Frame Relay, or ATM networks.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support for VPNs feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used for sending SNMP traps and informs and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

Support for VPNs allows you to configure an SNMP agent to accept only SNMP requests from a certain set of VPNs. With this configuration, service providers can provide network management services to their customers, so customers can manage all user VPN devices.

## Interface Index Persistence

One of the identifiers most commonly used in SNMP-based network management applications is the interface index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the “name” of the interface.

Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

This feature adds support for an ifIndex value that can persist across reboots, allowing users to avoid the workarounds previously required for consistent interface identification.

It is currently possible to poll the router at regular intervals to correlate the interfaces to the ifIndex, but it is not practical to poll this interface constantly. If this data is not correlated constantly, however, the data may be made invalid because of a reboot or the insertion of a new card into the router in between polls. Therefore, ifIndex persistence is the only way to guarantee data integrity.

IfIndex persistence means that the mapping between the ifDescr object values and the ifIndex object values (generated from the IF-MIB) will be retained across reboots.

## Benefits of Interface Index Persistence

### Association of Interfaces with Traffic Targets for Network Management

The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity (such as an ISP customer) allows network management data to be more effectively utilized.

### Accuracy for Mediation, Fault Detection, and Billing

Network data is increasingly being used worldwide for usage-based billing, network planning, policy enforcement, and trend analysis. The ifIndex information is used to identify input and output interfaces for traffic flows and SNMP statistics. Inability to reliably relate each interface to a known entity, such as a customer, invalidates the data.

## Event MIB

The Event MIB provides the ability to monitor MIB objects on a local or remote system using SNMP and initiate simple actions whenever a trigger condition is met; for example, an SNMP trap can be generated when an object is modified. When the notifications are triggered through events, the NMS does not need to constantly poll managed devices to track changes.

By allowing the SNMP notifications to take place only when a specified condition is met, Event MIB reduces the load on affected devices and improves the scalability of network management solutions.

The Event MIB operates based on event, object lists configured for the event, event action, trigger, and trigger test.

## Events

The event table defines the activities to be performed when an event is triggered. These activities include sending a notification and setting a MIB object. The event table has supplementary tables for additional objects that are configured according to event action. If the event action is set to notification, notifications are sent out whenever the object configured for that event is modified.

## Object List

The object table lists objects that can be added to notifications based on trigger, trigger test type, or the event that sends a notification. The Event MIB allows wildcarding, which enables you to monitor multiple instances of an object. To specify a group of object identifiers, you can use the wildcard option.

## Trigger

The trigger table defines conditions to trigger events. The trigger table lists the objects to be monitored and associates each trigger with an event. An event occurs when a trigger is activated. To create a trigger, you should configure a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the object identifier of the object to be monitored. Each trigger is configured to monitor a single object or a group of objects specified by a wildcard (\*). The Event MIB process checks the state of the monitored object at specified intervals.



## Trigger Test

The trigger table has supplementary tables for additional objects that are configured based on the type of test performed for a trigger. For each trigger entry type such as existence, threshold, or Boolean, the corresponding tables (existence, threshold, and Boolean tables) are populated with the information required to perform the test. Event MIB allows you to set event triggers based on existence, threshold, and Boolean trigger types. When the specified test on an object returns a value of *true*, the trigger is activated. You can configure Event MIB to send out notifications to the interested host when a trigger is activated.

## SNMP Notification Logging

Systems that support SNMP often need a mechanism for recording notification information. This mechanism protects against notifications being lost because they exceeded retransmission limits. The Notification Log MIB provides a common infrastructure for other MIBs in the form of a local logging function. The SNMP Notification Logging feature adds Cisco IOS CLI commands to change the size of the notification log, to set the global ageout value for the log, and to display logging summaries at the command line. The Notification Log MIB improves notification tracking and provides a central location for tracking all MIBs.

**Note**

---

The Notification Log MIB supports notification logging on the default log only.

---

## How to Configure SNMP Support

There is no specific command that you use to enable SNMP. The first **snmp-server** command that you enter enables the supported versions of SNMP. All other configurations are optional.

Perform the following tasks to configure SNMP support.

- [Configuring System Information, page 12](#) (optional)
- [Configuring SNMP Versions 1 and 2, page 13](#) (optional)
- [Configuring SNMP Version 3, page 18](#) (optional)
- [Configuring a Router as an SNMP Manager, page 22](#) (optional)
- [Enabling the SNMP Agent Shutdown Mechanism, page 25](#) (optional)
- [Defining the Maximum SNMP Agent Packet Size, page 25](#) (optional)
- [Limiting the Number of TFTP Servers Used via SNMP, page 26](#) (optional)
- [Disabling the SNMP Agent, page 27](#) (optional)
- [Configuring SNMP Notifications, page 28](#) (optional)
- [Configuring Interface Index Display and Interface Indexes and Long Name Support, page 34](#) (optional)
- [Configuring Interface Index Persistence, page 37](#) (optional)
- [Configuring SNMP Support for VPNs, page 40](#) (optional)
- [Configuring Event MIB, page 41](#)

## Configuring System Information

You can set the system contact, location, and serial number of the SNMP agent so that these descriptions can be accessed through the configuration file. Although the configuration steps described in this section are optional, configuring the basic information is recommended because it may be useful when troubleshooting your configuration. In addition, the first **snmp-server** command that you issue enables SNMP on the device.

Perform this task as needed.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server contact** *text*
4. **snmp-server location** *text*
5. **snmp-server chassis-id** *number*
6. **exit**
7. **show snmp contact**
8. **show snmp location**
9. **show snmp chassis**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server contact</b> <i>text</i>  <b>Example:</b> Router(config)# snmp-server contact NameOne	Sets the system contact string.
Step 4	<b>snmp-server location</b> <i>text</i>  <b>Example:</b> Router(config)# snmp-server location LocationOne	Sets the system location string.
Step 5	<b>snmp-server chassis-id</b> <i>number</i>  <b>Example:</b> Router(config)# snmp-server chassis-id 015A619T	Sets the system serial number.

	Command or Action	Purpose
Step 6	<code>exit</code>  <b>Example:</b> <code>Router(config)# exit</code>	Exits global configuration mode.
Step 7	<code>show snmp contact</code>  <b>Example:</b> <code>Router# show snmp contact</code>	(Optional) Displays the contact strings configured for the system.
Step 8	<code>show snmp location</code>  <b>Example:</b> <code>Router# show snmp location</code>	(Optional) Displays the location string configured for the system.
Step 9	<code>show snmp chassis</code>  <b>Example:</b> <code>Router# show snmp chassis</code>	(Optional) Displays the system serial number.

## Configuring SNMP Versions 1 and 2

When you configure SNMP versions 1 and 2, you can optionally create or modify views for community strings to limit which MIB objects an SNMP manager can access.

Perform the following tasks when configuring SNMP version 1 or version 2.

- [Creating or Modifying an SNMP View Record, page 13](#) (optional)
- [Creating or Modifying Access Control for an SNMP Community, page 15](#) (required)
- [Configuring a Recipient of an SNMP Trap Operation, page 16](#) (required)

### Prerequisites

- An established SNMP community string that defines the relationship between the SNMP manager and the agent
- A host defined to be the recipient of SNMP notifications

### Creating or Modifying an SNMP View Record

You can assign views to community strings to limit which MIB objects an SNMP manager can access. You can use a predefined view or create your own view. If you are using a predefined view or no view at all, skip this task.

Perform this task to create or modify an SNMP view record.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `snmp-server view view-name oid-tree {included | excluded}`

4. **no snmp-server view** *view-name oid-tree* {**included** | **excluded**}
5. **exit**
6. **show snmp view**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server view</b> <i>view-name oid-tree</i> { <b>included</b>   <b>excluded</b> }  <b>Example:</b> Router(config)# snmp-server view mib2 mib-2 included	Creates a view record. <ul style="list-style-type: none"> <li>In this example, the mib2 view that includes all objects in the MIB-II subtree is created.</li> </ul> <b>Note</b> You can use this command multiple times to create the same view record. If a view record for the same OID value is created multiple times, the latest entry of the object identifier takes precedence.
Step 4	<b>no snmp-server view</b> <i>view-name oid-tree</i> { <b>included</b>   <b>excluded</b> }  <b>Example:</b> Router(config)# no snmp-server view mib2 mib-2 included	Removes a server view.
Step 5	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 6	<b>show snmp view</b>  <b>Example:</b> Router# show snmp view	(Optional) Displays a view of the MIBs associated with SNMP.

## Examples

The following example shows the SNMP view for the system.1.0 OID tree:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server view test system 1.0 included
Router(config)# exit
```

```
Router# show snmp view
```

```
test system.1.0 - included nonvolatile active
*ilmi system - included permanent active
```

```
*ilmi atmForumUni - included permanent active
vldefault iso - included permanent active
vldefault internet - included permanent active
vldefault snmpUsmMIB - excluded permanent active
vldefault snmpVacmMIB - excluded permanent active
vldefault snmpCommunityMIB - excluded permanent active
vldefault ciscoIpTapMIB - excluded permanent active
vldefault ciscoMgmt.395 - excluded permanent active
vldefault ciscoTap2MIB - excluded permanent active
```

## Creating or Modifying Access Control for an SNMP Community

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the router. Optionally, you can specify one or more of the following characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.
- A MIB view, which defines the subset of all MIB objects accessible to the given community.
- Read and write or read-only permission for the MIB objects accessible to the community.

Perform this task to create or modify a community string.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6 nacl**] [*access-list-number*]
4. **no snmp-server community** *string*
5. **exit**
6. **show snmp community**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <b>ipv6 nacl</b> ] [ <i>access-list-number</i> ]	Defines the community access string.
	<b>Example:</b> Router(config)# snmp-server community comaccess ro 4	<ul style="list-style-type: none"> <li>• You can configure one or more community strings.</li> </ul>

	Command or Action	Purpose
Step 4	<code>no snmp-server community string</code>  <b>Example:</b> Router(config)# no snmp-server community comaccess	Removes the community string from the configuration.
Step 5	<code>exit</code>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 6	<code>show snmp community</code>  <b>Example:</b> Router# show snmp community	(Optional) Displays the community access strings configured for the system.

## Examples

The following example shows the community access strings configured to enable access to the SNMP manager:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community public ro
Router(config)# snmp-server community private rw
Router(config)# exit

Router# show snmp community

Community name: private
Community Index: private
Community SecurityName: private
storage-type: nonvolatile      active

Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile      active
```

## Configuring a Recipient of an SNMP Trap Operation

SNMP traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender does not know if the traps were received. However, a SNMP entity that receives an inform acknowledges the message with a SNMP response protocol data unit (PDU). If the sender never receives the response, the inform can be sent again. Thus, informs are more likely to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be sent several times. The retries increase traffic and overhead on the network.

If you do not enter a **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command without keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled and others are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** interface configuration command. These notification types do not require an **snmp-server enable** command.

A *notification-type* option's availability depends on the router type and Cisco IOS XE software features supported on the router. For example, the Cisco IOS XE software does not support the envmon notification type. To see what notification types are available on your system, use the command help (?) at the end of the **snmp-server host** command.

Perform this task to configure the recipient of an SNMP trap operation.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-id* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port-number*] [*notification-type*]
4. **exit**
5. **show snmp host**

## DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<pre>snmp-server host host-id [traps   informs][version {1   2c   3 [auth   noauth   priv]] community-string [udp-port port-number] [notification-type]</pre> <p><b>Example:</b> Router(config)# snmp-server host 172.16.1.27 version 2c public</p>	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.
Step 4	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode.
Step 5	<pre>show snmp host</pre> <p><b>Example:</b> Router# show snmp host</p>	(Optional) Displays the SNMP notifications sent as traps, the version of SNMP, and the host IP address of the notifications.

## Examples

The following example shows the host information configured for SNMP notifications:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host 10.2.28.1 inform version 2c public
Router(config)# exit

Router# show snmp host

Notification host: 10.2.28.1 udp-port: 162   type: inform
user: public   security model: v2c
```

## Configuring SNMP Version 3

When you configure SNMP version 3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords.

Perform the following tasks to configure SNMP version 3.

- [Specifying SNMP-Server Group Names, page 18](#)(required)
- [Configuring SNMP Server Users, page 20](#) (required)

### Specifying SNMP-Server Group Names

SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a MD5 password, see the documentation for the **snmp-server user** command.

Perform this task to specify a new SNMP group or a table that maps SNMP users to SNMP views.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server group** [*groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
4. **exit**
5. **show snmp group**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server group</b> [ <i>groupname</i> { <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]}}] [ <b>read</b> <i>readview</i> ] [ <b>write</b> <i>writeview</i> ] [ <b>notify</b> <i>notifyview</i> ] [ <b>access</b> <i>access-list</i> ]  <b>Example:</b> Router(config)# snmp-server group group1 v3 auth access lmnop	Configures the SNMP server group to enable authentication for members of a specified named access list. <ul style="list-style-type: none"> <li>In this example, the SNMP server group <i>group1</i> is configured to enable user authentication for members of the named access list <i>lmnop</i>.</li> </ul>
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 5	<b>show snmp group</b>  <b>Example:</b> Router# show snmp group	Displays information about each SNMP group on the network.

## Examples

The following example shows information about each SNMP group on the network:

```
Router# show snmp group
```

```

groupname: ILMI                      security model:v1
readview : *ilmi                     writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                      security model:v2c
readview : *ilmi                     writeview: *ilmi
notifyview: <no notifyview specified>
```

```

row status: active

groupname: group1
readview : vldefault
notifyview: <no notifyview specified>
row status: active

groupname: public
readview : <no readview specified>
notifyview: <no notifyview specified>
row status: active

security model:v3 auth
writeview: <no writeview specified>

access-list:lmnop

security model:v1
writeview: <no writeview specified>

```

## Configuring SNMP Server Users

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the remote option. The remote agent's SNMP engine ID is required when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password* arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You must configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

## Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although we recommend using at least eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain text password or a localized MD5 digest.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets in length.

Perform this task to add a new user to an SNMP group.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username groupname* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]
4. **exit**
5. **show snmp user** [*username*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server user</b> <i>username groupname</i> [ <b>remote</b> <i>ip-address</i> [ <b>udp-port</b> <i>port</i> ]] { <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>encrypted</b> ] [ <b>auth</b> { <b>md5</b>   <b>sha</b> } <i>auth-password</i> ]} [ <b>access</b> <i>access-list</i> ]  <b>Example:</b> Router(config)# snmp-server user user1 group1 v3 auth md5 password123	Configures a new user to an SNMP group with the plain text password “password123” for the user “user1” in the SNMPv3 group “group1”.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	<b>show snmp user</b> [ <i>username</i> ]  <b>Example:</b> Router# show snmp user user1	Displays the information about the configured characteristics of an SNMP user.

## Examples

The following example shows the information about the configured characteristics of the SNMP user1:

```
Router# show snmp user user1

User name: user1
Engine ID: 00000009020000000C025808
storage-type: nonvolatile      active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: None
Group name: group1
```

## Configuring a Router as an SNMP Manager

The SNMP manager feature allows a router to act as a network management station—an SNMP client. As an SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

### Security Considerations

Most network security policies assume that routers will accept SNMP requests, send SNMP responses, and send SNMP notifications.

With the SNMP manager functionality enabled, the router may also send SNMP requests, receive SNMP responses, and receive SNMP notifications. Your security policy implementation may need to be updated prior to enabling this feature.

SNMP requests typically are sent to User Datagram Protocol (UDP) port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

### SNMP Sessions

Sessions are created when the SNMP manager in the router sends SNMP requests, such as informs, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

Sessions consume memory. A reasonable session timeout value should be large enough that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used or one-time sessions are purged expeditiously.

### Enabling the SNMP Manager

Perform this task to enable the SNMP manager process and to set the session timeout value.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server manager**
4. **snmp-server manager session-timeout** *seconds*
5. **exit**
6. **show snmp**
7. **show snmp sessions** [*brief*]
8. **show snmp pending**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server manager</b>  <b>Example:</b> Router(config)# snmp-server manager	Enables the SNMP manager.
Step 4	<b>snmp-server manager session-timeout seconds</b>  <b>Example:</b> Router(config)# snmp-server manager session-timeout 30	(Optional) Changes the session timeout value.
Step 5	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 6	<b>show snmp</b>  <b>Example:</b> Router# show snmp	(Optional) Displays the status of SNMP communications.
Step 7	<b>show snmp sessions [brief]</b>  <b>Example:</b> Router# show snmp sessions	(Optional) Displays displays the status of SNMP sessions.
Step 8	<b>show snmp pending</b>  <b>Example:</b> Router# show snmp pending	(Optional) Displays the current set of pending SNMP requests.

## Examples

The following example shows the status of SNMP communications:

```
Router# show snmp
```

```
Chassis: 01506199
```

```
37 SNMP packets input
 0 Bad SNMP version errors
 4 Unknown community name
 0 Illegal operation for community name supplied
 0 Encoding errors
```

```

    24 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    28 Get-next PDUs
    0 Set-request PDUs

78 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    24 Response PDUs
    13 Trap PDUs

SNMP logging: enabled
    Logging to 172.17.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
    0 Drops

SNMP Manager-role input packets
    0 Inform response PDUs
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors

SNMP informs: enabled
    Informs in flight 0/25 (current/max)
    Logging to 172.17.217.141.162
        4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
    Logging to 172.17.58.33.162
        0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped

```

The following example displays the status of SNMP sessions:

```

Router# show snmp sessions

Destination: 172.17.58.33.162, V2C community: public
Round-trip-times: 0/0/0 (min/max/last)
packets output
    0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
    0 Timeouts, 0 Drops
packets input
    0 Traps, 0 Informs, 0 Responses (0 errors)

Destination: 172.17.217.141.162, V2C community: public, Expires in 575 secs
Round-trip-times: 1/1/1 (min/max/last)
packets output
    0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
    0 Timeouts, 0 Drops
packets input
    0 Traps, 0 Informs, 4 Responses (0 errors)

```

The following example shows the current set of pending SNMP requests:

```

Router# show snmp pending

```

```

req id: 47, dest: 172.17.58.33.161, V2C community: public, Expires in 5 secs

req id: 49, dest: 172.17.58.33.161, V2C community: public, Expires in 6 secs

req id: 51, dest: 172.17.58.33.161, V2C community: public, Expires in 6 secs

req id: 53, dest: 172.17.58.33.161, V2C community: public, Expires in 8 secs

```

## Enabling the SNMP Agent Shutdown Mechanism

Using SNMP packets, a network management tool can send messages to users on virtual terminals and on the console. This facility operates in a similar fashion to the **send EXEC** command; however, the SNMP request that causes the message to be issued to the users also specifies the action to be taken after the message is delivered. One possible action is a shutdown request. After a system is shut down, typically it is reloaded. Because the ability to cause a reload from the network is a powerful feature, it is protected by the **snmp-server system-shutdown** global configuration command. If you do not issue this command, the shutdown mechanism is not enabled.

Perform this task to enable the SNMP agent shutdown mechanism.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server system-shutdown**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server system-shutdown</b>  <b>Example:</b> Router(config)# snmp-server system-shutdown	Enables system shutdown using the SNMP message reload feature.

## Defining the Maximum SNMP Agent Packet Size

You can define the maximum packet size permitted when the SNMP agent is receiving a request or generating a reply.

Perform this task to set the maximum permitted packet size.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **snmp-server packetsize** *byte-count*

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>snmp-server packetsize</b> <i>byte-count</i>	Establishes the maximum packet size.
	<b>Example:</b> Router(config)# snmp-server packetsize 512	

**Limiting the Number of TFTP Servers Used via SNMP**

You can limit the number of TFTP servers used for saving and loading configuration files via SNMP by using an access list. Limiting the use of TFTP servers in this way conserves system resources and centralizes the operation for manageability.

Perform this task to limit the number of TFTP servers.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **snmp-server tftp-server-list** *number*



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server tftp-server-list number</b>  <b>Example:</b> Router(config)# snmp-server tftp-server-list 12	Limits the number of TFTP servers used for configuration file copies via SNMP to the servers in an access list.

## Troubleshooting Tips

To monitor SNMP trap activity in real time for the purposes of troubleshooting, use the SNMP **debug** commands, including the **debug snmp packet** EXEC command. For documentation of SNMP **debug** commands, see the *Cisco IOS Debug Command Reference*.

## Disabling the SNMP Agent

Perform this task to disable any version of an SNMP agent.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no snmp-server**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>no snmp-server</b>  <b>Example:</b> Router(config)# no snmp-server	Disables SNMP agent operation.

## Configuring SNMP Notifications

To configure a router to send SNMP traps or informs, perform the tasks described in the following sections:

- [Configuring the Router to Send SNMP Notifications, page 28](#) (required)
- [Changing Notification Operation Values, page 30](#) (optional)
- [Controlling Individual RFC 1157 SNMP Traps, page 31](#) (optional)
- [Configuring SNMP Notification Log Options, page 33](#) (optional)

**Note**

Many snmp-server commands use the word traps in their command syntax. Unless there is an option within the command to specify either traps or informs, the keyword **traps** should be taken to mean traps, informs, or both. Use the **snmp-server host** command to specify whether you want SNMP notifications to be sent as traps or informs.

To use informs, the SNMP manager (also known as the SNMP proxy manager) must be available and enabled on the device. Earlier, the SNMP manager was available only with Cisco IOS PLUS images. However, the SNMP manager is now available with all Cisco IOS XE releases that support SNMP.

Use Cisco Feature Navigator for information about SNMP manager support for Cisco IOS XE releases. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

## Configuring the Router to Send SNMP Notifications

Perform this task to configure the router to send traps or informs to a host.

## SUMMARY STEPS

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

3. **snmp-server user** *username groupname* [**remote** *host* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]
4. **snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
5. **snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [*notification-type*]
6. **snmp-server enable traps** [*notification-type*] [*notification-options*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server user</b> <i>username groupname</i> [ <b>remote</b> <i>host</i> [ <b>udp-port</b> <i>port</i> ] { <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>encrypted</b> ] [ <b>auth</b> { <b>md5</b>   <b>sha</b> } <i>auth-password</i> ]} [ <b>access</b> <i>access-list</i> ]  <b>Example:</b> Router(config)# snmp-server user abcd public v3 encrypted auth md5 cisco123	Configures a local or remote user to an SNMP group.  <b>Note</b> You cannot configure a remote user for an address without first configuring the engine ID for that remote host. This restriction is imposed in the design of these commands; if you try to configure the user before the host, you will receive a warning message and the command will not be executed. Use the <b>snmp-server engineid remote</b> command to specify the engine ID for a remote host.
Step 4	<b>snmp-server group</b> <i>groupname</i> { <b>v1</b>   <b>v2c</b>   <b>v3</b> { <b>auth</b>   <b>noauth</b>   <b>priv</b> }} [ <b>read</b> <i>readview</i> ] [ <b>write</b> <i>writeview</i> ] [ <b>notify</b> <i>notifyview</i> ] [ <b>access</b> <i>access-list</i> ]  <b>Example:</b> Router(config)# snmp-server group GROUP1 v2c auth read viewA write viewA notify viewB	Configures an SNMP group.

	Command or Action	Purpose
Step 5	<pre>snmp-server host host [traps   informs] [version {1   2c   3 [auth   noauth   priv]]] community-string [notification-type]</pre> <p><b>Example:</b> Router(config)# snmp-server host example.com informs version 3 public</p>	<p>Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.</p> <ul style="list-style-type: none"> <li>The <b>snmp-server host</b> command specifies which hosts will receive SNMP notifications, and whether you want the notifications sent as traps or informs.</li> </ul>
Step 6	<pre>snmp-server enable traps [notification-type [notification-options]]</pre> <p><b>Example:</b> Router(config)# snmp-server enable traps bgp</p>	<p>Enables sending of traps or informs and specifies the type of notifications to be sent.</p> <ul style="list-style-type: none"> <li>If a <i>notification-type</i> is not specified, all supported notification will be enabled on the router.</li> <li>To discover which notifications are available on your router, enter the <b>snmp-server enable traps ?</b> command.</li> <li>The <b>snmp-server enable traps</b> command globally enables the production mechanism for the specified notification types (such as Border Gateway Protocol [BGP] traps, config traps, entity traps, Hot Standby Router Protocol [HSRP] traps, and so on).</li> </ul>

## Changing Notification Operation Values

You can specify a value other than the default for the source interface, message (packet) queue length for each host, or retransmission interval.

Perform this task to change notification operation values as needed.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server trap-source** *interface*
4. **snmp-server queue-length** *length*
5. **snmp-server trap-timeout** *seconds*
6. **snmp-server informs** [*retries retries*] [*timeout seconds*] [*pending pending*]

### DETAILED STEPS

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

<b>Step 3</b>	<pre>snmp-server trap-source interface</pre> <p><b>Example:</b> Router(config)# snmp-server trap-source FastEthernet 2/1</p>	Sets the IP address for the Fast Ethernet interface in slot2, port 1 as the source for all SNMP notifications.
<b>Step 4</b>	<pre>snmp-server queue-length length</pre> <p><b>Example:</b> Router(config)# snmp-server queue-length 50</p>	Establishes the message queue length for each notification. <ul style="list-style-type: none"> <li>This example shows the queue length set to 50 entries.</li> </ul>
<b>Step 5</b>	<pre>snmp-server trap-timeout seconds</pre> <p><b>Example:</b> Router(config)# snmp-server trap-timeout 30</p>	Defines how often to resend notifications on the retransmission queue.
<b>Step 6</b>	<pre>snmp-server informs [retries retries] [timeout seconds] [pending pending]</pre> <p><b>Example:</b> Router(config)# snmp-server informs retries 10 timeout 30 pending 100</p>	Configures inform-specific operation values. <ul style="list-style-type: none"> <li>This example sets the maximum number of times to resend an inform, the number of seconds to wait for an acknowledgment before resending, and the maximum number of informs waiting for acknowledgments at any one time.</li> </ul>

## Controlling Individual RFC 1157 SNMP Traps

You can globally enable or disable authenticationFailure, linkUp, linkDown, warmStart, and coldStart traps or informs individually. (These traps constitute the “generic traps” defined in RFC 1157.) Note that linkUp and linkDown notifications are enabled by default on specific interfaces but will not be sent unless they are enabled globally.

Perform this task to enable the authenticationFailure, linkUp, linkDown, warmStart, and coldStart notification types.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps snmp [authentication] [linkup] [linkdown] [warmstart] [coldstart]**
4. **interface type slot/port**
5. **no snmp-server link-status**
6. **exit**
7. **exit**

## DETAILED STEPS

Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<pre>snmp-server enable traps snmp [authentication] [linkup] [linkdown] [warmstart] [coldstart]</pre> <p><b>Example:</b> Router(config)# snmp-server enable traps snmp</p>	<p>Enables RFC 1157 generic traps.</p> <ul style="list-style-type: none"> <li>When used without any of the optional keywords, enables authenticationFailure, linkUp, linkDown, warmStart, and coldStart traps.</li> <li>When used with keywords, enables only the trap types specified. For example, to globally enable only linkUp and linkDown SNMP traps or informs for all interfaces, use the <b>snmp-server enable traps snmp linkup linkdown</b> form of this command.</li> </ul>
Step 4	<pre>interface type slot/port</pre> <p><b>Example:</b> Router(config)# interface FastEthernet 0/0</p>	<p>Enters interface configuration mode for a specific interface.</p> <p><b>Note</b> To enable SNMP traps for individual interfaces such as Dialer, use the <b>snmp trap link-status permit duplicates</b> command in interface configuration mode. For example, to enter dialer interface configuration mode, enter the interface type as dialer.</p>
Step 5	<pre>no snmp-server link-status</pre> <p><b>Example:</b> Router(config-if)# no snmp-server link-status</p>	<p>Disables the sending of linkUp and linkDown notifications for all generic interfaces.</p>
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-if)# exit</p>	<p>Exits interface configuration mode.</p>
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

## Configuring SNMP Notification Log Options

Perform this task to configure SNMP notification log options. These options allow you to control the log size and timing values. The SNMP log can become very large and long if left unmodified.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp mib notification-log default**
4. **snmp mib notification-log globalageout *seconds***
5. **snmp mib notification-log globalsize *size***
6. **exit**
7. **show snmp mib notification-log**

### DETAILED STEPS

Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp mib notification-log default</b>  <b>Example:</b> Router(config)# snmp mib notification-log default	Creates an unnamed SNMP notification log.
Step 4	<b>snmp mib notification-log globalageout <i>seconds</i></b>  <b>Example:</b> Router(config)# snmp mib notification-log globalageout 20	Sets the maximum amount of time SNMP notification log entries remain in the system memory. <ul style="list-style-type: none"> <li>In this example, the system is configured to delete entries in the SNMP notification log that were logged more than 20 minutes ago.</li> </ul>
Step 5	<b>snmp mib notification-log globalsize <i>size</i></b>  <b>Example:</b> Router(config)# snmp mib notification-log globalsize 600	Sets the maximum number of entries that can be stored in all SNMP notification logs.

Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode.
Step 7	<pre>show snmp mib notification-log</pre> <p><b>Example:</b> Router# show snmp mib notification-log</p>	Displays information about the state of the local SNMP notification logging.

## Examples

This example shows information about the state of local SNMP notification logging:

```
Router# show snmp mib notification-log

GlobalAgeout 20, GlobalEntryLimit 600
Total Notifications logged in all logs 0
Log Name"", Log entry Limit 600, Notifications logged 0
Logging status enabled
Created by cli
```

## Configuring Interface Index Display and Interface Indexes and Long Name Support

The display of Interface Indexes lets advanced users of SNMP view information about the interface registrations directly on a managed agent. An external NMS is not required.

Configuration of Long Alias Names for the interfaces lets users configure the ifAlias (the object defined in the MIB whose length is restricted to 64) up to 255 bytes.

## Prerequisites

SNMP is enabled on your system.

## Restrictions

The Interface Index Display and Interface Alias Long Name Support feature is not supported on all Cisco platforms. Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support.

Perform this task to configure the IF-MIB to retain ifAlias values of longer than 64 characters and to configure the ifAlias values for an interface.



### Note

To verify if the ifAlias description is longer than 64 characters, perform an SNMP MIB walk for the ifMIB ifAlias variable from an NMS and verify that the entire description is displayed in the values for ifXEntry.18.

The description for interfaces also appears in the output from the **more system:running config** privileged EXEC mode command.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp ifmib ifalias long**
4. **interface** *type number*
5. **description** *text-string*
6. **exit**
7. **show snmp mib**
8. **show snmp mib ifmib ifindex** [*type number*] [**detail**] [**free-list**]

## DETAILED STEPS

Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp ifmib ifalias long</b>  <b>Example:</b> Router(config)# snmp ifmib ifalias long	Configures the Interfaces MIB (IF-MIB) on the system to return ifAlias values of longer than 64 characters to a Network Management System.  If the ifAlias values are not configured using the <b>snmp ifmib ifalias long</b> command, ifAlias description will be restricted to 64 characters.
Step 4	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface FastEthernet 2/4	Enters interface configuration mode. <ul style="list-style-type: none"> <li>The form of this command varies depending on the interface being configured.</li> </ul>
Step 5	<b>description</b> <i>text-string</i>  <b>Example:</b> Router(config)# description This text string description can be up to 256 characters long	Configures a free-text description of the specified interface. <ul style="list-style-type: none"> <li>This description can be up to 240 characters in length and is stored as the ifAlias object value in the IF-MIB.</li> </ul> If the ifAlias values are not configured using <b>snmp ifmib ifalias long</b> command, ifAlias description for SNMP set and get operations is restricted to 64 characters, although the interface description is configured for more than 64 characters by using the <b>description</b> command.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.

<b>Step 7</b>	<b>show snmp mib</b>  <b>Example:</b> Router# show snmp mib	Displays a list of the MIB module instance identifiers registered on your system. <ul style="list-style-type: none"> <li>The resulting display could be lengthy.</li> </ul>
<b>Step 8</b>	<b>show snmp mib ifmib ifindex</b> [ <i>type number</i> ] [ <i>detail</i> ] [ <i>free-list</i> ]  <b>Example:</b> Router# show snmp mib ifmib ifindex FastEthernet 2/0	Displays the Interfaces MIB ifIndex values registered on your system for all interfaces or the specified interface.

## Examples

The following example lists the MIB module instance identifiers registered on your system. The resulting display could be lengthy. Only a small portion is shown here.

```
Router# show snmp mib
```

```
system.1
system.2
sysUpTime
system.4
system.5
system.6
system.7
system.8
sysOREntry.2
sysOREntry.3
sysOREntry.4
interfaces.1
ifEntry.1
ifEntry.2
ifEntry.3
ifEntry.4
ifEntry.5
ifEntry.6
ifEntry.7
ifEntry.8
ifEntry.9
ifEntry.10
ifEntry.11
```

```
--More--
```

```
captureBufferEntry.2
captureBufferEntry.3
captureBufferEntry.4
captureBufferEntry.5
captureBufferEntry.6
captureBufferEntry.7
capture.3.1.1
eventEntry.1
eventEntry.2
eventEntry.3
eventEntry.4
eventEntry.5
eventEntry.6

eventEntry.7
```

```
logEntry.1
logEntry.2
logEntry.3
logEntry.4
rmon.10.1.1.2
rmon.10.1.1.3
rmon.10.1.1.4
rmon.10.1.1.5
rmon.10.1.1.6
rmon.10.1.1.7
rmon.10.2.1.2
rmon.10.2.1.3
rmon.10.3.1.2
```

--More--

The following example shows output for the Interfaces MIB ifIndex values registered on a system for a specific interface:

```
Router# show snmp mib ifmib ifindex FastEthernet 2/0
```

```
FastEthernet2/0: Ifindex = 2
```

The following example shows output for the Interfaces MIB ifIndex values registered on a system for all interfaces:

```
Router# show snmp mib ifmib ifindex
```

```
ATM1/0: Ifindex = 1
ATM1/0-aal5 layer: Ifindex = 12
ATM1/0-atm layer: Ifindex = 10
ATM1/0.0-aal5 layer: Ifindex = 13
ATM1/0.0-atm subif: Ifindex = 11
ATM1/0.9-aal5 layer: Ifindex = 32
ATM1/0.9-atm subif: Ifindex = 31
ATM1/0.99-aal5 layer: Ifindex = 36
ATM1/0.99-atm subif: Ifindex = 35
FastEthernet2/0: Ifindex = 2
FastEthernet2/1: Ifindex = 3
FastEthernet2/2: Ifindex = 4
FastEthernet2/3: Ifindex = 5
Null0: Ifindex = 14
Serial3/0: Ifindex = 6
Serial3/1: Ifindex = 7
Serial3/2: Ifindex = 8
Serial3/3: Ifindex = 9
```

## Configuring Interface Index Persistence

The following sections contain the tasks to configure Interface Index Persistence:

- [Enabling and Disabling IfIndex Persistence Globally, page 37](#)
- [Enabling and Disabling IfIndex Persistence on Specific Interfaces, page 39](#)

### Enabling and Disabling IfIndex Persistence Globally

Perform this task to enable IfIndex persistence globally.

## Prerequisites

The configuration tasks described in the next section assume that you have configured SNMP on your routing device and are using SNMP to monitor network activity using the Cisco IOS command line interface and/or a network management system (NMS) application.

## Restrictions

The interface-specific ifIndex persistence command (**snmp ifindex persistence**) cannot be used on subinterfaces. A command applied to an interface is automatically applied to all the subinterfaces associated with that interface.

Testing indicates that approximately 25 bytes of NVRAM storage are used by this feature per interface. There may be some boot delay exhibited on platforms with lower CPU speeds.



### Note

After ifIndex persistence commands have been entered, the configuration must be saved using the **copy running-config startup-config** EXEC mode command to ensure consistent ifIndex values.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server ifindex persist**
4. **no snmp-server ifindex persist**
5. **exit**

## DETAILED STEPS

Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server ifindex persist</b>  <b>Example:</b> Router(config)# snmp-server ifindex persist	Globally enables ifIndex values that will remain constant across reboots.

<b>Step 4</b>	<code>no snmp-server ifindex persist</code>  <b>Example:</b> Router(config)# no snmp-server ifindex persist	Disables global ifIndex persistence.
<b>Step 5</b>	<code>exit</code>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.

## Enabling and Disabling IfIndex Persistence on Specific Interfaces

Perform this task to configure ifIndex persistence only on a specific interface.



### Tips

Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **snmp ifindex persist**
5. **no snmp ifindex persist**
6. **exit**
7. **exit**

## DETAILED STEPS

<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<code>interface type slot/port</code>  <b>Example:</b> Router(config)# interface FastEthernet 0/1	Enters interface configuration mode for the specified interface. <b>Note</b> Note that the syntax of the interface command will vary depending on the platform you are using.
<b>Step 4</b>	<code>snmp ifindex persist</code>  <b>Example:</b> Router(config-if)# snmp ifindex persist	Enables an ifIndex value that is constant across reboots on the specified interface.

Step 5	<pre>no snmp ifindex persist</pre> <p><b>Example:</b> Router(config-if)# no snmp ifindex persist</p>	Disables an ifIndex value that is constant across reboots on the specified interface.
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-if)# exit</p>	Exits interface configuration mode.
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode.

## Configuring SNMP Support for VPNs

This section describes how to configure SNMP support for VPNs. The SNMP Support for VPNs feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used to send SNMP traps and informs and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

Support for VPNs allows users to configure an SNMP agent to only accept SNMP requests from a certain set of VPNs. With this configuration, providers can provide network management services to their customers who then can manage all user VPN devices.

### Restrictions

- This feature is not supported on all Cisco platforms. Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support.
- Not all MIBs are VPN aware. To list the VPN-aware MIBs, use the **show snmp mib context** command.

Perform this task to configure SNMP support for a specific VPN.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-address* [**vrf** *vrf-name*] [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
4. **snmp-server engineID remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
5. **exit**
6. **show snmp host**

## DETAILED STEPS

<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>snmp-server host</b> <i>host-address</i> [ <b>vrf</b> <i>vrf-name</i> ] [ <b>traps</b>   <b>informs</b> ] [ <b>version</b> { <b>1</b>   <b>2c</b>   <b>3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]}] <b>community-string</b> [ <b>udp-port</b> <i>port</i> ] [ <b>notification-type</b> ]  <b>Example:</b> Router(config)# snmp-server host example.com vrf trap-vrf public	Specifies the recipient of an SNMP notification operation and specifies the VRF table to be used for the sending of SNMP notifications.
<b>Step 4</b>	<b>snmp-server engineID remote</b> <i>ip-address</i> [ <b>udp-port</b> <i>udp-port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ] <i>engineid-string</i>  <b>Example:</b> Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf 80000009030000B064EFE100	Configures a name for the remote SNMP engine on a router when configuring SNMP over a specific VPN for a remote SNMP user.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
<b>Step 6</b>	<b>show snmp host</b>  <b>Example:</b> Router# show snmp host	(Optional) Displays the SNMP configuration and verifies that the SNMP Support for VPNs feature is configured properly.

## Configuring Event MIB

There are no Cisco IOS software configuration tasks associated with the Event MIB. All configuration of Event MIB functionality must be performed through applications using SNMP. This section provides a sample configuration session using a network management application on an external device. See the [“Related Documents” section on page 46](#) for information about configuring SNMP on your Cisco routing device.

All configuration of Event MIB functionality must be performed through applications using SNMP. The following section provides a step-by-step Event MIB configuration using SNMP research tools available for Sun workstations. The **setany** commands given below are executed using the SNMP application. Note that these commands are not Cisco IOS CLI commands. It is assumed that SNMP has been configured on your routing device.

In this configuration, the objective is to monitor ifInOctets for all interfaces. The Event MIB is configured to monitor the delta values of ifInOctets for all interfaces once per minute. If any of the samples exceed the specified threshold of 30, a Trap notification will be sent.

There are four parts to the following example:

- [Setting the Trigger in the Trigger Table, page 42](#)
- [Creating an Event in the Event Table, page 42](#)
- [Setting the Trigger Threshold in the Trigger Table, page 43](#)
- [Activating the Trigger, page 43](#)

## Setting the Trigger in the Trigger Table

Perform this task to set the trigger in the trigger table:

	Command	Purpose
<b>Step 1</b>	<code>setany -v2c \$ADDRESS private mteTriggerEntryStatus.4.106.111.104.110.1 -i 5</code>	Creates a trigger row in the table with john as the mteOwner and 1 as the trigger name. The index is given in decimal representation of the ASCII value of john.1.
<b>Step 2</b>	<code>setany -v2c \$ADDRESS private mteTriggerValueID.4.106.111.104.110.1 -d 1.3.6.1.2.1.2.2.1.10</code>	Sets the mteTriggerValueID to the OID to be watched. In this example, the OID to be monitored is ifInOctets.
<b>Step 3</b>	<code>setany -v2c \$ADDRESS private mteTriggerValueIDWildcard.4.106.111.104.110.1 -i 1</code>	Sets the mteTriggerValueIDWildcard to TRUE to denote a object referenced through wildcarding.
<b>Step 4</b>	<code>setany -v2c \$ADDRESS private mteTriggerTest.4.106.111.104.110.1 -o '20'</code>	Sets the mteTriggerTest to Threshold.
<b>Step 5</b>	<code>setany -v2c \$ADDRESS private mteTriggerFrequency.4.106.111.104.110.1 -g 60</code>	Sets the mteTriggerFrequency to 60. This means that ifInOctets are monitored once every sixty seconds.
<b>Step 6</b>	<code>setany -v2c \$ADDRESS private mteTriggerSampleType.4.106.111.104.110.1 -i 2</code>	Sets the sample type to Delta.
<b>Step 7</b>	<code>setany -v2c \$ADDRESS private mteTriggerEnabled.4.106.111.104.110.1 -i 1</code>	Enables the trigger.

## Creating an Event in the Event Table

Perform this task to create an event in the event table:

	Command	Purpose
<b>Step 1</b>	<code>setany -v2c \$ADDRESS private mteEventEntryStatus.4.106.111.104.110.101.118.101.11 0.116 -i 5</code>	Create a row in the Event Table. The mteOwner here is again john and mteEventName is event. The default action is to send out a notification.
<b>Step 2</b>	<code>setany -v2c \$ADDRESS private mteEventEnabled.4.106.111.104.110.101.118.101.110.11 6 -i 1</code>	Enables the Event.
<b>Step 3</b>	<code>setany -v2c \$ADDRESS private mteEventEntryStatus.4.106.111.104.110.101.118.101.11 0.116 -i 1</code>	Makes the EventRow active.



## Setting the Trigger Threshold in the Trigger Table

Perform this task to set the trigger threshold in the trigger table

	Command	Purpose
<b>Step 1</b>	<code>setany -v2c \$ADDRESS private mteTriggerThresholdRising.4.106.111.104.110.1 -i 30</code>	Sets the Rising Threshold value to 30. Note that a row would already exist for john.1 in the Trigger Threshold Table.
<b>Step 2</b>	<code>setany -v2c \$ADDRESS private mteTriggerThresholdRisingEventOwner.4.106.111.104.110.1 -D "john"  setany -v2c \$ADDRESS private mteTriggerThresholdRisingEvent.4.106.111.104.110.1 -D "event"</code>	Points to the entry in the Event Table that specifies the action that is to be performed.

## Activating the Trigger

Perform this task to activate the trigger:

	Command	Purpose
<b>Step 1</b>	<code>setany -v2c \$ADDRESS private mteTriggerEntryStatus.4.106.111.104.110.1 -i 1</code>	Makes the trigger active.

To confirm the above configuration is working, ensure that at least one of the interfaces gets more than 30 packets in a minute. This should cause a trap to be sent out after one minute.

## Monitoring and Maintaining Event MIB

Use the following commands to monitor Event MIB activity from the Cisco IOS command-line interface:

Command	Purpose
<code>debug management event mib</code>	Prints messages to the screen whenever the Event MIB evaluates a specified trigger. These messages are given in real-time, and are intended to be used by technical support engineers for troubleshooting purposes.
<code>show management event</code>	Displays the SNMP Event values that have been configured on your routing device through the use of the Event MIB.

## Configuration Examples for SNMP Support

This section provides the following configuration examples:

- [Configuring SNMPv1, SNMPv2c, and SNMPv3: Example, page 44](#)
- [Configuring IfAlias Long Name Support: Example, page 45](#)
- [Configuring SNMP Support for VPNs: Example, page 46](#)
- [Additional References, page 46](#)

## Configuring SNMPv1, SNMPv2c, and SNMPv3: Example

The following example shows how to enable SNMPv1 and SNMPv2c. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string named public. This configuration does not cause the router to send traps.

```
snmp-server community public
```

The following example shows how to permit SNMP access to all objects with read-only permission using the community string named public. The router also will send BGP traps to the hosts 172.16.1.111 and 172.16.1.33 using SNMPv1 and to the host 172.16.1.27 using SNMPv2c. The community string named public is sent with the traps.

```
snmp-server community public
snmp-server enable traps bgp
snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.33 public
```

The following example shows how to allow read-only access for all objects to members of access list 4 that specify the comaccess community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2c to the host example.com using the community string named public.

```
snmp-server community comaccess ro 4
snmp-server enable traps snmp authentication
snmp-server host example.com version 2c public
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host example.com using the community string public:

```
snmp-server enable traps
snmp-server host example.com public
```

The following example shows a configuration in which no traps are sent to a host. The BGP traps are enabled for all hosts, but only the OSPF traps are enabled to be sent to a host.

```
snmp-server enable traps bgp
snmp-server host host1 public ospf
```

The following example shows how to enable a router to send all informs to the host example.com using the community string named public:

```
snmp-server enable traps
snmp-server host example.com informs version 2c public
```

The following example shows how to enable the SNMP manager and set the session timeout to a value greater than the default:

```
snmp-server manager
snmp-server manager session-timeout 1000
```

The following example shows how to enable the SNMP manager to access all objects with read-only permissions. The user is specified as abcd and the authentication password is abcdpasswd. To obtain the automatically generated default local engine ID, use the **show snmp engineID** command.

```
snmp-server view readview internet included
snmp-server view readview iso included
snmp-server group group1 v3 noauth read readview
snmp-server user abcd group1 v3 auth md5 abcdpasswd
```

The following example shows the minimum configuration required for a Cisco ASR 1000 Series Aggregation Services Router to send SNMPv3 traps to the SNMP manager:

```
snmp-server user trapuser trapgroup v3
snmp-server host 9.0.0.115 traps version 3 noauth trapuser
```

## Configuring IfAlias Long Name Support: Example

In the following example a long description is applied to the Fast Ethernet interface in slot 1, port adapter 0, and port 0:

```
Router# configure terminal
Router(config)# interface FastEthernet1/0/0
Router(config-if)# description FastEthernet1/0/0 this is a test of a description that
exceeds 64 characters in length
Router(config-if)# ip address 192.168.134.55 255.255.255.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip route-cache distributed
```

Assuming that ifAlias long name support is not yet enabled (the default), the following example shows the results of a mibwalk operation from an NMS:

```
***** SNMP QUERY STARTED *****
.
.
.
ifXEntry.18.10 (octets) (zero-length)
ifXEntry.18.11 (octets) Fastethernet1/0/0 this is a test of a description that exceeds 64
ch
ifXEntry.18.12 (octets) (zero-length)
.
.
.
```

The following output shows the description that is displayed at the CLI:

```
Router# show interface FastEthernet0/0/0

FastEthernet1/0/0 is administratively down, line protocol is down
  Hardware is Lance, address is 0010.7b4d.7046 (bia 0010.7b4d.7046)
  Description: FastEthernet1/0/0 this is a test of a description that exceeds 64 chh
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 252/255, txload 1/255, rxload 1/255
.
.
.
```

In the following example, ifAlias long name support is enabled and the description is displayed again:

```
Router(config)# snmp ifmib ifalias long
Router(config)# interface FastEthernet1/0/0
Router(config-if)# description FastEthernet1/0/0 this is a test of a description that
exceeds 64 characters in length
Router(config)# end
Router# show interface FastEthernet1/0/0
```

```
FastEthernet1/0/0 is administratively down, line protocol is down
  Hardware is Lance, address is 0010.7b4d.7046 (bia 0010.7b4d.7046)
```

```

Description: FastEthernet1/0/0 this is a test of a description that exceeds 64
characters in length
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 252/255, txload 1/255, rxload 1/255
.
.
.
***** SNMP QUERY STARTED *****
.
.
.
ifXEntry.18.10 (octets) (zero-length)
ifXEntry.18.11 (octets) FastEthernet1/0/0 this is a test of a description that exceeds 64
characters in length
ifXEntry.18.12 (octets) (zero-length)
.
.
.

```

## Configuring SNMP Support for VPNs: Example

In the following example all SNMP notifications are sent to example.com over the VRF named trap-vrf:

```
Router(config)# snmp-server host example.com vrf trap-vrf
```

In the following example the VRF named “traps-vrf” is configured for the remote server 172.16.20.3:

```
Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf
80000009030000B064EFE100
```

## Additional References

The following sections provide references related to configuring SNMP support.

## Related Documents

Related Topic	Document Title
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS Network Management Command Reference</a></li> <li><a href="#">Cisco IOS Master Command List, All Releases</a></li> </ul>
Cisco IOS XE implementation of RFC 1724, RIP Version 2 MIB Extensions	<i>RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions</i> feature module
DSP Operational State Notifications for notifications to be generated when a digital signaling processor (DSP) is used	<i>DSP Operational State Notifications</i> feature module

## Standards

Standard	Title
CBC-DES (DES-56) standard	<i>Symmetric Encryption Protocol</i>
Standard 58	<i>Structure of Management Information Version 2 (SMIv2)</i>

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>• Cisco SNMPv2</li> <li>• Ethernet-like Interfaces MIB</li> <li>• Event MIB</li> <li>• Expression MIB Support for Delta, Wildcarding, and Aggregation</li> <li>• Interfaces Group MIB (IF-MIB)</li> <li>• Interfaces Group MIB Enhancements</li> <li>• MIB Enhancements for Universal Gateways and Access Servers</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 1067	<i>A Simple Network Management Protocol</i>
RFC 1091	<i>Telnet terminal-type option</i>
RFC 1098	<i>Simple Network Management Protocol (SNMP)</i>
RFC 1157	<i>Simple Network Management Protocol (SNMP)</i>
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based internets:MIB-II</i>
RFC 1215	<i>Convention for defining traps for use with the SNMP</i>
RFC 1901	<i>Introduction to Community-based SNMPv2</i>
RFC 1905	<i>Common Management Information Services and Protocol over TCP/IP (CMOT)</i>
RFC 1906	<i>Telnet X Display Location Option</i>
RFC 1908	<i>Simple Network Management Protocol (SNMP)</i>
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication</i>
RFC 2206	<i>RSVP Management Information Base using SMIv2</i>
RFC 2213	<i>Integrated Services Management Information Base using SMIv2</i>
RFC 2214	<i>Integrated Services Management Information Base Guaranteed Service Extensions using SMIv2</i>
RFC 2233	<i>The Interface Group MIB using SMIv2</i>

RFC	Title
RFC 2271	<i>An Architecture for Describing SNMP Management Frameworks</i>
RFC 2570	<i>Introduction to Version 3 of the Internet-standard Network Management Framework</i>
RFC 2578	<i>Structure of Management Information Version 2 (SMIv2)</i>
RFC 2579	<i>Textual Conventions for SMIv2</i>
RFC 2580	<i>Conformance Statements for SMIv2</i>
RFC 2981	<i>Event MIB</i>
RFC 3413	<i>SNMPv3 Applications</i>
RFC 3415	<i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuring SNMP Support

Table 2 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 2 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 2** Feature Information for Configuring SNMP Support

Feature Name	Releases	Feature Information
SNMP (Simple Network Management Protocol)	Cisco IOS XE Release 2.1	The following sections provide information about this feature: <ul style="list-style-type: none"> <li>“SNMP Operations” section on page 3</li> <li>“Versions of SNMP” section on page 6</li> <li>How to Configure SNMP Support, page 11</li> </ul>
SNMPv2C	Cisco IOS XE Release 2.1	The following sections provide information about this feature: <ul style="list-style-type: none"> <li>“SNMP Operations” section on page 3</li> <li>“Versions of SNMP” section on page 6</li> <li>How to Configure SNMP Support, page 11</li> </ul>
SNMP Version 3	Cisco IOS XE Release 2.1	The following sections provide information about this feature: <ul style="list-style-type: none"> <li>“SNMP Operations” section on page 3</li> <li>“Versions of SNMP” section on page 6</li> <li>How to Configure SNMP Support, page 11</li> </ul>
SNMP Inform Request	Cisco IOS XE Release 2.1	The following section provide information about this feature: <ul style="list-style-type: none"> <li>“SNMP Operations” section on page 3</li> </ul>

**Table 2**      **Feature Information for Configuring SNMP Support (continued)**

Feature Name	Releases	Feature Information
Interface Index Display and Interface Alias Long Name Support for SNMP	Cisco IOS XE Release 2.1	<p>The Interface Index Display for SNMP feature introduces new commands and command modifications that allow advanced users of SNMP to view information about the interface registrations directly on the managed agent. You can display MIB information from the agent without using an external NMS.</p> <p>This feature addresses three objects in the Interfaces MIB: <i>ifIndex</i>, <i>ifAlias</i>, and <i>ifName</i>. For complete definitions of these objects, see the IF-MIB.mib file available from the Cisco SNMPv2 MIB website at <a href="ftp://ftp.cisco.com/pub/mibs/v2/">ftp://ftp.cisco.com/pub/mibs/v2/</a>.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Detailed Interface Registration Information” section on page 8</a></li> <li>• <a href="#">“Configuring Interface Index Display and Interface Indexes and Long Name Support” section on page 34</a></li> </ul>
Interface Index Persistence	Cisco IOS XE Release 2.1	<p>This enhancement allows interfaces to be identified with unique values which will remain constant even when a device is rebooted. These interface identification values are used for network monitoring and management using SNMP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Interface Index Persistence, page 9</a></li> <li>• <a href="#">Configuring Interface Index Persistence, page 37</a></li> </ul>
SNMP Notification Logging	Cisco IOS XE Release 2.1	<p>The SNMP Notification Logging feature adds Cisco IOS CLI commands to change the size of the notification log, to set the global ageout value for the log, and to display logging summaries at the command line.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">“SNMP Notification Logging” section on page 11</a></li> <li>• <a href="#">“Configuring SNMP Notifications” section on page 28</a></li> </ul>
SNMP Support for VPNs	Cisco IOS XE Release 2.1	<p>The SNMP Support for VPNs feature allows SNMP traps and informs to be sent and received using VRF tables. In particular, this feature adds support to Cisco IOS XE software for sending and receiving SNMP traps and informs specific to individual VPNs.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">“SNMP Support for VPNs” section on page 9</a></li> <li>• <a href="#">“Configuring SNMP Support for VPNs” section on page 40</a></li> </ul>
SNMP Manager	Cisco IOS XE Release 2.1	This feature was implemented on the Cisco ASR 1000 series routers.
Event MIB	Cisco IOS XE Release 2.1	This feature was implemented on the Cisco ASR 1000 series routers.



# Glossary

**ifAlias**—SNMP Interface Alias. The ifAlias is an object in the Interfaces MIB (IF-MIB). The ifAlias is an alias name for the interface as specified by a network manager that provides a nonvolatile description for the interface. For a complete definition, see the IF-MIB.my file.

**ifIndex**—SNMP Interface Index. The ifIndex is an object in the Interfaces MIB (IF-MIB). The ifIndex is a unique integer assigned to every interface (including subinterfaces) on the managed system when the interface registers with the IF-MIB. For a complete definition, see the IF-MIB.my file.

**OID**—MIB object identifier. An object identifier is expressed as a series of integers or text strings. Technically, the numeric form is the *object name* and the text form is the *object descriptor*. In practice, both are called object identifiers, or OIDs. For example, the object name for the interfaces MIB is 1.3.6.1.2.1.2, and the object descriptor is 'iso.internet.mgmt.mib-2.interfaces' but either can be referred to as the OID. An OID can also be expressed as a combination of the two, such as iso.internet.2.1.2.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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.

© 2006–2009 Cisco Systems, Inc. All rights reserved.





## **Managing Configuration Files**





# Managing Configuration Files

---

**Last Updated: May 4, 2009**

This chapter describes how to create, load, and maintain configuration files. Configuration files contain a set of user-configured commands that customize the functionality of your Cisco routing device.

The tasks in this chapter assume that you have at least a minimal configuration running on your system. You can create a basic configuration file using the **setup** command (see [Using Setup Mode to Configure a Cisco Networking Device](#) for details).

For a complete description of the configuration file management commands in this chapter, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

To identify hardware or software image support for a specific feature, use Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see [About Cisco IOS Software Documentation](#).

## 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 Managing Configuration Files](#)” section on [page 19](#).

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

- [Understanding Configuration Files, page 2](#)
- [Configuration File Management Task List, page 3](#)
- [Displaying Configuration File Information, page 3](#)
- [Entering Configuration Mode and Selecting a Configuration Source, page 4](#)



---

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

© 2003-2008 Cisco Systems, Inc. All rights reserved.

- [Modifying the Configuration File at the CLI, page 4](#)
- [Copying Configuration Files from the Router to a Network Server, page 5](#)
- [Copying Configuration Files from a Network Server to the Router, page 6](#)
- [Maintaining Configuration Files Larger than NVRAM, page 7](#)
- [Controlling the Parser Cache, page 10](#)
- [Copying Configuration Files Between Different Locations, page 12](#)
- [Reexecuting the Configuration Commands in the Startup Configuration File, page 14](#)
- [Clearing Configuration Information, page 14](#)
- [Specifying the Startup Configuration File, page 15](#)
- [Technical Assistance, page 18](#)
- [Feature Information for Managing Configuration Files, page 19](#)

## Understanding Configuration Files

Configuration files contain the Cisco IOS XE software commands used to customize the functionality of your Cisco routing device (router, access server, switch, and so on). Commands are parsed (translated and executed) by the Cisco IOS XE software when the system is booted (from the startup-config file) or when you enter commands at the CLI in a configuration mode.

## Types of Configuration Files

Startup configuration files (startup-config) are used during system startup to configure the software. Running configuration files (running-config) contain the current configuration of the software. The two configuration files can be different. For example, you may want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration using the **configure terminal EXEC** command but not save the configuration using the **copy running-config startup-config EXEC** command.

To change the running configuration, use the **configure terminal** command, as described in the “[Modifying the Configuration File at the CLI](#)” section later in this chapter. As you use the Cisco IOS XE configuration modes, commands generally are executed immediately and are saved to the running configuration file either immediately after you enter them or when you exit a configuration mode.

To change the startup configuration file, you can either save the running configuration file to the startup configuration using the **copy running-config startup-config EXEC** command or copy a configuration file from a file server to the startup configuration (see the “[Copying Configuration Files from a Network Server to the Router](#)” section for more information).

## Location of Configuration Files

Configuration files are stored in the following locations:

- The running configuration is stored in RAM.
- On all platforms except the Class A Flash file system platforms, the startup configuration is stored in nonvolatile random-access memory (NVRAM).

- On Class A Flash file system platforms, the startup configuration is stored in the location specified by the CONFIG\_FILE environment variable (see the “[Specifying the CONFIG\\_FILE Environment Variable on Class A Flash File Systems](#)” section for more information). The CONFIG\_FILE variable defaults to NVRAM and can be a file in the following file systems:
  - **nvr**am: (NVRAM)
  - **bootflash**: (internal Flash memory)
  - **HDD**: (harddisk)
  - **usb0**: (external USB media 1)
  - **usb1**: (external USB media 2)

## Configuration File Management Task List

To understand the management of Cisco IOS XE software configuration files, perform the tasks described in the following sections:

- [Displaying Configuration File Information, page 3](#)
- [Entering Configuration Mode and Selecting a Configuration Source, page 4](#)
- [Modifying the Configuration File at the CLI, page 4](#)
- [Copying Configuration Files from the Router to a Network Server, page 5](#)
- [Copying Configuration Files from a Network Server to the Router, page 6](#)
- [Maintaining Configuration Files Larger than NVRAM, page 7](#)
- [Controlling the Parser Cache, page 10](#)
- [Copying Configuration Files Between Different Locations, page 12](#)
- [Reexecuting the Configuration Commands in the Startup Configuration File, page 14](#)
- [Clearing Configuration Information, page 14](#)
- [Specifying the Startup Configuration File, page 15](#)

## Displaying Configuration File Information

To display information about configuration files, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# <b>show bootvar</b>	Lists the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, and the contents of the BOOTLDR environment variable.
Router# <b>more file-url</b>	Displays the contents of a specified file.

Command	Purpose
Router# <b>show running-config</b>	Displays the contents of the running configuration file. (Command alias for the <b>more system:running-config</b> command.)
Router# <b>show startup-config</b>	Displays the contents of the startup configuration file. (Command alias for the <b>more nvram:startup-config</b> command.)  On all platforms except the Class A Flash file system platforms, the default startup-config file usually is stored in NVRAM. On the Class A Flash file system platforms, the CONFIG_FILE environment variable points to the default startup-config file. The CONFIG_FILE variable defaults to NVRAM.

## Entering Configuration Mode and Selecting a Configuration Source

To enter configuration mode on the router, enter the **configure** command at the privileged EXEC prompt. The Cisco IOS XE software responds with the following prompt asking you to specify the terminal, memory, or a file stored on a network server (network) as the source of configuration commands:

```
Configuring from terminal, memory, or network [terminal]?
```

Configuring from the terminal allows you to enter configuration commands at the command line, as described in the following section. Configuring from memory loads the startup configuration file. See the “[Reexecuting the Configuration Commands in the Startup Configuration File](#)” section for more information. Configuring from the network allows you to load and execute configuration commands over the network. See the “[Copying Configuration Files from a Network Server to the Router](#)” section for more information.

## Modifying the Configuration File at the CLI

The Cisco IOS XE software accepts one configuration command per line. You can enter as many configuration commands as you want.

You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!). Because comments are *not* stored in NVRAM or in the active copy of the configuration file, comments do not appear when you list the active configuration with the **show running-config** or **more system:running-config** EXEC command. Comments do not display when you list the startup configuration with the **show startup-config** or **more nvram:startup-config** EXEC mode command. Comments are stripped out of the configuration file when it is loaded onto the router. However, you can list the comments in configuration files stored on a Trivial File Transfer Protocol (TFTP) server.

When you configure the software using the CLI, the software executes the commands as you enter them. To configure the software using the CLI, use the following commands beginning in privileged EXEC mode:



	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2		Enter the necessary configuration commands. The Cisco IOS XE documentation set describes configuration commands organized by technology.
Step 3	Router(config)# <b>end</b>  or Router(config)# <b>^Z</b>	Ends the configuration session and exits to EXEC mode.  <b>Note</b> When you press the Ctrl and Z keys simultaneously, ^Z is displayed to the screen.
Step 4	Router# <b>copy system:running-config nvram:startup-config</b>	Saves the running configuration file as the startup configuration file. You may also use the <b>copy running-config startup-config</b> command alias, but you should be aware that this command is less precise. On most platforms, this command saves the configuration to NVRAM. On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable (the default CONFIG_FILE variable specifies that the file should be saved to NVRAM).

In the following example, the router prompt name of the router is configured. The comment line, indicated by the exclamation mark (!), does not execute any command.

In this example, the **hostname** command is used to change the router name from Router to new\_name. By pressing Ctrl-Z (^Z) or entering the **end** command, the user quits configuration mode. The **copy system:running-config nvram:startup-config** command saves the current configuration to the startup configuration.

```
Router# configure terminal
Router(config)# !The following command provides the router host name.
Router(config)# hostname new_name
new_name(config)# end
new_name# copy system:running-config nvram:startup-config
```

When the startup configuration is NVRAM, it stores the current configuration information in text format as configuration commands, recording only nondefault settings. The memory is checksummed to guard against corrupted data.


**Note**

Some specific commands might not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a list of these settings so that you can quickly reconfigure your router after rebooting.

## Copying Configuration Files from the Router to a Network Server

You can copy configuration files from the router to a file server using TFTP. For example, you might perform this task to back up a current configuration file to a server before changing its contents, thereby allowing you to later restore the original configuration file from the server.

To copy configuration files from a router to a server, perform the tasks described in the following sections:

- [Copying a Configuration File from the Router to a TFTP Server](#)

## Copying a Configuration File from the Router to a TFTP Server

In some implementations of TFTP, you must create a dummy file on the TFTP server and give it read, write, and execute permissions before copying a file over it. Refer to your TFTP documentation for more information.

To copy configuration information on a TFTP network server, use the following commands in the EXEC mode, as needed:

Command	Purpose
Router# <b>copy system:running-config</b> <b>tftp:[[/location]/directory]/filename]</b>	Copies the running configuration file to a TFTP server.
Router# <b>copy nvram:startup-config</b> <b>tftp:[[/location]/directory]/filename]</b>	Copies the startup configuration file to a TFTP server.

After you have issued the **copy** command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

The following example copies a configuration file from a router to a TFTP server:

```
Tokyo# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y

Writing tokyo-confg!!! [OK]
```

## Copying Configuration Files from a Network Server to the Router

You can copy configuration files from a TFTP server to the running configuration or startup configuration of the router. You may want to perform this function for one of the following reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another router. For example, you may add another router to your network and want it to have a similar configuration to the original router. By copying the file to the new router, you can change the relevant parts rather than re-creating the whole file.
- To load the same configuration commands on to all the routers in your network so that all the routers have similar configurations.

The **copy tftp: system:running-config** EXEC command loads the configuration files into the router as if you were typing the commands in at the command line. The router does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command will be erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration will be used. However, some commands in the existing configuration may not be replaced or negated. In this case, the resulting configuration file will be a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

In order to restore a configuration file to an exact copy of a file stored on a server, you need to copy the configuration file directly to the startup configuration (using the **copy tftp: nvram:startup-config** command) and reload the router.

To copy configuration files from a server to a router, perform the tasks described in the following sections:

- [Copying a Configuration File from a TFTP Server to the Router](#)

## Copying a Configuration File from a TFTP Server to the Router

To copy a configuration file from a TFTP server to the router, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# <b>copy tftp:[[/location]/directory]/filename</b> <b>system:running-config</b>	Copies a configuration file from a TFTP server to the running configuration.
Router# <b>copy tftp:[[/location]/directory]/filename</b> <b>nvrn:startup-config</b>	Copies a configuration file from a TFTP server to the startup configuration.

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

In the following example, the software is configured from the file named `tokyo-config` at IP address 172.16.2.155:

```
Router1# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

## Maintaining Configuration Files Larger than NVRAM

To maintain a configuration file that exceeds size of NVRAM, perform the tasks described in the following sections:

- [Compressing the Configuration File](#)
- [Storing the Configuration in Flash Memory on Class A Flash File Systems](#)
- [Loading the Configuration Commands from the Network](#)

### Compressing the Configuration File

The **service compress-config** global configuration command specifies that the configuration file be stored compressed in NVRAM. Once the configuration file has been compressed, the router functions normally. When the system is booted, it recognizes that the configuration file is compressed, expands it, and proceeds normally. The **more nvrn:startup-config** EXEC command expands the configuration before displaying it.

Before you compress configuration files, refer to the appropriate hardware installation and maintenance publication. Verify that your system's ROMs support file compression. If not, you can install new ROMs that support file compression.

To compress configuration files, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>service compress-config</b>	Specifies that the configuration file be compressed.
Step 2	Router(config)# <b>end</b>	Exits global configuration mode.
Step 3	Use TFTP to copy the new configuration. If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: "[buffer overflow - file-size/buffer-size bytes]."  or  Router# <b>configure terminal</b>	Enters the new configuration.
Step 4	Router(config)# <b>copy system:running-config nvram:startup-config</b>	When you have finished changing the running-configuration, saves the new configuration.

The size of the configuration must not exceed three times the NVRAM size. For a 128-KB size NVRAM, the largest expanded configuration file size is 384 KB.

The **service compress-config** global configuration command works only if you have Cisco IOS XE software Release 10 or later release boot ROMs. If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

Boot ROMs do not support NVRAM compression Config NOT written to NVRAM

The following example compresses a 129-KB configuration file to 11 KB:

```
Router# configure terminal
Router(config)# service compress-config
Router(config)# end
Router# copy tftp://172.16.2.15/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
Router# copy system:running-config nvram:startup-config
Building configuration...
Compressed configuration from 2654 bytes to 1332 bytes[OK]
Uncompressed configuration from 1332 bytes to 2654 bytes
```

## Storing the Configuration in Flash Memory on Class A Flash File Systems

On Class A Flash file system routers, you can store the startup configuration in Flash memory by setting the CONFIG\_FILE environment variable to a file in internal Flash memory or Flash memory in a USB port.

To store the startup configuration in Flash memory, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# <b>copy nvram:startup-config flash-file:filename</b>	Copies the current startup configuration to the new location to create the configuration file.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.

	Command	Purpose
Step 3	Router(config)# <b>boot config filesystem:filename</b>	Specifies that the startup configuration file be stored in Flash memory by setting the CONFIG_FILE variable.
Step 4	Router(config)# <b>end</b>	Exits global configuration mode.
Step 5	Use TFTP to copy the new configuration. If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: "[buffer overflow - file-size/buffer-size bytes]."  or  Router# <b>configure terminal</b>	Enters the new configuration.
Step 6	Router# <b>copy system:running-config nvram:startup-config</b>	When you have finished changing the running-configuration, saves the new configuration.

See the “[Specifying the CONFIG\\_FILE Environment Variable on Class A Flash File Systems](#)” section for more information.

The following example stores the configuration file in usb 0:

```
Router# copy nvram:startup-config usb0:router-config
Router# configure terminal
Router(config)# boot config usb0:router-config
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

Care must be taken when editing or changing a large configuration. Flash memory space is used every time a **copy system:running-config nvram:startup-config EXEC** command is issued. Because file management for Flash memory, such as optimizing free space, is not done automatically, you must pay close attention to available Flash memory. Use the **squeeze** command to reclaim used space. We recommend that you use a large-capacity Flash card of at least 20 MB.

## Loading the Configuration Commands from the Network

You can also store large configurations on TFTP servers and download them at system startup. To use a network server to store large configurations, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# <b>copy system:running-config {tftp:}</b>	Saves the running configuration to an TFTP server.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>boot network {tftp:[[[//location]/directory]/filename]}</b>	Specifies that the startup configuration file be loaded from the network server at startup.
Step 4	Router(config)# <b>service config</b>	Enables the router to download configuration files at system startup.
Step 5	Router(config)# <b>end</b>	Exits global configuration mode.
Step 6	Router# <b>copy system:running-config nvram:startup-config</b>	Saves the configuration.

See the “[Copying Configuration Files from the Router to a Network Server](#)” and “[Configuring the Router to Download Configuration Files](#)” sections for more information on these commands.

## Controlling the Parser Cache

The Cisco IOS XE command-line parser in the Cisco IOS XE software performs the translation and execution (parsing) of command lines. The Parser Cache feature was developed to rapidly process large configuration files, thereby dramatically improving load time.

The Parser Cache feature allows the rapid recognition and translation of configuration lines in a configuration file that differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on) by dynamically creating, caching, and reusing simplified parse graphs. This improvement is useful primarily for configuration files that repeat similar commands hundreds or thousands of times, such as cases in which thousands of virtual circuits must be configured for subinterfaces, or hundreds of access lists must be configured. Performance will improve the most for those files in which the same commands are used repeatedly but the numerical arguments change from command to command.

The Parser Cache is enabled by default. However, users with Cisco devices that do not require large configuration files may want to disable the Parser Cache to free the resources used by this feature. (Memory used by this feature depends on the size of the configuration files parsed, but is generally less than 512 KB.)

To control the Parser Cache feature, perform the tasks described in the following sections. All of these tasks are optional:

- [Clearing the Parser Cache](#)
- [Disabling the Parser Cache](#)
- [Reenabling the Parser Cache](#)
- [Monitoring the Parser](#)

## Clearing the Parser Cache

To free resources or to reset the parser cache memory, you may wish to clear the parse entries and hit/miss statistics stored by the Parser Cache feature. To clear the information stored by the Parser Cache feature, use the following command in privileged EXEC mode:

Command	Purpose
Router# <code>clear parser cache</code>	Clears the parse cache entries and hit/miss statistics stored for the Parser Cache feature.

## Disabling the Parser Cache

The Parser Cache feature is enabled by default. To disable the Parser Cache feature, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>no parser cache</b>	Disables the Parser Cache feature.

When the parser cache is disabled, the **no parser cache** command line is written to the running configuration file.

**Tip**

If you wish to disable the parser cache to free system resources, you should clear the parser cache before issuing the **no parser cache** command. You will not be able to clear the parser cache after disabling it.

## Reenabling the Parser Cache

To reenable the Parser Cache feature after disabling it, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>parser cache</b>	Enables the Parser Cache feature.

## Monitoring the Parser

Statistics about the last configuration file parsed are kept in the system memory, along with hit/miss statistics on the commands parsed by the Parser Cache feature. “Hits” and “misses” refer to the matches that the parser cache was able to make to similar commands used previously in the configuration session. Those commands that are matched (“hits”) be parsed more efficiently. The parser cache cannot improve the parse time for those commands it was unable to match (“misses”).

To display the parser statistics, use the following command in privileged EXEC mode:

Command	Purpose
Router# <b>show parser statistics</b>	Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.

The following example shows sample output from the **show parser statistics** command:

```
Router# show parser statistics
Last configuration file parsed: Number of Commands:1484, Time:1272 ms

Parser cache:disabled, 0 hits, 0 misses
```

The **show parser statistics** command displays two sets of data, as follows:

- The number of commands in the configuration file that was last copied into the running configuration, and the time it took for the system to parse them (a configuration file can be loaded into the running configuration at system startup, or by issuing commands such as the **copy source running-config** EXEC command).
- The status of the parser cache (enabled or disabled) and the number of command matches (hits or misses) since the system was started or since the parser cache was cleared.

In the example shown, the hit/miss statistics (0/0) do not match the number of commands in the last configuration file parsed (1484), which indicates that the last configuration file was loaded while the parser cache was disabled.

## Copying Configuration Files Between Different Locations

On many platforms, you can copy configuration files from one Flash memory device, such as internal Flash memory or a Flash memory attached to a USB port, to other locations. You also can copy configuration files from an TFTP server to Flash memory.

### Copying Configuration Files from Flash Memory to the Startup or Running Configuration

To copy a configuration file from Flash memory directly to your startup configuration in NVRAM or your running configuration, enter one following commands in EXEC mode, as needed:

Command	Purpose
Router> <b>copy</b> filesystem:[partition-number:][filename] nvram:startup-config	Loads a configuration file directly into NVRAM.
Router> <b>copy</b> filesystem:[partition-number:][filename] system:running-config	Copies a configuration file to your running configuration.

The following example copies the file named ios-upgrade-1 from partition 4 of the Flash memory PC Card in usb 0 to the router startup configurations:

```
Router# copy bootflash: nvram:startup-config
Source filename []? 50K_ACL-config
Destination filename [startup-config]?
Compressed configuration from 2580593 bytes to 207846 bytes[OK]
2580593 bytes copied in 39.059 secs (66069 bytes/sec)
```

### Copying Configuration Files Between Flash Memory File Systems

On platforms with multiple Flash memory file systems, you can copy files from one Flash memory file system, such as internal Flash memory or a Flash memory card, to another Flash memory file system. Copying files to different Flash memory file systems lets you create backup copies of working configurations and duplicate configurations for other routers.

To copy a configuration file between Flash memory file systems, use the following commands in EXEC mode:



	Command	Purpose
Step 1	Router> <b>show source-filesystem:</b>	Displays the layout and contents of Flash memory to verify the filename.
Step 2	Router> <b>copy</b> source-filesystem:[partition-number:][filename] dest-filesystem:[partition-number:][filename]	Copies a configuration file between Flash memory devices.
Step 3	Router> <b>verify</b> dest-filesystem:[partition-number:][filename]	Verifies the checksum of the file you copied.

## Copying a Configuration File Between Local Flash Memory Devices Example

The following example copies the file named running-config from partition 1 of internal Flash memory to partition 1 of usb 1 on a ASR1000 series router. In this example, the source partition is not specified, so the router prompts for the partition number.

```
Router# copy bootflash: usb0:
Source filename [50K_ACL-config]?
Destination filename [50K_ACL-config]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
2580593 bytes copied in 0.473 secs (5455799 bytes/sec)

Source file name? running-config

Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)... OK

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'running-config' from flash: device
as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
...erased
!
[OK - 850/4194304 bytes]

Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum... OK (0x16)
```

## Copying a Configuration File from a Server to Flash Memory Devices

To copy a configuration file from a TFTP server to the router, use the following command in EXEC mode:

Command	Purpose
Router> <b>copy tftp:[[/location]/directory]/filename]</b> flash-filesystem:[partition-number:][filename]	Copies the file from a TFTP server to the Flash memory device. Reply to any router prompts for additional information or confirmation. The prompting will depend on how much information you provide in the <b>copy</b> command and the current setting of the <b>file prompt</b> command.

The following example shows the copying of the configuration file named router-config from a TFTP server to the Flash memory inserted in usb 0 of a Cisco ASR1000 series router. The copied file is renamed new-config.

```
Router# copy tftp:router-config usb0:new-config
```

## Reexecuting the Configuration Commands in the Startup Configuration File

To reexecute the commands located in the startup configuration file, use the following command in privileged EXEC mode:

Command	Purpose
Router# <b>configure memory</b>	Reexecutes the configuration commands located in the startup configuration file.

## Clearing Configuration Information

You can clear the configuration information from the startup configuration. If you reboot the router with no startup configuration, the router will enter the Setup command facility so that you can configure the router from scratch.

## Clearing the Startup Configuration

To clear the contents of your startup configuration, use the following command in EXEC mode:

Command	Purpose
Router> <b>erase nvram:</b>	Clears the contents of your startup configuration.

For all platforms except the Class A Flash file system platforms, this command erases NVRAM. The startup configuration file cannot be restored once it has been deleted.

On Class A Flash file system platforms, when you use the **erase startup-config** EXEC command, the router erases or deletes the configuration pointed to by CONFIG\_FILE environment variable. If this variable points to NVRAM, the router erases NVRAM. If the CONFIG\_FILE environment variable specifies a Flash memory device and configuration filename, the router deletes the configuration file. That is, the router marks the file as “deleted,” rather than erasing it. This feature allows you to recover a deleted file.

## Deleting a Specified Configuration File

To delete a specified configuration on a specific Flash device, use the following command in EXEC mode:

Command	Purpose
Router> <b>delete</b> <i>flash-filesystem:filename</i>	Deletes a specified configuration file on a specified Flash device.

On Class A and B Flash file systems, when you delete a specific file in Flash memory, the system marks the file as deleted. Deleted files cannot be recovered.

If you attempt to delete the configuration file specified by the CONFIG\_FILE environment variable, the system prompts you to confirm the deletion.

The following example deletes the file named myconfig from a Flash memory inserted in usb 0:

```
Router# delete usb0:myconfig
```

## Specifying the Startup Configuration File

Normally, the router uses the startup configuration file in NVRAM or the Flash file system specified by the CONFIG\_FILE environment variable (Class A Flash file systems only) at startup. See the [“Specifying the CONFIG\\_FILE Environment Variable on Class A Flash File Systems”](#) section for more information on setting the CONFIG\_FILE variable.

You can also configure the router to automatically request and receive two configuration files from the network server at startup. See the [“Configuring the Router to Download Configuration Files”](#) section for more information.

## Specifying the CONFIG\_FILE Environment Variable on Class A Flash File Systems

On Class A Flash file systems, you can configure the Cisco IOS XE software to load the startup configuration file specified by the CONFIG\_FILE environment variable. The CONFIG\_FILE variable defaults to NVRAM. To change the CONFIG\_FILE environment variable, use the following commands beginning in EXEC mode:

	Command	Purpose
<b>Step 1</b>	Router> <b>copy</b> [ <i>flash-url</i>   <i>tftp-url</i>   <b>system:running-config</b>   <b>nvrasm:startup-config</b> ] <i>dest-flash-url</i>	Copies the configuration file to the Flash file system from which the router will load the file upon restart.
<b>Step 2</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	Router(config)# <b>boot config</b> <i>dest-flash-url</i>	Sets the CONFIG_FILE environment variable. This step modifies the runtime CONFIG_FILE environment variable.
<b>Step 4</b>	Router(config)# <b>end</b>	Exits global configuration mode.
<b>Step 5</b>	Router> <b>copy system:running-config nvrasm:startup-config</b>	Saves the configuration performed in Step 3 to the startup configuration.
<b>Step 6</b>	Router> <b>show bootvar</b>	(Optional) Allows you to verify the contents of the CONFIG_FILE environment variable.

After you specify a location for the startup configuration file, the **nvramp:startup-config** command is aliased to the new location of the startup configuration file. The **more nvramp:startup-config EXEC** command will display the startup configuration, regardless of its location. The **erase nvramp:startup-config EXEC** command will erase the contents of NVRAM and delete the file pointed to by the **CONFIG\_FILE** environment variable.

When you save the configuration using the **copy system:running-config nvramp:startup-config** command, the router saves a complete version of the configuration file to the location specified by the **CONFIG\_FILE** environment variable and a distilled version to NVRAM. A distilled version is one that does not contain access list information. If NVRAM contains a complete configuration file, the router prompts you to confirm your overwrite of the complete version with the distilled version. If NVRAM contains a distilled configuration, the router does not prompt you for confirmation and proceeds with overwriting the existing distilled configuration file in NVRAM.



#### Note

If you specify a file in a Flash device as the **CONFIG\_FILE** environment variable, every time you save your configuration file with the **copy system:running-config nvramp:startup-config** command, the old configuration file is marked as “deleted,” and the new configuration file is saved to that device. Eventually, Flash memory will be full, because the old configuration files still take up memory. Use the **squeeze EXEC** command to permanently delete the old configuration files and reclaim the space.

The following example copies the running configuration file to the first USB port of a Cisco ASR1000 series router. This configuration is then used as the startup configuration when the system is restarted.

```
Router# copy system:running-config usb0:config2
Router# configure terminal
Router(config)# boot config usb0:config2
Router(config)# end
Router# copy system:running-config nvramp:startup-config
[ok]
Router# show bootvar
BOOT variable = usb0:rsp-boot-m
CONFIG_FILE variable = nvramp:
Current CONFIG_FILE variable = usb0:config2

Configuration register is 0x010F
```

## Configuring the Router to Download Configuration Files

You can configure the router to load one or two configuration files at system startup. The configuration files are loaded into memory and read in as if you were typing the commands at the command line. Thus, the configuration for the router will be a mixture of the original startup configuration and the one or two downloaded configuration files.

## Network Versus Host Configuration Files

For historical reasons, the first file the router downloads is called the network configuration file. The second file the router downloads is called the host configuration file. Two configuration files can be used when all of the routers on a network use many of the same commands. The network configuration file contains the standard commands used to configure all of the routers. The host configuration files contain the commands specific to one particular host. If you are loading two configuration files, the host configuration file should be the configuration file you want to have precedence over the other file. Both the network and host configuration files must reside on a network server reachable via TFTP.

## Configuring the Router to Download Configuration Files

You can specify an ordered list of network configuration and host configuration filenames. The Cisco IOS XE software scans this list until it loads the appropriate network or host configuration file.

To configure the router to download configuration files at system startup, perform at least one of the tasks described in the following sections:

- [Configuring the Router to Download the Network Configuration File](#)
- [Configuring the Router to Download the Host Configuration File](#)

If the router fails to load a configuration file during startup, it tries again every 10 minutes (the default setting) until a host provides the requested files. With each failed attempt, the router displays the following message on the console terminal:

```
Booting host-config... [timed out]
```

Refer to the *Internetwork Troubleshooting Guide* for troubleshooting procedures.

If there are any problems with the startup configuration file, or if the configuration register is set to ignore NVRAM, the router enters the Setup command facility. See the “Using the Setup Command Facility for Configuration Changes” chapter in this publication for details on the Setup command facility.

## Configuring the Router to Download the Network Configuration File

To configure the Cisco IOS XE software to download a network configuration file from a server at startup, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>boot network</b> { <b>tftp</b> :[[[//location]/directory]/filename]}	Specifies the network configuration file to download at startup, and the protocol to be used (TFTP).
Step 3	Router(config)# <b>service config</b>	Enables the system to automatically load the network file upon restart.
Step 4	Router(config)# <b>end</b>	Exits global configuration mode.
Step 5	Router# <b>copy system:running-config</b> <b>nvrām:startup-config</b>	Saves the running configuration to the startup configuration file.

For Step 2, if you do not specify a network configuration filename, the Cisco IOS XE software uses the default filename network-config. If you omit the address, the router uses the broadcast address.

You can specify more than one network configuration file. The software tries them in order entered until it loads one. This procedure can be useful for keeping files with different configuration information loaded on a network server.

## Configuring the Router to Download the Host Configuration File

To configure the Cisco IOS XE software to download a host configuration file from a server at startup, use the following commands in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>boot host</b> { <b>tftp:</b> [[[//location]/directory]/filename] }	Specifies the host configuration file to download at startup, and the protocol to be used (TFTP).
<b>Step 3</b>	Router(config)# <b>service config</b>	Enables the system to automatically load the host file upon restart.
<b>Step 4</b>	Router(config)# <b>end</b>	Exits global configuration mode.
<b>Step 5</b>	Router# <b>copy system:running-config</b> <b>nvram:startup-config</b>	Saves the running configuration to the startup configuration file.

If you do not specify a host configuration filename, the router uses its own name to form a host configuration filename by converting the name to all lowercase letters, removing all domain information, and appending “-config.” If no host name information is available, the software uses the default host configuration filename router-config. If you omit the address, the router uses the broadcast address.

You can specify more than one host configuration file. The Cisco IOS XE software tries them in order entered until it loads one. This procedure can be useful for keeping files with different configuration information loaded on a network server.

### Configuring the Router to Download Configuration Files at System Startup Example

In the following example, a router is configured to download the host configuration file named hostfile1 and the network configuration file named networkfile1. The router uses TFTP and the broadcast address to obtain the file.

```
Router# configure terminal
Router(config)# boot host tftp:hostfile1
Router(config)# boot network tftp:networkfile1
Router(config)# service config
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

## 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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>
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..	

# Feature Information for Managing Configuration Files

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 Configuration File Management Features

Feature Name	Releases	Feature Information
Parser Cache	Cisco IOS XE Release 2.1	<p>The Cisco IOS XE command-line parser in the Cisco IOS XE software performs the translation and execution (parsing) of command lines. The Parser Cache feature was developed to rapidly process large configuration files, thereby dramatically improving load time.</p> <p>For information about feature support in Cisco IOS XE software, use <a href="#">Feature Navigator</a>.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Controlling the Parser Cache</a></li> </ul>

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

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

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

© 2003-2009 Cisco Systems, Inc. All rights reserved.







# Exclusive Configuration Change Access and Access Session Locking

---

**First Published: February 28, 2005**  
**Last Updated: May 4, 2009**

Exclusive Configuration Change Access (also called the “Configuration Lock” feature) allows you to have exclusive change access to the Cisco IOS XE running configuration, preventing multiple users from making concurrent configuration changes.

The Access Session Locking addition to this feature extends the Exclusive Configuration Change Access feature such that **show** and **debug** commands entered by the user holding the configuration lock always have execution priority; **show** and **debug** commands entered by other users are only allowed to run after the processes initiated by the configuration lock owner have finished.

The Exclusive Configuration Change Access feature (“exposed lock”) is complementary with the locking mechanism in the [Configuration Replace and Configuration Rollback](#) feature (“rollback lock”).

## 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 Exclusive Configuration Change Access and Access Session Locking”](#) section on page 9.

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

- [Information About Exclusive Configuration Change Access and Access Session Locking](#), page 2
- [How to Use Exclusive Configuration Change Access and Access Session Locking](#), page 3



---

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Exclusive Configuration Change Access and Access Session Locking, page 6](#)
- [Additional References, page 7](#)
- [Feature Information for Exclusive Configuration Change Access and Access Session Locking, page 9](#)

## Information About Exclusive Configuration Change Access and Access Session Locking

To use the Exclusive Configuration Change Access and Access Session Locking feature, you should understand the following concepts:

- [Exclusive Configuration Change Access Functionality, page 2](#)
- [Access Session Locking, page 2](#)

### Exclusive Configuration Change Access Functionality

Devices running Cisco IOS XE software maintain a running configuration that determines the configuration state of the device. Changes to the running configuration alter the behavior of the device. Because Cisco IOS XE software allows multiple users to change the running configuration via the device CLI (including the device console and telnet SSH), in some operating environments it would be beneficial to prevent multiple users from making concurrent changes to the Cisco IOS XE running configuration. Temporarily limiting access to the Cisco IOS XE running configuration prevents inadvertent conflicts or cases where two users attempt to configure the same portion of the running configuration.

Exclusive configuration change access provides a mechanism to prevent concurrent configuration of Cisco IOS XE software by multiple users.

This feature provides exclusive change access to the Cisco IOS XE running configuration from the time you enter global configuration mode by using the **configure terminal** command. This gives the effect of a “configuration lock,” preventing other users from changing the Cisco IOS XE running configuration. The configuration lock is automatically released when the user exits Cisco IOS XE configuration mode.

The Exclusive Configuration Change Access feature is enabled using the **configuration mode exclusive** command in global configuration mode. Exclusive Configuration Change Access can be set to **auto**, so that the Cisco IOS XE configuration mode is locked whenever anyone uses the **configure terminal** command, or it can be set to **manual**, so that the Cisco IOS XE configuration mode is locked only when the **configure terminal lock** command is issued.

### Access Session Locking

Access Session Locking, in addition to preventing concurrent configuration access, provides an option to prevent simultaneous processes, such as a **show** command entered by another user, from executing while other configuration commands are being executed. When this feature is enabled, the commands entered by the user with the configuration lock (such as configuration commands) always have priority over commands entered by other users.

# How to Use Exclusive Configuration Change Access and Access Session Locking

This section contains the following procedures:

- [Enabling Exclusive Configuration Change Access and Access Session Locking, page 3](#) (required)
- [Obtaining Exclusive Configuration Change Access, page 4](#) (optional)
- [Monitoring and Troubleshooting the Exclusive Configuration Change Access and Access Session Locking Feature, page 5](#) (optional)

## Enabling Exclusive Configuration Change Access and Access Session Locking


Perform this task to gain exclusive access to the Cisco IOS XE configuration mode.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `configuration mode exclusive {auto | manual}`
4. `end`

### DETAILED STEPS

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

Command or Action	Purpose
<p><b>Step 3</b></p> <pre>configuration mode exclusive {auto   manual}</pre> <p><b>Example:</b> Router(config)# configuration mode exclusive auto</p>	<p>Enables exclusive configuration change access (configuration lock feature). When enabled, configuration sessions are performed in single-user (exclusive) mode.</p> <ul style="list-style-type: none"> <li>The <b>auto</b> keyword automatically locks the configuration session whenever the <b>configure terminal</b> command is used. This is the default.</li> <li>The <b>manual</b> keyword allows you to choose to lock the configuration session manually or leave it unlocked.</li> </ul> <div>  <p><b>Caution</b> If you use the <b>manual</b> keyword, you must perform the task described in the <a href="#">“Obtaining Exclusive Configuration Change Access”</a> section on page 4.</p> </div>
<p><b>Step 4</b></p> <pre>end</pre> <p><b>Example:</b> Router(config)# end</p>	<p>Ends your configuration session and returns the CLI to privileged EXEC mode.</p>

## Obtaining Exclusive Configuration Change Access

Perform this task to obtain exclusive configuration change access for the duration of your configuration session.



### Note

Use of the **lock** keyword with the **configure terminal** command is only necessary if the exclusive configuration mode has been set to **manual** (see the [“Enabling Exclusive Configuration Change Access and Access Session Locking”](#) section).

## SUMMARY STEPS

1. **enable**
2. **configure terminal lock**
3. Configure the system by entering your changes to the running configuration.
4. **end**  
or  
**exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal lock</b>  <b>Example:</b> Router# configure terminal lock	(Optional) Locks the Cisco IOS XE software in exclusive (single-user) mode.  <b>Note</b> This command can only be used if you have previously enabled configuration locking by using the <b>configuration mode exclusive</b> command.
Step 3	Configure the system by entering your changes to the running configuration.	—
Step 4	<b>end</b> or <b>exit</b>  <b>Example:</b> Router(config)# end Router# or  <b>Example:</b> Router(config)# exit Router#	Ends your configuration session, automatically releases the session lock obtained in Step 1, and exits to privileged EXEC mode.  <b>Note</b> Either the <b>end</b> command, the <b>exit</b> command, or the Ctrl-Z key combination releases the configuration lock. Use of the <b>end</b> command is recommended.

## Monitoring and Troubleshooting the Exclusive Configuration Change Access and Access Session Locking Feature

Perform one or both of the steps in this task to monitor or troubleshoot the Exclusive Configuration Change Access and Access Session Locking feature.

### SUMMARY STEPS

1. **show configuration lock**
2. **debug configuration lock**

### DETAILED STEPS

#### Step 1 **show configuration lock**

Use this command to display the status and details of any current configuration locks, including the owner, user, terminal, lock state, and lock class.

If you cannot enter global configuration mode, you can use this command to determine if the configuration session is currently locked by another user, and who that user is.

Router# **show configuration lock**

```

Parser Configure Lock
-----
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0

User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Router(config)#

```

## Step 2 debug configuration lock

Use this command to enable debugging of Cisco IOS XE configuration locks (exposed class locks).

```
Router# debug configuration lock
```

```

Session1 from console
=====

```

```

Router# configure terminal lock
Configuration mode locked exclusively. The lock will be cleared once you exit out of
configuration mode using end/exit
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Parser : LOCK REQUEST in EXCLUSIVE mode
Parser: <configure terminal lock> - Config. Lock requested by process <3> client <PARSER
Client>
Parser: <configure terminal lock> - Config. Lock acquired successfully !
Router(config)#

```

# Configuration Examples for Exclusive Configuration Change Access and Access Session Locking

This section provides the following configuration examples:

- [Configuring an Exclusive Lock in Auto Mode: Example, page 7](#)
- [Configuring an Exclusive Lock in Manual Mode: Example, page 7](#)

## Configuring an Exclusive Lock in Auto Mode: Example

The following example shows how to enable the exclusive lock in auto mode for single-user auto configuration mode using the **configuration mode exclusive auto** command. Once the Cisco IOS XE configuration file is locked exclusively, you can verify this configuration by using the **show configuration lock** command.

```
Router#
Router# configure terminal
Router(config)# configuration mode exclusive auto
Router(config)# exit
```

```
Router#
Router# configure terminal
! Locks configuration mode exclusively.
```

```
Router(config)# show configuration lock
```

```
Parser Configure Lock
```

```
Owner PID      : 10
User           : User1
TTY            : 3
Type           : EXCLUSIVE
State          : LOCKED
Class          : Exposed
Count          : 0
Pending Requests : 0
User debug info : 0
```

## Configuring an Exclusive Lock in Manual Mode: Example

The following example shows how to enable the exclusive locking feature in manual mode by using the **configuration mode exclusive manual** command. Once you have configured manual exclusive mode, you can lock the configuration mode by using the **configure terminal lock** command. In this mode, the **configure terminal** command will not automatically lock the parser configuration mode.

```
Router#
Router# configure terminal
Router(config)# configuration mode exclusive manual
Router(config)# exit
```

```
Router# configure terminal lock
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

```
*Mar 25 17:02:45.928: Configuration mode locked exclusively. The lock will be cleared
once you exit out of configuration mode using end/exit
```

## Additional References

The following sections provide references related to the Exclusive Configuration Change Access and Access Session Locking feature.

## Related Documents

Related Topic	Document Title
Commands for managing configuration files	<a href="#">Cisco IOS Configuration Management Command Reference</a>
Information about managing configuration files	<a href="#">Managing Configuration Files</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>



# Feature Information for Exclusive Configuration Change Access and Access Session Locking

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 Exclusive Configuration Change Access and Access Session Locking

Feature Name	Releases	Feature Information
Exclusive Configuration Change Access and Access Session Locking	Cisco IOS XE Release 2.1	<p>Exclusive Configuration Change Access (also called the “Configuration Lock” feature) allows you to have exclusive change access to the Cisco IOS running configuration, preventing multiple users from making concurrent configuration changes.</p> <p>The Access Session Locking addition to this feature extends the Exclusive Configuration Change Access feature such that <b>show</b> and <b>debug</b> commands entered by the user holding the configuration lock always have execution priority; <b>show</b> and <b>debug</b> commands entered by other users are only allowed to run after the processes initiated by the configuration lock owner have finished.</p> <p>The Exclusive Configuration Change Access feature (“exposed lock”) is complementary with the locking mechanism in the <a href="#">Configuration Replace and Configuration Rollback</a> feature (“rollback lock”).</p> <p>The Configuration Lock feature was integrated into Release 12.0S, and the Access Session Locking feature extension was implemented. The <b>configuration mode exclusive command</b> was extended to include the following keyword options: <b>expire</b>, <b>lock-show</b>, <b>interleave</b>, <b>terminate</b>, <b>config_wait</b>, and <b>retry_wait</b>. The output of the <b>show configuration lock</b> command was improved.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Information About Exclusive Configuration Change Access and Access Session Locking</a></li> <li><a href="#">How to Use Exclusive Configuration Change Access and Access Session Locking</a></li> </ul>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace,

MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2005-2009 Cisco Systems, Inc. All rights reserved.



# Configuration Generation Performance Enhancement

---

**First Published: March 2004**  
**Last Updated: May 4, 2009**

The Configuration Generation Performance Enhancement feature assists configuration management by enabling faster collection of running configuration file information. This feature is especially useful in managing large networks with numerous interfaces configured.

## 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 Configuration Generation Performance Enhancement” 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

- [Restrictions for Configuration Generation Performance Enhancement, page 2](#)
- [Information About Configuration Generation Performance Enhancement, page 2](#)
- [How to Configure the Configuration Generation Performance Enhancement, page 3](#)
- [Configuration Examples for the Configuration Generation Performance Enhancement, page 4](#)
- [Additional References, page 4](#)
- [Feature Information for Configuration Generation Performance Enhancement, page 6](#)



---

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

© 2004-2009 Cisco Systems, Inc. All rights reserved.

# Restrictions for Configuration Generation Performance Enhancement

The device on which the Configuration Generation Performance Enhancement feature is used must have enough memory available to store (cache) a large interface configuration file. For example, if the interface configurations take up 15 KB of memory, using this feature would require having an additional 15 KB of memory space available.

## Information About Configuration Generation Performance Enhancement

Before enabling the Configuration Generation Performance Enhancement feature, you should understand the following concepts:

- [Cisco IOS XE Software Configuration Storage, page 2](#)
- [Benefits of the Configuration Generation Performance Enhancement, page 2](#)

## Cisco IOS XE Software Configuration Storage

In the Cisco IOS XE software configuration model, the configuration state is maintained in a distributed manner, with each component storing its own configuration state. To retrieve configuration information, the software must poll every component to collect the distributed information. This configuration state retrieval operation is performed by a process known as nonvolatile generation (NVGEN), and it is used by command-line interface (CLI) commands such as **show running-configuration**, **write memory**, and **copy system:running-configuration** to display or copy the running system configuration. When invoked, NVGEN queries each system component and each instance of interface or other configuration objects. A running configuration file is constructed as NVGEN traverses the system performing these queries.

## Benefits of the Configuration Generation Performance Enhancement

Before the Configuration Generation Performance Enhancement feature was introduced, NVGEN always had to query the entire system and could generate only a total configuration. The time required to process the running configuration creates performance problems for configuration management, because completion of the NVGEN operation can take many minutes.

The Configuration Generation Performance Enhancement feature reduces the execution time for NVGEN processes and is especially useful for managing large configuration files that contain numerous interface configurations. This feature provides faster execution of commands that process the running system configuration by caching interface configuration information in system memory, and by retrieving only configuration information that has changed.

# How to Configure the Configuration Generation Performance Enhancement

This section contains the following procedure:

- [Configuring the Configuration Generation Performance Enhancement, page 3](#) (required)

## Configuring the Configuration Generation Performance Enhancement

Perform this task to enable the Configuration Generation Performance Enhancement.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parser config cache interface**
4. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>parser config cache interface</b>  <b>Example:</b> Router(config)# parser config cache interface	Reduces the time required for the CLI to execute commands that manage the running system configuration, especially for large configuration files.
Step 4	<b>end</b>  <b>Example:</b> Router(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

# Configuration Examples for the Configuration Generation Performance Enhancement

This section provides the following examples:

- [Configuring the Configuration Generation Performance Enhancement: Example, page 4](#)
- [Verifying the Configuration Generation Performance Enhancement: Example, page 4](#)

## Configuring the Configuration Generation Performance Enhancement: Example

The following example shows how to enable the Configuration Generation Performance Enhancement feature:

```
Router(config)# parser config cache interface
```

## Verifying the Configuration Generation Performance Enhancement: Example

You can verify that the **parser config cache interface** command has been enabled by checking for the command in the system configuration file displayed when you enter the **show running-configuration EXEC** command.



### Note

The first time you display the configuration file, you will not see much evidence of improvement in performance because the interface cache will be filled up. However, you will notice performance improvements when you enter subsequent NVGEN-type commands such as the **show running-configuration EXEC** command.

Each time the interface configuration of an changes, the cache of the specified interface is flushed. The other interface data remains cached as before. Entering an NVGEN-type command after modifying the interface configuration will once again not show much evidence of improvement until the next NVGEN-type command is entered.

```
Router# show running-configuration  
!  
!  
parser config cache interface  
!  
!
```

## Additional References

The following sections provide references related to the Configuration Generation Performance Enhancement feature.

## Related Documents

Related Topic	Document Title
System configuration file management	<a href="#">“Managing Configuration Files”</a> module in the <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i>
System configuration file management commands	<a href="#">Cisco IOS Configuration Fundamentals Command Reference</a>

## Standards

Standards	Title
None	—

## MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
None	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuration Generation Performance Enhancement

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 the Configuration Generation Performance Enhancement Feature

Feature Name	Releases	Feature Information
Configuration Generation Performance Enhancement	Cisco IOS XE Release 2.1, 2.2, 2.3	<p>The Configuration Generation Performance Enhancement feature assists configuration management by enabling faster collection of running configuration file information. This feature is especially useful in managing large networks with numerous interfaces configured.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Information About Configuration Generation Performance Enhancement</a></li> <li><a href="#">How to Configure the Configuration Generation Performance Enhancement</a></li> </ul> <p>Commands associated with this feature:</p> <ul style="list-style-type: none"> <li><b>parser config cache interface</b></li> <li><b>parser config partition</b></li> <li><b>parser cache</b></li> </ul>

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)



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

© 2004-2009 Cisco Systems, Inc. All rights reserved.





# Configuration Replace and Configuration Rollback

---

**First Published:** March 3, 2004  
**Last Updated:** May 4, 2009

The Configuration Replace and Configuration Rollback feature provides the capability to replace the current running configuration with any saved Cisco IOS XE configuration file. This functionality can be used to revert to a previous configuration state, effectively rolling back any configuration changes that were made since that configuration file was saved.

## 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 Configuration Replace and Configuration Rollback” section on page 16](#).

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

- [Information About Configuration Replace and Configuration Rollback, page 2](#)
- [How to Use Configuration Replace and Configuration Rollback, page 5](#)
- [Configuration Examples for Configuration Replace and Configuration Rollback, page 11](#)
- [Additional References, page 14](#)



---

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

© 2004-2009 Cisco Systems, Inc. All rights reserved.

- [Feature Information for Configuration Replace and Configuration Rollback, page 16](#)

# Information About Configuration Replace and Configuration Rollback

To use the Configuration Replace and Configuration Rollback feature, you should understand the following concepts:

- [Configuration Archive, page 2](#)
- [Configuration Replace, page 2](#)
- [Configuration Rollback, page 3](#)
- [Benefits of Configuration Replace and Configuration Rollback, page 4](#)

## Configuration Archive

The Cisco IOS XE configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco IOS XE configuration files to enhance the configuration rollback capability provided by the **configure replace** command. Before this feature was introduced, you could save copies of the running configuration using the **copy running-config destination-url** command, storing the replacement file either locally or remotely. However, this method lacked any automated file management. On the other hand, the Configuration Replace and Configuration Rollback feature provides the capability to automatically save copies of the running configuration to the Cisco IOS XE configuration archive. These archived files serve as checkpoint configuration references and can be used by the **configure replace** command to revert to previous configuration states.

The **archive config** command allows you to save Cisco IOS XE configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved Cisco IOS XE configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** command displays information for all configuration files saved in the Cisco IOS XE configuration archive.

The Cisco IOS XE configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, can be located on the following file systems:

- harddisk:
- bootflash:
- usb0:
- usb1:

## Configuration Replace

The **configure replace** command provides the capability to replace the current running configuration with any saved Cisco IOS XE configuration file. This functionality can be used to revert to a previous configuration state, effectively rolling back any configuration changes that were made since the previous configuration state was saved.

When using the **configure replace** command, you must specify a saved Cisco IOS XE configuration as the replacement configuration file for the current running configuration. The replacement file must be a complete configuration generated by a Cisco IOS XE device (for example, a configuration generated by the **copy running-config destination-url** command), or, if generated externally, the replacement file must comply with the format of files generated by Cisco IOS XE devices.

When the **configure replace** command is entered, the current running configuration is compared with the specified replacement configuration and a set of diffs is generated. The algorithm used to compare the two files is the same as that employed by the **show archive config differences** command. The resulting diffs are then applied by the Cisco IOS XE parser to achieve the replacement configuration state. Only the diffs are applied, avoiding potential service disruption from reapplying configuration commands that already exist in the current running configuration. This algorithm effectively handles configuration changes to order-dependent commands (such as access lists) through a multiple pass process. Under normal circumstances, no more than three passes are needed to complete a configuration replace operation, and a limit of five passes is performed to preclude any looping behavior.

The Cisco IOS XE **copy source-url running-config** command is often used to copy a stored Cisco IOS XE configuration file to the running configuration. When using the **copy source-url running-config** command as an alternative to the **configure replace target-url** command, the following major differences should be noted:

- The **copy source-url running-config** command is a merge operation and preserves all the commands from both the source file and the current running configuration. This command does not remove commands from the current running configuration that are not present in the source file. In contrast, the **configure replace target-url** command removes commands from the current running configuration that are not present in the replacement file and adds commands to the current running configuration that need to be added.
- The **copy source-url running-config** command applies every command in the source file, whether or not the command is already present in the current running configuration. This algorithm is inefficient and, in some cases, can result in service outages. In contrast, the **configure replace target-url** command only applies the commands that need to be applied—no existing commands in the current running configuration are reapplied.
- A partial configuration file may be used as the source file for the **copy source-url running-config** command, whereas a complete Cisco IOS XE configuration file must be used as the replacement file for the **configure replace target-url** command.

**Note**

When the **configure replace** command is used, the running configuration file is locked by default for the duration of the configuration replace operation. This locking mechanism prevents other users from changing the running configuration while the replacement operation is taking place, which might otherwise cause the replacement operation to terminate unsuccessfully. You can disable the locking of the running configuration by using the **no lock** keyword when issuing the **configure replace** command.

The running configuration lock is automatically cleared at the end of the configuration replace operation. You can display any locks that may be currently applied to the running configuration using the **show configuration lock** command.

**Note**

The **configure replace** command only replaces the running-configuration. However, certificates are associated with its private key and the private key resides in the private NVRAM which is not a part of running-configuration. So, the PKI certificate will be non-operational because of the private and public key mismatch and PKI cannot support the configure replace functionality.

## Configuration Rollback

The concept of rollback comes from the transactional processing model common to database operations. In a database transaction, you might make a set of changes to a given database table. You then must choose whether to commit the changes (apply the changes permanently) or to roll back the changes

(discard the changes and revert to the previous state of the table). In this context, rollback means that a journal file containing a log of the changes is discarded, and no changes are applied. The result of the rollback operation is to revert to the previous state, before any changes were applied.

The **configure replace** command allows you to revert to a previous configuration state, effectively rolling back changes that were made since the previous configuration state was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the Cisco IOS XE configuration rollback capability uses the concept of reverting to a specific configuration state based on a saved Cisco IOS XE configuration file. This concept is similar to the database idea of saving a checkpoint (a saved version of the database) to preserve a specific state.

If the configuration rollback capability is desired, you must save the Cisco IOS XE running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes (using the **configure replace target-url** command). Furthermore, since you can specify any saved Cisco IOS XE configuration file as the replacement configuration, you are not limited to a fixed number of rollbacks, as is the case in some rollback models based on a journal file.

## Configuration Rollback Confirmed Change

The Configuration Rollback Confirmed Change feature enables an added criteria of a confirmation to configuration changes. This functionality enables a rollback to occur if a confirmation of the requested changes is not received in a configured time frame. Command failures can also be configured to trigger a configuration rollback.

The following steps outline how this process is achieved:

1. When entering configuration mode, this new option allows you to request confirmation (a confirmation time limit must be supplied) of the configuration changes.
2. After exiting configuration mode, you must enter the confirmation command. If no confirmation is entered within the requested time limit, the configuration will revert to its previous state.

## Benefits of Configuration Replace and Configuration Rollback

- Allows you to revert to a previous configuration state, effectively rolling back configuration changes.
- Allows you to replace the current running configuration file with the startup configuration file without having to reload the router or manually undo CLI changes to the running configuration file, therefore reducing system downtime.
- Allows you to revert to any saved Cisco IOS XE configuration state.
- Simplifies configuration changes by allowing you to apply a complete configuration file to the router, where only the commands that need to be added or removed are affected.
- When using the **configure replace** command as an alternative to the **copy source-url running-config** command, increases efficiency and prevents risk of service outages by not reapplying existing commands in the current running configuration.

# How to Use Configuration Replace and Configuration Rollback

This section contains the following procedures:

- [Creating a Configuration Archive, page 5](#) (optional)
- [Performing a Configuration Replace or Configuration Rollback Operation, page 7](#) (required)
- [Monitoring and Troubleshooting the Configuration Replace and Configuration Rollback Feature, page 9](#) (optional)

## Creating a Configuration Archive

No prerequisite configuration is needed to use the **configure replace** command. Using the **configure replace** command in conjunction with the Cisco IOS XE configuration archive and the **archive config** command is optional but offers significant benefit for configuration rollback scenarios. Before using the **archive config** command, the configuration archive must be configured. Perform this task to configure the characteristics of the configuration archive.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **path** *url*
5. **maximum** *number*
6. **time-period** *minutes*
7. **end**
8. **archive config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>archive</b>  <b>Example:</b> Router(config)# archive	Enters archive configuration mode.

	Command or Action	Purpose
Step 4	<p><b>path</b> <i>url</i></p> <p><b>Example:</b> Router(config-archive)# path bootflash:myconfig</p>	<p>Specifies the location and filename prefix for the files in the Cisco IOS XE configuration archive.</p> <ul style="list-style-type: none"> <li>The <i>url</i> argument is a URL (accessible by the Cisco IOS XE file system) used for saving archive files of the running configuration file in the Cisco IOS XE configuration archive. You can set up an archive on any file system that your platform supports (see the “<a href="#">Configuration Archive</a>” section on page 2).</li> </ul> <p><b>Note</b> If a directory is specified in the path instead of file, the directory name must be followed by a forward slash as follows: <code>path flash:/directory/</code>. The forward slash is not necessary after a file name, only when specifying a directory.</p>
Step 5	<p><b>maximum</b> <i>number</i></p> <p><b>Example:</b> Router(config-archive)# maximum 14</p>	<p>(Optional) Sets the maximum number of archive files of the running configuration to be saved in the Cisco IOS XE configuration archive.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument is the maximum number of archive files of the running configuration to be saved in the Cisco IOS XE configuration archive. Valid values are from 1 to 14. The default is 10.</li> </ul> <p><b>Note</b> Before using this command, you must configure the <b>path</b> command to specify the location and filename prefix for the files in the Cisco IOS XE configuration archive.</p>
Step 6	<p><b>time-period</b> <i>minutes</i></p> <p><b>Example:</b> Router(config-archive)# time-period 10</p>	<p>(Optional) Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS XE configuration archive.</p> <ul style="list-style-type: none"> <li>The <i>minutes</i> argument specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco IOS XE configuration archive.</li> </ul> <p><b>Note</b> Before using this command, you must configure the <b>path</b> command to specify the location and filename prefix for the files in the Cisco IOS XE configuration archive.</p>
Step 7	<p><b>end</b></p> <p><b>Example:</b> Router(config-archive)# end</p>	<p>Exits to privileged EXEC mode.</p>
Step 8	<p><b>archive</b> <i>config</i></p> <p><b>Example:</b> Router# archive config</p>	<p>Saves the current running configuration file to the configuration archive.</p> <p><b>Note</b> The <b>path</b> command must be configured before using this command.</p>



## Performing a Configuration Replace or Configuration Rollback Operation

Perform this task to replace the current running configuration file with a saved Cisco IOS XE configuration file.

**Note**

You must create a configuration archive before performing this procedure. See [Creating a Configuration Archive, page 5](#) for detailed steps. The following procedure details how to return to that archived configuration in the event of a problem with the current running configuration.

### SUMMARY STEPS

1. **enable**
2. **configure replace** *target-url* [**nolock**] [**list**] [**force**] [**ignorecase**] [**revert trigger** [**error**] [**timer** *minutes*] | **time** *minutes*]
3. **configure revert** {**now** | **timer** {*minutes* | **idle** *minutes*}}
4. **configure confirm**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure replace</b> <i>target-url</i> [<b>nolock</b>] [<b>list</b>] [<b>force</b>] [<b>ignorecase</b>] [<b>revert trigger</b> [<b>error</b>] [<b>timer minutes</b>]   <b>time minutes</b>]</p> <p><b>Example:</b> Router# configure replace bootflash:myconfig-1 list time 30</p>	<p>Replaces the current running configuration file with a saved Cisco IOS XE configuration file.</p> <ul style="list-style-type: none"> <li>The <i>target-url</i> argument is a URL (accessible by the Cisco IOS XE file system) of the saved Cisco IOS XE configuration file that is to replace the current running configuration, such as the configuration file created using the <b>archive config</b> command.</li> <li>The <b>list</b> keyword displays a list of the command lines applied by the Cisco IOS XE software parser during each pass of the configuration replace operation. The total number of passes performed is also displayed.</li> <li>The <b>force</b> keyword replaces the current running configuration file with the specified saved Cisco IOS XE configuration file without prompting you for confirmation.</li> <li>The <b>time minutes</b> keyword and argument specify the time (in minutes) within which you must enter the <b>configure confirm</b> command to confirm replacement of the current running configuration file. If the <b>configure confirm</b> command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the <b>configure replace</b> command).</li> <li>The <b>nolock</b> keyword disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replace operation.</li> <li>The <b>revert trigger</b> keywords set the following triggers for reverting to the original configuration: <ul style="list-style-type: none"> <li><b>error</b>—Reverts to the original configuration upon error.</li> <li><b>timer minutes</b>—Reverts to the original configuration if specified time elapses.</li> </ul> </li> <li>The <b>ignorecase</b> keyword allows the configuration to ignore the case of the confirmation command.</li> </ul>

	Command or Action	Purpose
Step 3	<pre>configure revert {now   timer {minutes   idle minutes}}</pre> <p><b>Example:</b> Router# configure revert now</p>	<p>(Optional) To cancel the timed rollback and trigger the rollback immediately, or to reset parameters for the timed rollback, use the <b>configure revert</b> command in privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• <b>now</b>—Triggers the rollback immediately.</li> <li>• <b>timer</b>—Resets the configuration revert timer. <ul style="list-style-type: none"> <li>– Use the <i>minutes</i> argument with the <b>timer</b> keyword to specify a new revert time in minutes.</li> <li>– Use the <b>idle</b> keyword along with a time in minutes to set the maximum allowable time period of no activity before reverting to the saved configuration.</li> </ul> </li> </ul>
Step 4	<pre>configure confirm</pre> <p><b>Example:</b> Router# configure confirm</p>	<p>(Optional) Confirms replacement of the current running configuration file with a saved Cisco IOS XE configuration file.</p> <p><b>Note</b> Use this command only if the <b>time seconds</b> keyword and argument of the <b>configure replace</b> command are specified.</p>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router# exit</p>	Exits to user EXEC mode.

## Monitoring and Troubleshooting the Configuration Replace and Configuration Rollback Feature

Perform this task to monitor and troubleshoot the Configuration Replace and Configuration Rollback feature.

### SUMMARY STEPS

1. **enable**
2. **show archive**
3. **debug archive versioning**
4. **debug archive config timestamp**
5. **exit**

### DETAILED STEPS

- |               |  |
|---------------|--|
| <b>Step 1</b> | <b>enable</b><br>Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:<br><pre>Router&gt; enable</pre> <pre>Router#</pre> |
| <b>Step 2</b> | <b>show archive</b>  |

Use this command to display information about the files saved in the Cisco IOS XE configuration archive. For example:

```
Router# show archive
```

```
There are currently 1 archive configurations saved.
The next archive file will be named bootflash:myconfig-2
Archive #  Name
0
1      bootflash:myconfig-1 <- Most Recent
2
3
4
5
6
7
8
9
10
11
12
13
14
```

The following is sample output from the **show archive** command after several archive files of the running configuration have been saved. In this example, the maximum number of archive files to be saved is set to three.

```
Router# show archive
```

```
There are currently 3 archive configurations saved.
The next archive file will be named bootflash:myconfig-8
Archive #  Name
0
1      :Deleted
2      :Deleted
3      :Deleted
4      :Deleted
5      bootflash:myconfig-5
6      bootflash:myconfig-6
7      bootflash:myconfig-7 <- Most Recent
8
9
10
11
12
13
14
```

### Step 3 debug archive versioning

Use this command to enable debugging of the Cisco IOS XE configuration archive activities to help monitor and troubleshoot configuration replace and rollback. For example:

```
Router# debug archive versioning
```

```
Jan  9 06:46:28.419:backup_running_config
Jan  9 06:46:28.419:Current = 7
Jan  9 06:46:28.443:Writing backup file bootflash:myconfig-7
Jan  9 06:46:29.547: backup worked
```

### Step 4 debug archive config timestamp

Use this command to enable debugging of the processing time for each integral step of a configuration replace operation and the size of the configuration files being handled. For example:

```
Router# debug archive config timestamp
Router# configure replace bootflash:myconfig force

Timing Debug Statistics for IOS Config Replace operation:
  Time to read file slot0:sample_2.cfg = 0 msec (0 sec)
  Number of lines read:55
  Size of file          :1054

Starting Pass 1
  Time to read file system:running-config = 0 msec (0 sec)
  Number of lines read:93
  Size of file          :2539
  Time taken for positive rollback pass = 320 msec (0 sec)
  Time taken for negative rollback pass = 0 msec (0 sec)
  Time taken for negative incremental diffs pass = 59 msec (0 sec)
  Time taken by PI to apply changes = 0 msec (0 sec)
  Time taken for Pass 1 = 380 msec (0 sec)

Starting Pass 2
  Time to read file system:running-config = 0 msec (0 sec)
  Number of lines read:55
  Size of file          :1054
  Time taken for positive rollback pass = 0 msec (0 sec)
  Time taken for negative rollback pass = 0 msec (0 sec)
  Time taken for Pass 2 = 0 msec (0 sec)

Total number of passes:1
Rollback Done
```

#### Step 5 exit

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Configuration Examples for Configuration Replace and Configuration Rollback

This section provides the following configuration examples:

- [Creating a Configuration Archive: Example, page 12](#)
- [Replacing the Current Running Configuration with a Saved Cisco IOS XE Configuration File: Example, page 12](#)
- [Reverting to the Startup Configuration File: Example, page 13](#)
- [Performing a Configuration Replace Operation with the configure confirm Command: Example, page 13](#)
- [Performing a Configuration Rollback Operation: Example, page 13](#)

## Creating a Configuration Archive: Example

The following example shows how to perform the initial configuration of the Cisco IOS XE configuration archive. In this example, `bootflash:myconfig` is specified as the location and filename prefix for the files in the configuration archive and a value of 10 is set as the maximum number of archive files to be saved.

```
configure terminal
!
archive
 path bootflash:myconfig
 maximum 10
end
```

## Replacing the Current Running Configuration with a Saved Cisco IOS XE Configuration File: Example

The following example shows how to replace the current running configuration with a saved Cisco IOS XE configuration file named `bootflash:myconfig`. The **configure replace** command interactively prompts you to confirm the operation.

```
Router# configure replace bootflash:myconfig
```

```
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
```

```
Total number of passes: 1
Rollback Done
```

In the following example, the **list** keyword is specified in order to display the command lines that were applied during the configuration replace operation:

```
Router# configure replace bootflash:myconfig list
```

```
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
```

```
!Pass 1
```

```
!List of Commands:
no snmp-server community public ro
snmp-server community mystring ro
end
```

```
Total number of passes: 1
Rollback Done
```

## Reverting to the Startup Configuration File: Example

The following example shows how to revert to the Cisco IOS XE startup configuration file using the **configure replace** command. This example also shows the use of the optional **force** keyword to override the interactive user prompt.

```
Router# configure replace nvram:startup-config force

Total number of passes: 1
Rollback Done
```

## Performing a Configuration Replace Operation with the configure confirm Command: Example

The following example shows the use of the **configure replace** command with the **time seconds** keyword and argument. You must enter the **configure confirm** command within the specified time limit to confirm replacement of the current running configuration file. If the **configure confirm** command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored back to the configuration state that existed prior to entering the **configure replace** command).

```
Router# configure replace nvram:startup-config time 120

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y

Total number of passes: 1
Rollback Done

Router# configure confirm
```

## Performing a Configuration Rollback Operation: Example

The following example shows how to make changes to the current running configuration and then roll back the changes. As part of the configuration rollback operation, you must save the current running configuration before making changes to the file. In this example, the **archive config** command is used to save the current running configuration. The generated output of the **configure replace** command indicates that only one pass was performed to complete the rollback operation.



### Note

Before using the **archive config** command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS XE configuration archive.

You first save the current running configuration in the configuration archive as follows:

```
archive config
```

You then enter configuration changes as shown in the following example:

```
configure terminal
!
user netops2 password rain
```

```
user netops3 password snow
exit
```

After having made changes to the running configuration file, assume you now want to roll back these changes and revert to the configuration that existed before the changes were made. The **show archive** command is used to verify the version of the configuration to be used as a replacement file. The **configure replace** command is then used to revert to the replacement configuration file as shown in the following example:

```
Router# show archive

There are currently 1 archive configurations saved.
The next archive file will be named bootflash:myconfig-2
Archive #   Name
0
1          bootflash:myconfig-1 <- Most Recent
2
3
4
5
6
7
8
9
10

Router# configure replace bootflash:myconfig-1

Total number of passes: 1
Rollback Done
```

# Additional References

The following sections provide references related to the Configuration Replace and Configuration Rollback feature.

## Related Documents

Related Topic	Document Title
Configuration Locking	<a href="#">Exclusive Configuration Change Access and Access Session Locking</a>
Commands for managing configuration files	<a href="#">Cisco IOS Configuration Fundamentals Command Reference</a>
Information about managing configuration files	<a href="#">Managing Configuration Files</a>
Using the Contextual Configuration Diff Utility feature	<a href="#">Contextual Configuration Diff Utility</a>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—



## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuration Replace and Configuration Rollback

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. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release also support that feature.

**Table 1** Feature Information for Configuration Replace and Configuration Rollback

Feature Name	Releases	Feature Information
Configuration Replace and Configuration Rollback	Cisco IOS XE Release 2.1	<p>The Configuration Replace and Configuration Rollback feature provides the capability to replace the current running configuration with any saved Cisco IOS XE configuration file. This functionality can be used to revert to a previous configuration state, rolling back any configuration changes that were made since that configuration file was saved.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide feature information:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuration Archive, page 2</a></li> <li>• <a href="#">Configuration Replace, page 2</a></li> <li>• <a href="#">Configuration Rollback, page 3</a></li> <li>• <a href="#">Benefits of Configuration Replace and Configuration Rollback, page 4</a></li> <li>• <a href="#">Creating a Configuration Archive, page 5</a></li> <li>• <a href="#">Performing a Configuration Replace or Configuration Rollback Operation, page 7</a></li> <li>• <a href="#">Monitoring and Troubleshooting the Configuration Replace and Configuration Rollback Feature, page 9</a></li> </ul> <p>The following commands were modified by this feature: <b>archive config</b>, <b>configure confirm</b>, <b>configure replace</b>, <b>debug archive config timestamp</b>, <b>debug archive versioning</b>, <b>maximum</b>, <b>path</b> (archive configuration), <b>show archive</b>, <b>show configuration lock</b>, <b>time-period</b>.</p>

**Table 1**      **Feature Information for Configuration Replace and Configuration Rollback (continued)**

Feature Name	Releases	Feature Information
Configuration Versioning	Cisco IOS XE Release 2.1	<p>The Configuration Versioning feature allows you to maintain and manage backup copies of the Cisco IOS XE running configuration on or off the device. The Configuration Replace feature uses the Configuration Versioning feature to provide a rollback to a saved copy of the running configuration.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p>
Exclusive Configuration Change Access	Cisco IOS XE Release 2.1	<p>The Exclusive Configuration Change Access feature (also called the “Configuration Lock” feature) allows you to have exclusive change access to the Cisco IOS XE running configuration, preventing multiple users from making concurrent configuration changes.</p> <p>The following command was modified by this feature and applies to the Configuration Replace and Configuration Rollback feature: <b>show configuration lock</b>.</p> <p>Refer to the separate module, <a href="#">Exclusive Configuration Change Access and Access Session Locking</a>, for details</p>
Configuration Rollback Confirmed Change	Cisco IOS XE Release 2.1	<p>The Configuration Rollback Confirmed Change feature allows configuration changes to be performed with an optional requirement that they be confirmed.</p> <p>If this confirmation is not received, the configuration is returned to the state prior to the changes being applied.</p> <p>This mechanism provides a safeguard against inadvertent loss of connectivity between a network device and the user or management application due to configuration changes.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuration Rollback Confirmed Change, page 4</a></li> <li>• <a href="#">Performing a Configuration Replace or Configuration Rollback Operation, page 7</a></li> </ul> <p>The following commands were modified by this feature: <b>configure confirm</b>, <b>configure replace</b>, <b>configure revert</b>, <b>configure terminal</b></p>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace,

MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

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

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

© 2003-2009 Cisco Systems, Inc. All rights reserved.



# Contextual Configuration Diff Utility

---

**First Published: November 2003**

**Last Updated: May 4, 2009**

The Contextual Configuration Diff Utility feature provides the ability to perform a line-by-line comparison of any two configuration files (accessible through the Cisco IOS XE Integrated File System [IFS]) and generate a list of the differences between them. The generated output includes information regarding configuration lines that have been added, modified, or deleted, and the configuration modes within which a changed configuration line exists.

## 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 Contextual Configuration Diff Utility” section on page 8](#).

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

- [Prerequisites for Contextual Configuration Diff Utility, page 2](#)
- [Restrictions for Contextual Configuration Diff Utility, page 2](#)
- [Information About Contextual Configuration Diff Utility, page 2](#)
- [How to Use the Contextual Configuration Diff Utility, page 3](#)
- [Configuration Examples for the Contextual Configuration Diff Utility, page 4](#)
- [Additional References, page 7](#)
- [Feature Information for Contextual Configuration Diff Utility, page 8](#)



---

**Americas Headquarters:**

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

© 2003-2008 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Contextual Configuration Diff Utility

The format of the configuration files used for the Contextual Configuration Diff Utility feature must comply with standard Cisco IOS XE configuration file indentation rules as follows:

- Start all commands on a new line with no indentation, unless the command is within a configuration submode.
- Indent commands within a first-level configuration submode one space.
- Indent commands within a second-level configuration submode two spaces.
- Indent commands within subsequent submodes accordingly.

The router must have a contiguous block of memory larger than the combined size of the two configuration files being compared.

## Restrictions for Contextual Configuration Diff Utility

If the router does not have a contiguous block of memory larger than the combined size of the two configuration files being compared, the diff operation fails.

## Information About Contextual Configuration Diff Utility

Before using the Contextual Configuration Diff Utility feature, you should understand the following concepts:

- [Benefits of the Contextual Configuration Diff Utility, page 2](#)
- [Contextual Configuration Diff Utility Output Format, page 2](#)

## Benefits of the Contextual Configuration Diff Utility

The Contextual Configuration Diff Utility feature provides the ability to perform a line-by-line comparison of any two configuration files (accessible through the Cisco IOS XE File System [IFS]) and generate a list of the differences between them. The generated output includes information regarding the following items:

- Configuration lines that have been added, modified, or deleted.
- Configuration modes within which a changed configuration line exists.
- Location changes of configuration lines that are order-sensitive. For example, the **ip access-list** and **community-lists** commands are order-sensitive commands dependent on where they are listed within a configuration file in relation to other Cisco IOS XE commands of similar type.

## Contextual Configuration Diff Utility Output Format

### Diff Operation

The Contextual Configuration Diff Utility feature uses the filenames of two configuration files as input. A diff operation is performed on the specified files and a list of differences between the two files is generated as output. Interpreting the output is dependent on the order in which the two files are

configured (**show archive config differences** command). In this section, we assume that the filename of the file entered first is file1 and the filename of the file entered second is file2. Each entry in the generated output list is prefixed with a unique text symbol to indicate the type of difference found. The text symbols and their meanings are as follows:

- A minus symbol (-) indicates that the configuration line exists in file1 but not in file2.
- A plus symbol (+) indicates that the configuration line exists in file2 but not in file1.
- An exclamation point (!) with descriptive comments is used to identify order-sensitive configuration lines whose location is different in file1 than in file2.

#### Incremental Diff Operation

Some applications require that the generated output of a diff operation contain configuration lines that are unmodified (in other words, without the minus and plus symbols). For these applications, an incremental diff operation can be performed, which compares a specified configuration file to the running configuration file (**show archive config incremental-diffs** command).

When an incremental diff operation is performed, a list of the configuration lines that do not appear in the running configuration file (in other words, configuration lines that only appear in the specified file that is being compared to the running configuration file) is generated as output. An exclamation point (!) with descriptive comments is used to identify order-sensitive configuration lines whose location is different in the specified configuration file than in the running configuration file.

## How to Use the Contextual Configuration Diff Utility

This section provides the following procedure:

- [Using the Contextual Configuration Diff Utility, page 3](#) (required)

### Using the Contextual Configuration Diff Utility

This task describes how to use the Contextual Configuration Diff Utility feature.

#### SUMMARY STEPS

1. **enable**
2. **show archive config differences** [*file1 path*] [*file2 path*][*ignorecase*]  
or  
**show archive config incremental-diffs** [*file path*]
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show archive config differences</b> <i>[file1 path[file2 path][ignorecase]]</i> or <b>show archive config incremental-diffs</b> <i>file</i>  <b>Example:</b> Router# show archive config differences harddisk:test1 bootflash:test2 or  <b>Example:</b> Router# show archive config incremental-diffs nvram:startup-config	Performs a line-by-line comparison of any two configuration files (accessible through the IFS) and generates a list of the differences between them.  or Performs a line-by-line comparison of a specified configuration file to the running configuration file and generates a list of the configuration lines that do not appear in the running configuration file.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Exits to user EXEC mode.

## Configuration Examples for the Contextual Configuration Diff Utility

This section contains the following configuration examples:

- [Diff Operation: Example, page 4](#)
- [Incremental Diff Operation: Example, page 6](#)

### Diff Operation: Example

In this example, a diff operation is performed on the running and startup configuration files. [Table 1](#) shows the configuration files used for this example.



**Table 1** Configuration Files Used for the Diff Operation Example

Running Configuration File	Startup Configuration File
<pre>no ip subnet-zero ip cef interface FastEthernet1/0   ip address 10.7.7.7 255.0.0.0   no ip route-cache   no ip mroute-cache   duplex half no ip classless snmp-server community public RO</pre>	<pre>ip subnet-zero ip cef ip name-server 10.4.4.4 voice dnis-map 1   dnis 111 interface FastEthernet1/0   no ip address   no ip route-cache   no ip mroute-cache   shutdown   duplex half ip default-gateway 10.5.5.5 ip classless access-list 110 deny ip any host 10.1.1.1 access-list 110 deny ip any host 10.1.1.2 access-list 110 deny ip any host 10.1.1.3 snmp-server community private RW</pre>

The following is sample output from the **show archive config differences** command. This sample output displays the results of the diff operation performed on the configuration files in [Table 1](#).

```
Router# show archive config differences system:running-config nvram:startup-config
```

```
+ip subnet-zero
+ip name-server 10.4.4.4
+voice dnis-map 1
  +dnis 111
interface FastEthernet1/0
  +no ip address
  +shutdown
+ip default-gateway 10.5.5.5
+ip classless
+access-list 110 deny ip any host 10.1.1.1
+access-list 110 deny ip any host 10.1.1.2
+access-list 110 deny ip any host 10.1.1.3
+snmp-server community private RW
-no ip subnet-zero
interface FastEthernet1/0
  -ip address 10.7.7.7 255.0.0.0
-no ip classless
-snmpp-server community public RO
```

## Incremental Diff Operation: Example

In this example, an incremental diff operation is performed on the startup and running configuration files. [Table 2](#) shows the configuration files used for this example.

**Table 2** Configuration Files Used for the Incremental Diff Operation Example

Startup Configuration File	Running Configuration File
<pre>ip subnet-zero ip cef ip name-server 10.4.4.4 voice dnis-map 1   dnis 111 interface FastEthernet1/0   no ip address   no ip route-cache   no ip mroute-cache   shutdown   duplex half ip default-gateway 10.5.5.5 ip classless access-list 110 deny   ip any host 10.1.1.1 access-list 110 deny   ip any host 10.1.1.2 access-list 110 deny   ip any host 10.1.1.3 snmp-server community private RW</pre>	<pre>no ip subnet-zero ip cef interface FastEthernet1/0   ip address 10.7.7.7 255.0.0.0   no ip route-cache   no ip mroute-cache   duplex half no ip classless snmp-server community public RO</pre>

The following is sample output from the **show archive config incremental-diffs** command. This sample output displays the results of the incremental diff operation performed on the configuration files in [Table 2](#).

Router# **show archive config incremental-diffs startup-config**

```
ip subnet-zero
ip name-server 10.4.4.4
voice dnis-map 1
  dnis 111
interface FastEthernet1/0
  no ip address
  shutdown
ip default-gateway 10.5.5.5
ip classless
access-list 110 deny   ip any host 10.1.1.1
access-list 110 deny   ip any host 10.1.1.2
access-list 110 deny   ip any host 10.1.1.3
snmp-server community private RW
```

# Additional References

This section provides references related to the Contextual Configuration Diff Utility feature.

## Related Documents

Related Topic	Document Title
Information about managing configuration files	<a href="#">Managing Configuration Files</a>
Commands for managing configuration files	The <i>Cisco IOS Configuration Fundamentals Command Reference</i>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Feature Information for Contextual Configuration Diff Utility

[Table 3](#) 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 3](#) lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release also support that feature.

**Table 3**      **Feature Information for Contextual Configuration Diff Utility**

Feature Name	Releases	Feature Information
Contextual Configuration Diff Utility	Cisco IOS XE Release 2.1	<p>The Contextual Configuration Diff Utility feature provides the ability to perform a line-by-line comparison of any two configuration files and generate a list of the differences between them. The generated output includes information regarding configuration lines that have been added, modified, or deleted, and the configuration modes within which a changed configuration line exists.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Benefits of the Contextual Configuration Diff Utility, page 2</a></li> <li>• <a href="#">Contextual Configuration Diff Utility Output Format, page 2</a></li> <li>• <a href="#">Using the Contextual Configuration Diff Utility, page 3</a></li> </ul> <p>The following commands were modified by this feature:  <b>show archive config differences</b>, <b>show archive config incremental-diffs</b>.</p>

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

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

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

© 2003-2008 Cisco Systems, Inc. All rights reserved.





# Configuration Change Notification and Logging

---

**First Published: November 3, 2003**

**Last Updated: May 4, 2009**

Prior to the introduction of this feature, the only way to determine if the Cisco IOS XE software configuration had changed was to save a copy of the running and startup configurations to a local computer and do a line-by-line comparison. This comparison method can identify changes that occurred, but does not specify the sequence in which the changes occurred, or the person responsible for the changes.

The Configuration Change Notification and Logging (Config Log Archive) feature allows the tracking of configuration changes entered on a per-session and per-user basis by implementing an archive function. This archive saves 'configuration logs' that track each configuration command that is applied, who applied the command, the parser return code (PRC) for the command, and the time the command was applied. This feature also adds a notification mechanism that sends asynchronous notifications to registered applications whenever the configuration log changes.

## 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 Configuration Change Notification and Logging” section on page 12](#).

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

- [Restrictions for Configuration Change Notification and Logging, page 2](#)
- [Information About Configuration Change Notification and Logging, page 2](#)
- [How to Configure the Configuration Change Notification and Logging Feature, page 3](#)



---

**Americas Headquarters:**

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

© 2003-2009 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for the Configuration Change Notification and Logging Feature, page 10](#)
- [Additional References, page 10](#)
- [Feature Information for Configuration Change Notification and Logging, page 12](#)

## Restrictions for Configuration Change Notification and Logging

- Only complete commands input in a configuration mode are logged.
- Commands that are part of a configuration file applied with the **copy** command are not logged.

## Information About Configuration Change Notification and Logging

To configure the Configuration Change Notification and Logging feature, you must understand the following concepts:

- [Configuration Log, page 2](#)
- [Configuration Change Notifications and Config Change Logging, page 3](#)

## Configuration Log

The Configuration Change Notification and Logging feature tracks changes made to the Cisco IOS XE software running configuration by maintaining a configuration log. This configuration log tracks changes initiated only through the command-line interface (CLI) or HTTP. Only complete commands that result in the invocation of action routines are logged. The following types of entries are not logged:

- Commands that result in a syntax error message
- Partial commands that invoke the router help system

For each configuration command that is executed, the following information is logged:

- The command that was executed
- The configuration mode in which the command was executed
- The name of the user that executed the command
- The time at which the command was executed
- A configuration change sequence number
- Parser return codes for the command

You can display information from the configuration log through the use of the **show archive log config** command, with the exception of the parser return codes, which are for use by internal Cisco IOS XE applications only.



## Configuration Change Notifications and Config Change Logging

You can configure the Configuration Change and Notification Logging feature to send notification of configuration changes to the Cisco IOS XE software system logging (syslog) process. Syslog notifications allow monitoring of the configuration log information without performing polling and information gathering tasks.

The Configuration Change Notification and Logging feature allows the tracking of configuration changes entered by users on a per-session and per-user basis. This tool allows administrators to track any configuration change made to the Cisco IOS XE software running configuration, and identify the user that made that change.

## How to Configure the Configuration Change Notification and Logging Feature

This section contains the following procedures:

- [Configuring the Configuration Change Notification and Logging Feature, page 3](#)
- [Displaying Configuration Log Entries and Statistics, page 5](#)
- [Clearing Configuration Log Entries, page 7](#)

## Configuring the Configuration Change Notification and Logging Feature

Perform this task to enable the Configuration Change Notification and Logging feature.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging enable**
6. **logging size *entries***
7. **hidekeys**
8. **notify syslog**
9. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>archive</b>  <b>Example:</b> Router(config)# archive	Enters archive configuration mode.
Step 4	<b>log config</b>  <b>Example:</b> Router(config-archive)# log config	Enters configuration change logger configuration mode.
Step 5	<b>logging enable</b>  <b>Example:</b> Router(config-archive-log-config)# logging enable	Enables the logging of configuration changes. <ul style="list-style-type: none"> <li>Logging of configuration changes is disabled by default.</li> </ul>
Step 6	<b>logging size entries</b>  <b>Example:</b> Router(config-archive-log-config)# logging size 200	(Optional) Specifies the maximum number of entries retained in the configuration log. <ul style="list-style-type: none"> <li>Valid values for the <i>entries</i> argument range from 1 to 1000. The default value is 100 entries.</li> <li>When the configuration log is full, the oldest entry is deleted every time a new entry is added.</li> </ul> <b>Note</b> If a new log size is specified that is smaller than the current log size, the oldest log entries is immediately purged until the new log size is satisfied, regardless of the age of the log entries.
Step 7	<b>hidekeys</b>  <b>Example:</b> Router(config-archive-log-config)# hidekeys	(Optional) Suppresses the display of password information in configuration log files. <b>Note</b> Enabling the <b>hidekeys</b> command increases security by preventing password information from being displayed in configuration log files.

	Command or Action	Purpose
Step 8	<code>notify syslog</code>  <b>Example:</b> Router(config-archive-log-config)# <code>notify syslog</code>	(Optional) Enables the sending of notifications of configuration changes to a remote syslog.
Step 9	<code>end</code>  <b>Example:</b> Router(config-archive-log-config)# <code>end</code>	Exits to privileged EXEC mode.

## Displaying Configuration Log Entries and Statistics

Perform this task to display entries from the configuration log or statistics about the memory usage of the configuration log.

To display configuration log entries and to monitor the memory usage of the configuration log, the Configuration Change Notification and Logging feature provides the **show archive log config** command.

### SUMMARY STEPS

1. `enable`
2. `show archive log config number [end-number]`
3. `show archive log config all provisioning`
4. `show archive log config statistics`
5. `exit`

## DETAILED STEPS

### Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
```

### Step 2 **show archive log config *number* [*end-number*]**

Use this command to display configuration log entries by record numbers. If you specify a record number for the optional *end-number* argument, all log entries with record numbers between the values entered for the *number* and *end-number* arguments are displayed. For example:

```
Router# show archive log config 1 2
```

idx	sess	user@line	Logged command
1	1	user1@console	logging enable
2	1	user1@console	logging size 200

This example displays configuration log entry numbers 1 and 2. Valid values for the *number* and *end-number* argument range from 1 to 2147483647.

### Step 3 **show archive log config provisioning**

Use this command to display all configuration log files as they would appear in a configuration file rather than in tabular format. For example:

```
Router# show archive log config all provisioning
```

```
archive
log config
logging enable
logging size 200
```

This display also shows the commands used to change configuration modes, which are required to correctly apply the logged commands.

### Step 4 **show archive log config statistics**

Use this command to display memory usage information for the configuration. For example:

```
Router# show archive log config statistics
```

```
Config Log Session Info:
  Number of sessions being tracked: 1
  Memory being held: 3910 bytes
  Total memory allocated for session tracking: 3910 bytes
  Total memory freed from session tracking: 0 bytes
```

```
Config Log log-queue Info:
  Number of entries in the log-queue: 3
  Memory being held in the log-queue: 671 bytes
  Total memory allocated for log entries: 671 bytes
  Total memory freed from log entries: 0 bytes
```

### Step 5 **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Clearing Configuration Log Entries

Entries from the configuration log can be cleared in one of two ways. The size of the configuration log can be reduced using the **logging size** command, or the configuration log can be disabled and then reenabled with the **logging enable** command.

This section contains the following procedures:

- [Clearing the Configuration Log by Reducing the Log Size, page 7](#)
- [Clearing the Configuration Log by Disabling the Configuration Log, page 8](#)

### Clearing the Configuration Log by Reducing the Log Size

Perform this task to clear entries from the configuration log using the **logging size** command.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging size entries**
6. **logging size entries**
7. **end**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>archive</b>  <b>Example:</b> Router(config)# archive	Enters archive configuration mode.
Step 4	<b>log config</b>  <b>Example:</b> Router(config-archive)# log config	Enters configuration change logger configuration mode.

	Command or Action	Purpose
Step 5	<code>logging size entries</code>	Specifies the maximum number of entries retained in the configuration log.
	<b>Example:</b> <pre>Router(config-archive-log-config)# logging size 1</pre>	<b>Note</b> Setting the size of the configuration log to 1 results in all but the most recent entry being purged.
Step 6	<code>logging size entries</code>	Specifies the maximum number of entries retained in the configuration log.
	<b>Example:</b> <pre>Router(config-archive-log-config)# logging size 200</pre>	<b>Note</b> The size of the configuration log should be reset to the desired value after clearing the configuration log.
Step 7	<code>end</code>	Exits to privileged EXEC mode.
	<b>Example:</b> <pre>Router(config-archive-log-config)# end</pre>	

## Examples

The following example shows how to clear the configuration log by reducing the log size to 1, then resetting the log size to the desired value:

```
Router# configure terminal

Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# logging size 1
Router(config-archive-log-config)# logging size 200
Router(config-archive-log-config)# end
```

## Clearing the Configuration Log by Disabling the Configuration Log

Perform this task to clear entries from the configuration log using the **logging enable** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **no logging enable**
6. **logging enable**
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>archive</b>  <b>Example:</b> Router(config)# archive	Enters archive configuration mode.
Step 4	<b>log config</b>  <b>Example:</b> Router(config-archive)# log config	Enters configuration change logger configuration mode.
Step 5	<b>no logging enable</b>  <b>Example:</b> Router(config-archive-log-config)# no logging enable	Disables the logging of configuration changes.  <b>Note</b> Disabling the configuration log results in all records being purged.
Step 6	<b>logging enable</b>  <b>Example:</b> Router(config-archive-log-config)# logging enable	Enables the logging of configuration changes.
Step 7	<b>end</b>  <b>Example:</b> Router(config-archive-log-config)# end	Exits to privileged EXEC mode.

## Examples

The following example clears the configuration log by disabling and then reenabling the configuration log:

```
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# no logging enable
Router(config-archive-log-config)# logging enable
Router(config-archive-log-config)# end
```

# Configuration Examples for the Configuration Change Notification and Logging Feature

- This section provides the following configuration example:
- [Configuring the Configuration Change Notification and Logging Feature: Example](#)

## Configuring the Configuration Change Notification and Logging Feature: Example

The following example shows how to enable configuration logging with a maximum of 200 entries in the configuration log. In the example, security is increased by suppressing the display of password information in configuration log records, and syslog notifications are turned on.

```
configure terminal

archive
 log config
 logging enable
 logging size 200
 hidekeys
 notify syslog
```

## Additional References

The following sections provide references related to the Configuration Change Notification and Logging. feature:

## Related Documents

Related Topic	Document Title
Information about managing configuration files	<a href="#">Managing Configuration Files</a>
Commands for managing configuration files	<a href="#">Cisco IOS Configuration Fundamentals Command Reference</a>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—



## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuration Change Notification and Logging

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 Configuration Change Notification and Logging

Feature Name	Releases	Feature Information
Configuration Change Notification and Logging	Cisco IOS XE Release 2.1	<p>The Configuration Change Notification and Logging (Configuration Logging) feature allows the tracking of configuration changes entered on a per-session and per-user basis by implementing a configuration log. The configuration log tracks each configuration command that is applied, who applied the command, the parser return code for the command, and the time the command was applied. This feature also adds a notification mechanism that sends asynchronous notifications to registered applications whenever the configuration log changes.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Configuration Change Notifications and Config Change Logging, page 3</a></li> <li><a href="#">Configuring the Configuration Change Notification and Logging Feature, page 3</a></li> <li><a href="#">Displaying Configuration Log Entries and Statistics, page 5</a></li> </ul> <p>The following commands were modified by this feature: <b>archive</b>, <b>hidekeys</b>, <b>log config</b>, <b>logging enable</b>, <b>logging size</b>, <b>notify syslog</b>, <b>show archive log config</b>.</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus,

Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

© 2003-2009 Cisco Systems, Inc. All rights reserved.





# Configuration Partitioning

---

**First Published: February 26, 2007**

**Last Updated: May 4, 2009**

The Configuration Partitioning feature provides modularization (“partitioning”) of the running configuration state to provide granular access to the running configuration in Cisco IOS XE software.

This feature is enabled by default in Cisco IOS XE software images that include this feature.

The configuration state of a device is retrieved dynamically whenever a user issues the **show running-config** command. When the Configuration Partitioning feature is enabled, the system groups the configuration state of the device into parts (called “partitions”) so that only the configuration state the user wishes to review is retrieved when generating a displayed list of commands in the running configuration. This feature improves performance for high-end systems with complex configurations because only a part of the running configuration state is processed when generating the running configuration command list, as opposed to the existing method of processing the entire system configuration state.

Default configuration partitions are provided by the introduction of this feature; other Cisco IOS XE software features may define their own command partitions in later releases.

## 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 Configuration Partitioning” section on page 19](#).

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

- [Information About Configuration Partitioning, page 2](#)



---

**Americas Headquarters:**

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

© 2007-2009 Cisco Systems, Inc. All rights reserved.

- [How to Use the Configuration Partitioning Feature, page 3](#)
- [Configuration Examples for Configuration Partitioning, page 6](#)
- [Additional References, page 17](#)
- [Feature Information for Configuration Partitioning, page 19](#)

## Information About Configuration Partitioning

To use the Configuration Partitioning feature, you should understand the following concepts:

- [System Running Configurations](#)
- [Retrieving the Running Configuration for Display or Copy Operations](#)
- [Benefits of Partitioning the Running Configuration](#)

### System Running Configurations

Managing the configuration of any Cisco IOS XE software-based device involves managing the startup configuration (startup-config), which is a file stored in nonvolatile memory, and the running configuration (running-config), which is the set of all configuration options currently in effect on the system. Typically, the startup configuration file is loaded when the system boots, and changes to the system's running configuration, applied using the command-line interface (CLI), are saved by copying the running configuration to a configuration file (either locally or on the network), which can then be used to configure the device at startup, or used to configure other devices.

### Retrieving the Running Configuration for Display or Copy Operations

In the Cisco IOS XE software configuration model, the configuration state is maintained in a distributed manner, with each component storing its own configuration state. To retrieve global configuration information, the software must poll every component to collect the distributed information. This configuration state retrieval operation is performed by a process known as nonvolatile generation (NVGEN), and it is invoked by commands such as **show running-config**, which is used to display the current configuration state, and **copy system:running-configuration**, which is used to save the running configuration by copying it to a file. When invoked, the NVGEN process queries each system component, each interface instance, and all other configured component objects in a standard sequence. A running configuration file is constructed as NVGEN traverses the system performing these queries, and it is this "virtual file" that is displayed or copied.

### Benefits of Partitioning the Running Configuration

The Configuration Partitioning feature is the latest in a series of Configuration Generation Performance Enhancement Features for Cisco IOS XE software. (See the "[Related Documents](#)" section on [page 17](#) for related features.) This feature improves the system's response time by providing a method for querying only the system component you wish to review when issuing the **show running-config** command.

When the Configuration Partitioning feature is enabled, the system groups the configuration state of the device into parts (called “partitions”) for the purpose of generating the virtual running configuration file (the list of configuration commands). A new command, **show running-config partition**, allows you to display only the part of the running configuration that you want to examine, rather than having to display the entire running configuration at once, or displaying only lines that match a certain string.

The key benefit of this feature is that it increases system performance by allowing the system to run the NVGEN process for only the collection of system components (such as specific interfaces) that you need to display. This is in contrast to other existing extensions to the **show running-config** command, which only *filter* the generated list after all system components have been processed.

The selective processing of the system’s configuration state for the purpose of generating a partial running configuration is called “configuration partitioning.”

More granular access to configuration information offers important performance benefits for high-end routing platforms with very large configuration files, while also enhancing configuration management by allowing advanced configuration features to be implemented at a more granular level. Advanced configuration options include Cisco IOS XE software support for provisioning of customer services, Config Rollback, Config Locking, and configuration access control.

## How to Use the Configuration Partitioning Feature

This section contains the following tasks:

- [Displaying Configuration Partitions, page 3](#) (optional)
- [Disabling the Configuration Partitioning Feature, page 5](#) (optional)

### Displaying Configuration Partitions

The main method of taking advantage of this feature is by using the **show running-config partition part** command, which is a specialized extension to the **show running-config** command.

**Note**

The **partition part** command extension is not available for the **more system:running-config** command.

Because this feature offers improved performance for existing commands, this feature is enabled by default in Cisco IOS XE software images that support this feature. To quickly determine if this feature is supported and running on your system, issue the **show running-config partition ?** command in privileged EXEC mode.

#### SUMMARY STEPS

1. **show running-config partition ?**
2. **show runningconfig partition part**

#### DETAILED STEPS

**Step 1** **show running-config partition ?**

Issuing this command will show you the list of running configuration parts available for display on your system.

If the Configuration Partitioning feature is supported on your system and is enabled, you will see the string “config partition is TRUE” as the first line of help output.

If you receive an error message when entering the command syntax shown here, this feature is not supported on your system. See the command documentation for the **show running-config** command for existing extensions of that command in other releases that allow you to show only part of the running configuration.

**Note**

The list of available configuration parts may vary by software image and is dependent on what features are currently configured.

```
Router# show running-config partition ?
access-list      All access-list configurations
class-map        All class-map configurations
common           All remaining unregistered configurations
global-cdp       All global cdp configurations
interface        Each Interface specific Configurations
ip-as-path       All IP as-path configurations
ip-community     All IP community list configurations
ip-domain-list   All ip domain list configurations
ip-prefix-list   All ip prefix-list configurations
ip-static-routes All IP static configurations
line             All line mode configurations
policy-map       All policy-map configurations
route-map        All route-map configurations
router           All routing configurations
snmp             All SNMP configurations
tacacs           All TACACS configurations
```

Choose the part of the running configuration you want to display, and use the associated keyword as the *part* argument in Step 2.

**Step 2** **show running-config partition part**

As an example, to have the system perform the NVGEN process on only the components associated with the access-list parts of the running configuration state, and display only the access-list related configurations, you would enter the **show running-config partition access-list** command:

```
Router# show running-config partition access-list
Building configuration...

Current configuration : 127 bytes
!
Configuration of Partition access-list
!
!
!
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
!
end
```

**Note**

This command also allows you to run the NVGEN process and display the resulting output for specific interfaces. This is a key capability of this feature, as it was designed for systems with numerous active interfaces.

In the following example, the main configuration partition is the interface configuration, and the specific part of the configuration to be generated is the configuration for Fast Ethernet interface 0/0.



```
Router# show running-config partition interface fastethernet0/0
Building configuration...

Current configuration : 213 bytes
!
Configuration of Partition interface FastEthernet0/0
!
!
interface FastEthernet0/0
 ip address 10.4.2.39 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 ipv6 enable
 no cdp enable
!
!
end
```

## Disabling the Configuration Partitioning Feature

Because this feature offers improved performance for existing commands, this feature is enabled by default for Cisco IOS XE software images that support this feature. However, you may want to disable this feature if you determine that it is not needed, as this feature does use a small amount of system resources (memory and CPU utilization). To disable configuration partitioning, perform the following task, which assumes you are starting in user EXEC mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no parser config partition**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>no parser config partition</b>  <b>Example:</b> Router(config)# no parser config partition	Disables the configuration partitioning feature.

## What to Do Next

To reenable the feature after it has been disabled, use the **parser config partition** command in global configuration mode.



### Note

As this feature is enabled by default, only the **no** form will appear in the running configuration file, or will be written to the startup configuration file when you issue the **copy running-config startup-config** command.

# Configuration Examples for Configuration Partitioning

This section provides examples of displaying configuration partitions with the **show running-config partition** command:

- [Displaying Configuration Partitions: Example](#)

## Displaying Configuration Partitions: Example

In this example, the **show running-config partition** command is used with related commands in a series of steps an administrator might take to check the status of a specific interface and the current configuration of some of the system's other components. Comparable filtered output from the standard **show running-config** command (for example, **show running-config | include access-list**) is included for demonstration purposes.



### Note

The *part* argument can consist of multiple partition name keywords, as in **show running-config part router eigrp 1**.

```
Router# show running-config partition ?
access-list      All access-list configurations
class-map        All class-map configurations
```

common	All remaining unregistered configurations
global-cdp	All global cdp configurations
interface	Each Interface specific Configurations
ip-as-path	All IP as-path configurations
ip-community	All IP community list configurations
ip-domain-list	All ip domain list configurations
ip-prefix-list	All ip prefix-list configurations
ip-static-routes	All IP static configurations
line	All line mode configurations
policy-map	All policy-map configurations
route-map	All route-map configurations
router	All routing configurations
snmp	All SNMP configurations
tacacs	All TACACS configurations

```
Router# show running-config partition access-list
Building configuration...
```

```
Current configuration : 87 bytes
!
!
!
!
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
!
end
```

```
Router# show running-config | include access-list
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
Router#
```

```
Router# show running-config partition class-map
Building configuration...
```

```
Current configuration : 78 bytes
!
!
!
class-map match-all abc
  match any
class-map match-all xyz
!
!
!
end
```

```
Router# show running-config | begin class-map
class-map match-all abc
  match any
class-map match-all xyz
!
!
```

```
Router# show running-config partition global-cdp
Building configuration...
```

```
Current configuration : 43 bytes
!
!
!
cdp timer 20
```

```

cdp holdtime 100
!
end

```

```
Router# show running-config | include global-cdp
```

```

cdp timer 20
cdp holdtime 100
Router#

```

```
Router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet2/0	10.4.2.32	YES	NVRAM	up	up
FastEthernet2/1	unassigned	YES	NVRAM	administratively down	down
FastEthernet2/2	unassigned	YES	NVRAM	administratively down	down
FastEthernet2/3	unassigned	YES	NVRAM	administratively down	down
Serial3/0	unassigned	YES	NVRAM	administratively down	down
Serial3/1	unassigned	YES	NVRAM	administratively down	down
Serial3/2	unassigned	YES	NVRAM	administratively down	down
Serial3/3	unassigned	YES	NVRAM	administratively down	down
Loopback0	unassigned	YES	NVRAM	administratively down	down
Loopback234	unassigned	YES	NVRAM	administratively down	down

```
Router# show running-config partition interface fastethernet0/0
```

```
Building configuration...
```

```
Current configuration : 98 bytes
```

```

!
!
!
interface FastEthernet0/0
  no ip address
  no ip route-cache
  shutdown
  duplex half
!
!
end

```

```
Router# show running-config partition interface FastEthernet2/0
```

```
Building configuration...
```

```
Current configuration : 122 bytes
```

```

!
!
!
interface FastEthernet2/0
  ip address 10.4.2.32 255.255.255.0
  no ip proxy-arp
  no ip route-cache
  duplex half
!
!
end

```

```
Router# show running-config partition interface FastEthernet2/1
```

```
Building configuration...
```

```
Current configuration : 94 bytes
```

```

!
!
!
interface FastEthernet2/1
  no ip address

```

```
no ip route-cache
shutdown
duplex half
!
!
end
```

```
Router# show running-config partition interface FastEthernet2/2
Building configuration...
```

```
Current configuration : 94 bytes
!
!
!
interface FastEthernet2/2
no ip address
no ip route-cache
shutdown
duplex half
!
!
end
```

```
Router# show running-config partition interface FastEthernet2/3
Building configuration...
```

```
Current configuration : 94 bytes
!
!
!
interface FastEthernet2/3
no ip address
no ip route-cache
shutdown
duplex half
!
!
end
```

```
Router# show running-config partition interface serial3/0
Building configuration...
```

```
Current configuration : 103 bytes
!
!
!
interface Serial3/0
no ip address
no ip route-cache
shutdown
serial restart-delay 0
!
!
end
```

```
Router# show running-config partition interface serial3/1
Building configuration...
```

```
Current configuration : 103 bytes
!
!
!
interface Serial3/1
no ip address
```

```

no ip route-cache
shutdown
serial restart-delay 0
!
!
end

```

```

Router# show running-config partition interface serial3/2
Building configuration...

```

```

Current configuration : 103 bytes
!
!
!
interface Serial3/2
no ip address
no ip route-cache
shutdown
serial restart-delay 0
!
!
end

```

```

Router# show running-config partition interface serial3/3
Building configuration...

```

```

Current configuration : 103 bytes
!
!
!
interface Serial3/3
no ip address
no ip route-cache
shutdown
serial restart-delay 0
!
!
end

```

```

Router# show running-config partition interface loopback0
Building configuration...

```

```

Current configuration : 79 bytes
!
!
!
interface Loopback0
no ip address
no ip route-cache
shutdown
!
!
end

```

```

Router# show running-config partition interface loopback1
                                     ^
% Invalid input detected at '^' marker.

```

```

Router# show running-config partition interface loopback234
Building configuration...

```

```

Current configuration : 81 bytes
!
!

```

```
!
interface Loopback234
  no ip address
  no ip route-cache
  shutdown
!
!
end

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface FastEthernet 2/0.1
Router(config-subif)# exit
Router(config)# exit

Router#
00:13:05: %SYS-5-CONFIG_I: Configured from console by console
Router# show running-config partition interface FastEthernet2/0.1
Building configuration...

Current configuration : 58 bytes
!
!
!
interface FastEthernet2/0.1
  no ip route-cache
!
!
end
Router# show run partition ip?
ip-as-path ip-community ip-domain-list ip-static-routes

Router# show running-config partition ip-as
Router# show running-config partition ip-as-path

Building configuration...

Current configuration : 125 bytes
!
!
!
ip as-path access-list 2 permit $ABC
ip as-path access-list 2 permit $xyz*
ip as-path access-list 2 permit qwe*
!
end
Router# show running-config partition ip-community
Building configuration...

Current configuration : 92 bytes
!
!
!
ip community-list standard asd permit
ip community-list expanded qwe deny uio*
!
end

Router# show running-config | include ip community
ip community-list standard asd permit
ip community-list expanded qwe deny uio*
Router#
Router# show running-config partition ip-domain-list
Building configuration...
```

```

Current configuration : 70 bytes
!
ip domain-list iop
ip domain-list tyu
ip domain-list jkl
!
!
!
end
Router# show running-config partition ip-static-routes
Building configuration...

Current configuration : 98 bytes
!
!
!
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0
ip route 171.69.1.129 255.255.255.255 10.4.29.1
!
end

Router# show running-config partition line
Building configuration...

Current configuration : 489 bytes
!
!
!
!
line con 0
  exec-timeout 0 0
  transport output lat pad v120 mop telnet rlogin udptn nasi
  stopbits 1
line aux 0
  transport output lat pad v120 mop telnet rlogin udptn nasi
  stopbits 1
line vty 0
  password lab
  login
  transport input lat pad v120 mop telnet rlogin udptn nasi
  transport output lat pad v120 mop telnet rlogin udptn nasi
line vty 1 4
  login
  transport input lat pad v120 mop telnet rlogin udptn nasi
  transport output lat pad v120 mop telnet rlogin udptn nasi
!
end
Router# show running-config partition policy-map
Building configuration...

Current configuration : 162 bytes
!
!
!
policy-map qwer
  description policy-map qwer.
  class xyz
    shape peak 8000 32 32
policy-map p1
policy-map sdf
  class abc
    set precedence 4
!

```



```
!
!
end
Router# show running-config partition route-map
Building configuration...

Current configuration : 65 bytes
!
!
!
route-map iop permit 10
!
route-map rty permit 10
!
!
end
Router# show running-config partition router bgp 1
Building configuration...

Current configuration : 111 bytes
!
!
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  distance bgp 2 2 2
  no auto-summary
!
!
end

Router# show running-config partition router egp ?
<0-65535> Remote autonomous system number

Router# show running-config partition router egp 1
Building configuration...

Current configuration : 46 bytes
!
!
!
router egp 1
  timers egp 20 20
!
!
end

Router# show running-config partition router ?
  bgp      Border Gateway Protocol (BGP)
  egp      Exterior Gateway Protocol (EGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis     ISO IS-IS
  iso-igrp IGRP for OSI networks
  mobile   Mobile routes
  odr      On Demand stub Routes
  ospf     Open Shortest Path First (OSPF)
  rip      Routing Information Protocol (RIP)

Router# show running-config partition router eigrp ?
<1-65535> Autonomous system number

Router# show running-config partition router eigrp 1
Building configuration...
```

```

Current configuration : 13 bytes
!
!
!
!
end

Router#
Router# show running-config partition router eigrp 2
Building configuration...

Current configuration : 57 bytes
!
!
!
router eigrp 2
  variance 10
  auto-summary
!
!
end

Router# show running-config partition router ?
  bgp      Border Gateway Protocol (BGP)
  egp      Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)

Router# show running-config partition router isis ?
  WORD      ISO routing area tag
  |          Output modifiers
  <cr>

Router# show running-config partition router isis qwe
Building configuration...

Current configuration : 86 bytes
!
!
!
router isis qwe
  set-attached-bit route-map qwer
  use external-metrics
!
!
end

Router# show running-config partition router isis ?
  WORD      ISO routing area tag
  |          Output modifiers
  <cr>

Router# show running-config partition router iso
Router# show running-config partition router iso-igrp ?
  WORD      ISO routing area tag
  |          Output modifiers
  <cr>

```

```
Router# show running-config partition router iso-igrp
Building configuration...

Current configuration : 31 bytes
!
!
!
router iso-igrp
!
!
end

Router# show running-config | begin iso
router iso-igrp
!
router isis qwe
  set-attached-bit route-map qwer
  use external-metrics
!
router egp 1
  timers egp 20 20
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  distance bgp 2 2 2
  no auto-summary
!

Router# show running-config partition router ?
  bgp      Border Gateway Protocol (BGP)
  egp      Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)

Router# show running-config partition router mobile ?
  | Output modifiers
  <cr>

Router# show running-config partition router mobile
Building configuration...

Current configuration : 42 bytes
!
!
!
router mobile
  distance 20
!
!
end

Router# show running-config | include router
router mobile
router odr
router eigrp 2
router ospf 4
router iso-igrp
```

```
router isis qwe
router egp 1
router bgp 1
```

```
Router# show running-config partition router ?
  bgp      Border Gateway Protocol (BGP)
  egp      Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)
```

```
Router# show running-config partition router ospf ?
  <1-65535> Process ID
```

```
Router# show running-config partition router ospf 4
Building configuration...
```

```
Current configuration : 64 bytes
!
!
!
router ospf 4
  log-adjacency-changes
  distance 4
!
!
end
```

```
Router# show running-config partition service
Building configuration...
```

```
Current configuration : 190 bytes
!
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
!
!
end
```

```
Router# show running-config partition snmp
Building configuration...
```

```
Current configuration : 84 bytes
!
!
!
snmp-server community user101 RW
snmp mib target list qwe host 0.0.0.0
!
```

end

## Additional References

The following sections provide references related to the Configuration Partitioning feature.

### Related Documents

Related Topic	Document Title
Running configuration performance enhancement— <b>parser config cache</b> for interfaces.	<a href="#">“Configuration Generation Performance Enhancement”</a>
Provisioning of customer services, Config Rollback, Config Locking, and configuration access control	<a href="#">“Contextual Configuration Diff Utility”</a>
Configuration management—Config change logging.	<a href="#">“Configuration Change Notification and Logging”</a>
Configuration management—Quick-save for config change logging <sup>1</sup> .	<a href="#">“Configuration Logger Persistency”</a>
Cisco IOS XE software configuration access control and config session locking (“Config Lock”).	<a href="#">“Exclusive Configuration Change Access and Access Session Locking”</a>

1. The “Configuration Logger Persistency” feature allows saving just the commands entered since the last startup-config file was generated, rather than saving the entire startup configuration.

### Standards

Standard	Title
No standards are associated with this feature.	—

### MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	—

## RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuration Partitioning

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 Configuration Partitioning

Feature Name	Releases	Feature Information
Configuration Partitioning	Cisco IOS XE Release 2.1	<p>The Configuration Partitioning feature provides modularization (“partitioning”) of the running configuration state to provide granular access to the running configuration in Cisco IOS XE software. This feature is enabled by default in Cisco IOS XE software images that include this feature.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Information About Configuration Partitioning</a></li> <li><a href="#">How to Use the Configuration Partitioning Feature</a></li> </ul>

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses and phone numbers in illustrative content is unintentional and coincidental.







## **Configuring Basic File Transfer Services**





# Configuring Basic File Transfer Services

---

**Last Updated: May 4, 2009**

This module describes how to configure a router as a Trivial File Transfer Protocol (TFTP) or Reverse Address Resolution Protocol (RARP) server, configure the router to forward extended BOOTP requests over asynchronous interfaces, and configure rcp, rsh, and FTP.

## 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 Configuring Basic File Transfer Services” section on page 13](#).

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.

## Basic File Transfer Services Configuration Task List

To configure basic file transfer services, perform any of the tasks described in the following sections:

- [Configuring a Router as a TFTP or RARP Server](#)
- [Configuring System BOOTP Parameters](#)
- [Configuring a Router to Use rsh and rcp](#)
- [Configuring a Router to Use FTP Connections](#)
- [Feature Information for Configuring Basic File Transfer Services](#)

All tasks in this chapter are optional.



---

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

© 2007-2009 Cisco Systems, Inc. All rights reserved.

# Configuring a Router as a TFTP or RARP Server

It is too costly and inefficient to have a machine that acts only as server on every network segment. However, when you do not have a server on every segment, your network operations can incur substantial time delays across network segments. You can configure a router to serve as a RARP or TFTP server to reduce costs and time delays in your network while allowing you to use your router for its regular functions.

Typically, a router that is configured as a TFTP or RARP server provides other routers with system image or router configuration files from its Flash memory. You can also configure the router to respond to other types of service requests, such as requests.

## TFTP Router Configuration Prerequisite Tasks

The server and client router must be able to reach each other before the TFTP function can be implemented. Verify this connection by testing the connection between the server and client router (in either direction) using the **ping** *a.b.c.d* command (where *a.b.c.d* is the address of the client device). After the **ping** command is issued, connectivity is indicated by a series of exclamation points (!), while a series of periods (.) plus [timed out] or [failed] indicates that the connection attempt failed. If the connection fails, reconfigure the interface, check the physical connection between the Flash server and client router, and ping again.

After you verify the connection, ensure that a TFTP-bootable image is present on the server. This is the system software image the client router will boot. Note the name of this software image so you can verify it after the first client boot.



### Caution

For full functionality, the software image sent to the client must be the same type as the ROM software installed on the client router. For example, if the server has X.25 software, and the client does not have X.25 software in ROM, the client will not have X.25 capabilities after booting from the server's image in Flash memory.

## Configuring a Router as a TFTP Server

As a TFTP server host, the router responds to TFTP Read Request messages by sending a copy of the system image contained in ROM or one of the system images contained in Flash memory to the requesting host. The TFTP Read Request message must use one of the filenames that are specified in the configuration.

Flash memory can be used as a TFTP file server for other routers on the network. This feature allows you to boot a remote router with an image that resides in the Flash server memory.

Some Cisco devices allow you to specify one of the different Flash memory locations (**bootflash:**, **slot0:**, **slot1:**, **slavebootflash:**, **slaveslot0:**, or **slaveslot1:**) as the TFTP server.

In the description that follows, one router is referred to as the *Flash server*, and all other routers are referred to as *client routers*. Example configurations for the Flash server and client routers include commands as necessary.

## Enabling the TFTP Server

To enable TFTP server operation, use the following commands, beginning in privileged EXEC mode:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>tftp-server flash</b> [partition-number:]filename1 [alias filename2] [access-list-number]  or  Router(config)# <b>tftp-server rom alias</b> filename1 [access-list-number]	Specifies the system image to send in response to Read Requests. You can enter multiple lines to specify multiple images.
<b>Step 3</b>	Router(config)# <b>end</b>	Ends the configuration session and returns you to privileged EXEC mode.
<b>Step 4</b>	Router# <b>copy running-config startup-config</b>	Saves the running configuration to the startup configuration file.

The TFTP session can sometimes fail. TFTP generates the following special characters to help you determine why a TFTP session fails:

- An “E” character indicates that the TFTP server received an erroneous packet.
- An “O” character indicates that the TFTP server received an out-of-sequence packet.
- A period (.) indicates a timeout.

For diagnosing any undue delay in the transfer, the output is useful. For troubleshooting procedures, refer to the *Internetwork Troubleshooting Guide* publication.

In the following example, the system can use TFTP to send copies of the Flash memory file *version-10.3* in response to a TFTP Read Request for that file. The requesting host is checked against access list 22.

```
tftp-server flash version-10.3 22
```

In the following example, the system can use TFTP to send a copy of the ROM image *gs3-k.101* in response to a TFTP Read Request for the *gs3-k.101* file:

```
tftp-server rom alias gs3-k.101
```

The following example a router to send a copy of the file *gs7-k.9.17* in Flash memory in response to a TFTP Read Request. The client router must reside on a network specified by access list 1. Thus, in the example, the any clients on network 172.16.101.0 are permitted access to the file.

```
Server# configure terminal
Enter configuration commands, one per line. End with CTRL/Z
Server(config)# tftp-server flash gs7-k.9.17 1
Server(config)# access-list 1 permit 172.16.101.0 0.0.0.255
Server(config)# end
Server# copy running-config startup-config
[ok]
Server#
```

## Configuring the Client Router

Configure the client router to first load a system image from the server. As a backup, configure the client router to then load its own ROM image if the load from a server fails. To configure the client router, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>boot system</b> [tftp] filename [ip-address]  Example: ASR1006-1(config)#boot system tftp boot 172.16.101.0	Specifies that the client router load a system image from the server.
<b>Step 3</b>	Router(config)# <b>boot system rom</b>	Specifies that the client router loads its own ROM image if the load from a server fails.
<b>Step 4</b>	Router(config)# <b>config-register</b> value	Sets the configuration register to enable the client router to load a system image from a network server.  The general autoboot config register is 0x2.
<b>Step 5</b>	Router(config)# <b>end</b>	Exits global configuration mode.
<b>Step 6</b>	Router# <b>copy running-config startup-config</b>	Saves the configuration file to your startup configuration.
<b>Step 7</b>	Router# <b>reload</b>	(Optional) Reloads the router to make your changes take effect.

## Configuring a Router as a RARP Server

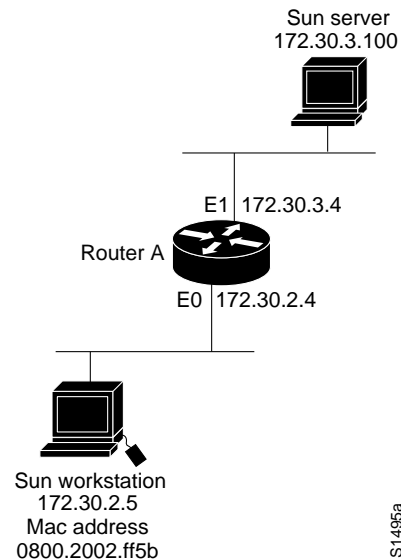
Reverse Address Resolution Protocol (RARP) is a protocol in the TCP/IP stack that provides a method for finding IP addresses based on MAC (physical) addresses. This functionality is the reverse of broadcasting Address Resolution Protocols (ARPs), through which a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address. RARP makes diskless booting of various systems possible (for example, diskless workstations that do not know their IP addresses when they boot, such as Sun workstations or PCs on networks where the client and server are on separate subnets). RARP relies on the presence of a RARP server with cached table entries of MAC-layer-to-IP address mappings.

You can configure a Cisco router as a RARP server. This feature enables the Cisco IOS software to answer RARP requests.

To configure the router as a RARP server, use the following commands, beginning in global configuration mode:

Command	Purpose
Router(config)# <b>interface</b> type [slot/]port	Specifies the interface that you will be configuring the RARP service on and enters interface configuration mode for the specified interface.
Router(config-if)# <b>ip rarp-server</b> ip-address	Enables the RARP service on the router.

Figure 13 illustrates a network configuration in which a router is configured to act as a RARP server for a diskless workstation. In this example, the Sun workstation attempts to resolve its MAC (hardware) address to an IP address by sending a SLARP request, which is forwarded by the router to the Sun server.

**Figure 13**      **Configuring a Router As a RARP Server**

Router A has the following configuration:

```

! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface FastEthernet 0
! Configure the router to act as a RARP server, using the Sun Server's IP
! address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100

```

The Sun client and server's IP addresses must use the same major network number because of a limitation with the current SunOS *rpc.bootparamd* daemon.

In the following example, an access server is configured to act as a RARP server.

```

! Allow the access server to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the access server with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface FastEthernet 0/0
! Configure the access server to act as a RARP server, using the Sun Server's
! IP address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100

```

## Configuring System BOOTP Parameters

The Boot Protocol (BOOTP) server for asynchronous interfaces supports extended BOOTP requests (defined in RFC 1084).

To configure extended BOOTP parameters for asynchronous interfaces, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>async-bootp</b> tag [:hostname] data	Configures extended BOOTP requests for asynchronous interfaces.

You can display the extended data that will be sent in BOOTP responses by using the following command in EXEC mode:

Command	Purpose
Router# <b>show async bootp</b>	Displays parameters for BOOTP responses.

For example, if the DNS server address is specified as extended data for BOOTP responses, you will see output similar to the following:

```
Router# show async bootp
The following extended data will be sent in BOOTP responses:

dns-server 172.22.53.210
```

For information about configuring your Cisco device as a BOOTP server, see the [“Using AutoInstall and Setup”](#) chapter.

## Configuring a Router to Use rsh and rcp

Remote shell (rsh) gives users the ability to execute commands remotely. Remote copy (rcp) allows users to copy files to and from a file system residing on a remote host or server on the network. Cisco’s implementation of rsh and rcp interoperates with the industry standard implementations. Cisco uses the abbreviation RCMD (Remote Command) to indicate both rsh and rcp.

This section is divided into the following sections:

- [Specifying the Source Interface for Outgoing RCMD Communications](#)
- [About DNS Reverse Lookup for rcmd](#)
- [Enabling and Using rsh](#)
- [Enabling and Using rcp](#)

## Specifying the Source Interface for Outgoing RCMD Communications

You can specify the source interface for RCMD (rsh and rcp) communications. For example, the router can be configured so that RCMD connections use the loopback interface as the source address of all packets leaving the router. To specify the interface associated with RCMP communications, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>ip rcmd source-interface</b> interface-id	Specifies the interface address that will be used to label all outgoing rsh and rcp traffic.



Specifying the source-interface is most commonly used to specify a loopback interface. This allows you to associate a permanent IP address with RCMD communications. Having a permanent IP address is useful for session identification (remote device can consistently identify the origin of packets for the session). A “well-known” IP address can also be used for security purposes, as you can then create access lists on remote devices which include the address.

## About DNS Reverse Lookup for rcmd

As a basic security check, the Cisco IOS XE software does a reverse lookup of the client IP address using DNS for the remote command (rcmd) applications (rsh and rcp). This check is performed using a host authentication process.

When enabled, the system records the address of the requesting client. That address is mapped to a host name using DNS. Then a DNS request is made for the IP address for that host name. The IP address received is then checked against the original requesting address. If the address does not match with any of the addresses received from DNS, the rcmd request will not be serviced.

This reverse lookup is intended to help protect against “spoofing.” However, please note that the process only confirms that the IP address is a valid routable address; it is still possible for a hacker to spoof the valid IP address of a known host.

This feature is enabled by default. You can disable the DNS check for RCMD (rsh and rcp) access using the following command in global configuration mode:

Command	Purpose
Router(config)# <b>no ip rcmd domain-lookup</b>	Disables the Domain Name Service (DNS) reverse lookup function for remote command (rcmd) applications (rsh and rcp).

## Enabling and Using rsh

You can use rsh (remote shell) to execute commands on remote systems to which you have access. When you issue the **rsh** command, a shell is started on the remote system. The shell allows you to execute commands on the remote system without having to log in to the target host.

You do not need to connect to the system, router, or access server and then disconnect after you execute a command if you use rsh. For example, you can use rsh to remotely look at the status of other devices *without* connecting to the target device, executing the command, and then disconnecting. This capability is useful for looking at statistics on many different routers. Configuration commands for enabling rsh use the acronym “rcmd”, which is short for “remote command”.

## Maintaining rsh Security

To gain access to a remote system running rsh, such as a UNIX host, an entry must exist in the system’s *.rhosts* file or its equivalent identifying you as a user who is authorized to execute commands remotely on the system. On UNIX systems, the *.rhosts* file identifies users who can remotely execute commands on the system.

You can enable rsh support on a router to allow users on remote systems to execute commands. However, our implementation of rsh does not support an *.rhosts* file. Instead, you must configure a local authentication database to control access to the router by users attempting to execute commands remotely using rsh. A local authentication database is similar to a UNIX *.rhosts* file. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user.

## Configuring the Router to Allow Remote Users to Execute Commands Using rsh

To configure the router as an rsh server, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip rcmd remote-host</b> <i>local-username</i> { <i>ip-address</i>   <i>host</i> } <i>remote-username</i> [ <b>enable</b> [ <i>level</i> ]]	Creates an entry in the local authentication database for each remote user who is allowed to execute rsh commands.
Step 2	Router(config)# <b>ip rcmd rsh-enable</b>	Enables the software to support incoming rsh commands.

To disable the software from supporting incoming rsh commands, use the **no ip rcmd rsh-enable** command.



### Note

When support of incoming rsh commands is disabled, you can still issue an rsh command to be executed on other routers that support the remote shell protocol and on UNIX hosts on the network.

The following example shows how to add two entries for remote users to the authentication database, and enable a router to support rsh commands from remote users:

```
ip rcmd remote-host Router1 172.16.101.101 rmtnetad1
ip rcmd remote-host Router1 172.16.101.101 netadmin4 enable
ip rcmd rsh-enable
```

The users, named *rmtnetad1* and *netadmin4*, are both on the remote host at IP address 172.16.101.101. Although both users are on the same remote host, you must include a unique entry for each user. Both users are allowed to connect to the router and remotely execute rsh commands on it after the router is enabled for rsh. The user named *netadmin4* is allowed to execute privileged EXEC mode commands on the router. Both authentication database entries give the router's host name *Router1* as the local username. The last command enables the router for to support rsh commands issued by remote users.

## Executing Commands Remotely Using rsh

You can use rsh to execute commands remotely on network servers that support the remote shell protocol. To use this command, the *.rhosts* files (or equivalent files) on the network server must include an entry that permits you to remotely execute commands on that host.

If the remote server has a directory structure, as do UNIX systems, the rsh command that you issue is remotely executed from the directory of the account for the remote user that you specify through the *username* keyword and argument pair.

If you do not specify the **/user** keyword and argument, the Cisco IOS XE software sends a default remote username. As the default value of the remote username, the software sends the remote username associated with the current tty process, if that name is valid. If the tty remote username is invalid, the software uses the router host name as the both the remote and local usernames.

To execute a command remotely on a network server using rsh, use the following commands in user EXEC mode:

	Command	Purpose
Step 1	Router> <b>enable</b> [ <i>password</i> ]	Enters privileged EXEC mode.
Step 2	Router# <b>rsh</b> { <i>ip-address</i>   <i>host</i> } [/user <i>username</i> ] <i>remote-command</i>	Executes a command remotely using rsh.

The following example executes the “ls -a” command in the home directory of the user sharon on mysys.cisco.com using rsh:

```
Router# enable
Router# rsh mysys.cisco.com /user sharon ls -a
.
..
.alias
.cshrc
.emacs
.exrc
.history
.login
.mailrc
.newsrc
.oldnewsrc
.rhosts
.twmrc
.xsession
jazz
Router#
```

## Enabling and Using rcp

The remote copy (rcp) commands rely on the rsh server (or daemon) on the remote system. To copy files using rcp, you do not need to create a server for file distribution, as you do with TFTP. You need only to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission in the destination directory. If the destination file does not exist, rcp creates it for you.

Although Cisco’s rcp implementation emulates the functions of the UNIX rcp implementation—copying files among systems on the network—Cisco’s command syntax differs from the UNIX rcp command syntax. The Cisco IOS XE software offers a set of copy commands that use rcp as the transport mechanism. These rcp copy commands are similar in style to the Cisco IOS XE TFTP copy commands, but they offer an alternative that provides faster performance and reliable delivery of data. These improvements are possible because the rcp transport mechanism is built on and uses the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection-oriented. You can use rcp commands to copy system images and configuration files from the router to a network server and vice versa.

You can also enable rcp support to allow users on remote systems to copy files to and from the router.

## Configuring the Router to Accept rcp Requests from Remote Users

To configure the Cisco IOS XE software to support incoming rcp requests, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip rcmd remote-host</b> <i>local-username</i> { <i>ip-address</i>   <i>host</i> } <i>remote-username</i> [ <b>enable</b> [ <i>level</i> ]]	Create an entry in the local authentication database for each remote user who is allowed to execute rcp commands.
Step 2	Router(config)# <b>ip rcmd rcp-enable</b>	Enable the software to support incoming rcp requests.

To disable the software from supporting incoming rcp requests, use the **no ip rcmd rcp-enable** command.

**Note**

When support for incoming rcp requests is disabled, you can still use the rcp commands to copy images from remote servers. The support for incoming rcp requests is distinct from its ability to handle outgoing rcp requests.

The following example shows how to add two entries for remote users to the authentication database and then enable the software to support remote copy requests from remote users. The users, named *netadmin1* on the remote host at IP address 172.16.15.55 and *netadmin3* on the remote host at IP address 172.16.101.101, are both allowed to connect to the router and remotely execute rcp commands on it after the router is enabled to support rcp. Both authentication database entries give the host name *Router1* as the local username. The last command enables the router to support for rcp requests from remote users.

```
ip rcmd remote-host Router1 172.16.15.55 netadmin1
ip rcmd remote-host Router1 172.16.101.101 netadmin3
ip rcmd rcp-enable
```

## Configuring the Remote to Send rcp Requests

The rcp protocol requires a client to send a remote username on each rcp request to a server. When you copy a configuration file from a server to the router using rcp, the Cisco IOS XE software sends the first valid username in the following list:

1. The username set by the **ip rcmd remote-username** command, if the command is configured.
2. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the router software sends the Telnet username as the remote username.

**Note**

In Cisco products, ttys are commonly used in access servers. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called *tty devices*, which stands for *teletype*, the original UNIX terminal.

3. The router host name.

For **boot** commands using rcp, the software sends the router host name; you cannot explicitly configure the remote username.

For the rcp copy request to execute successfully, an account must be defined on the network server for the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, you must add an entry to the *.rhosts* file for the remote user on the rcp server. For example, if the router contains the following configuration lines.

```
hostname Rtr1
```

```
ip rcmd remote-username User0
```

and the router's IP address translates to Router1.company.com, then the `.rhosts` file for User0 on the rcp server should contain the following line:

```
Router1.company.com Rtr1
```

Refer to the documentation for your rcp server for more details.

If the server has a directory structure, the configuration file or image is written or copied relative to the directory associated with the remote username on the server. Use the **ip rcmd remote-username** command to specify which directory on the server to use. For example, if the system image resides in the home directory of a user on the server, you can specify that user's name as the remote username.

If you copy the configuration file to a personal computer used as a file server, the computer must support rsh.

To override the default remote username sent on rcp requests, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>ip rcmd remote-username</b> <i>username</i>	Specifies the remote username.

To remove the remote username and return to the default value, use the **no ip rcmd remote-username** command.

## Configuring a Router to Use FTP Connections

You configure a router to transfer files between systems on the network using the File Transfer Protocol (FTP). With the Cisco IOS XE implementation of FTP, you can set the following FTP characteristics:

- Passive-mode FTP
- User name
- Password
- IP address

To configure these FTP characteristics, use any of the following commands in global configuration mode:

Command	Purpose
Router(config)# <b>ip ftp username</b> <i>string</i>	Specifies the user name to be used for the FTP connection.
Router(config)# <b>ip ftp password</b> [ <i>type</i> ] <i>password</i>	Specifies the password to be used for the FTP connection.
Router(config)# <b>ip ftp passive</b>	Configures the router to only use passive-mode FTP connections.
or Router(config)# <b>no ip ftp passive</b>	or Allows all types of FTP connections (default).
Router(config)# <b>ip ftp source-interface</b> <i>interface</i>	Specifies the source IP address for FTP connections.

The following example demonstrates how to capture a core dump using the Cisco IOS XE FTP feature. The router accesses a server at IP address 192.168.10.3 with login name zorro and password sword. The default passive-mode FTP is used, and the server is accessed using Token Ring interface to1 on the router where the core dump will occur:

```
ip ftp username zorro
ip ftp password sword
ip ftp passive
ip ftp source-interface to1
! The following command allows the core-dump code to use FTP rather than TFTP or RCP
exception protocol ftp
! The following command creates the core dump in the event the system at IP address
! 192.168.10.3 crashes
exception dump 192.168.10.3
```

# Feature Information for Configuring Basic File Transfer Services

Table 18 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 18 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 18**      **Feature Information for Configuring Basic File Transfer Services**

Feature Name	Releases	Feature Information
Configuring Basic File Transfer Services	Cisco IOS XE Release 2.1	This feature was introduced.

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

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

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

© 2007-2009 Cisco Systems, Inc. All rights reserved.







## **Advanced Infrastructure Management**





# Unique Device Identifier Retrieval

---

The Unique Device Identifier Retrieval feature provides the ability to retrieve and display the Unique Device Identifier (UDI) information from any Cisco product that has electronically stored such identity information.

## 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 Unique Device Identifier Retrieval](#)” 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

- [Prerequisites for Unique Device Identifier Retrieval, page 1](#)
- [Information About Unique Device Identifier Retrieval, page 2](#)
- [How to Retrieve the Unique Device Identifier, page 3](#)
- [Configuration Examples for Unique Device Identifier Retrieval, page 5](#)
- [Additional References, page 5](#)
- [Feature Information for Unique Device Identifier Retrieval, page 7](#)

## Prerequisites for Unique Device Identifier Retrieval

In order to use UDI retrieval, the Cisco product in use must be UDI-enabled. A UDI-enabled Cisco product supports five required Entity MIB objects. The five Entity MIB v2 (RFC-2737) objects are as follows:



---

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

- entPhysicalName
- entPhysicalDescr
- entPhysicalModelName
- entPhysicalHardwareRev
- entPhysicalSerialNum

Although the **show inventory** command may be available, using that command on devices that are not UDI-enabled will likely produce no output.

## Information About Unique Device Identifier Retrieval

Before using the UDI Retrieval feature, you should understand the following concepts:

- [Unique Device Identifier Overview, page 2](#)
- [Benefits of the Unique Device Identifier Retrieval Feature, page 3](#)

## Unique Device Identifier Overview

Each identifiable product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. A Fast Ethernet switch might be a member of a superentity like a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

## Benefits of the Unique Device Identifier Retrieval Feature

- Identifies individual Cisco products in your networks.
- Reduces operating expenses for asset management through simple, cross-platform, consistent identification of Cisco products.
- Identifies PIDs for replaceable products.
- Facilitates discovery of products subject to recall or revision.
- Automates Cisco product inventory (capital and asset management).
- Provides a mechanism to determine the entitlement level of a Cisco product for repair and replacement service.

## How to Retrieve the Unique Device Identifier

This section contains the following task:

- [Retrieving the Unique Device Identifier, page 3](#) (required)

## Retrieving the Unique Device Identifier

Perform this task to retrieve and display identification information for a Cisco product.

### SUMMARY STEPS

1. **enable**
2. **show inventory [raw] [entity]**

### DETAILED STEPS

---

**Step 1**    **enable**

Enters privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

**Step 2**    **show inventory [raw] [entity]**

Enter the **show inventory** command to retrieve and display information about all of the Cisco products installed in the networking device that are assigned a PID, VID, and SN. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

```
Router# show inventory
```

```
NAME: "Chassis", DESCR: "12008/GRP chassis"  
PID: GSR8/40           , VID: V01, SN: 63915640
```

```
NAME: "slot 0", DESCR: "GRP"  
PID: GRP-B             , VID: V01, SN: CAB021300R5
```

```
NAME: "slot 1", DESCR: "4 port ATM OC3 multimode"  
PID: 4OC3/ATM-MM-SC    , VID: V01, SN: CAB04036GT1
```

```
NAME: "slot 3", DESCR: "4 port OC3 POS multimode"
```

```

PID: LC-4OC3/POS-MM      ,  VID: V01,  SN: CAB014900GU

NAME: "slot 5", DESCR: "1 port Gigabit Ethernet"
PID: GE-GBIC-SC-B        ,  VID: V01,  SN: CAB034251NX

NAME: "slot 7", DESCR: "GRP"
PID: GRP-B               ,  VID: V01,  SN: CAB0428AN40

NAME: "slot 16", DESCR: "GSR 12008 Clock Scheduler Card"
PID: GSR8-CSC/ALRM       ,  VID: V01,  SN: CAB0429AUYH

NAME: "sfslot 1", DESCR: "GSR 12008 Switch Fabric Card"
PID: GSR8-SFC            ,  VID: V01,  SN: CAB0428ALOS

NAME: "sfslot 2", DESCR: "GSR 12008 Switch Fabric Card"
PID: GSR8-SFC            ,  VID: V01,  SN: CAB0429AUOM

NAME: "sfslot 3", DESCR: "GSR 12008 Switch Fabric Card"
PID: GSR8-SFC            ,  VID: V01,  SN: CAB0429ARD7

NAME: "PSSlot 1", DESCR: "GSR 12008 AC Power Supply"
PID: FWR-GSR8-AC-B       ,  VID: V01,  SN: CAB041999CW

```

Enter the **show inventory** command with an *entity* argument value to display the UDI information for a specific type of Cisco entity installed in the networking device. In this example, a list of Cisco entities that match the module RO argument string is displayed.

```
Router# show inventory "module RO"
```

```

NAME: 'module R0'', DESCR: 'Cisco ASR1000 Route Processor 2'
PID: ASR1000-RP2 ,  VID: V01,  SN: JAE13041JEX

```



#### Note

The **raw** keyword option is primarily intended for troubleshooting problems with the **show inventory** command itself.

```
Router# show inventory raw
```

```

NAME: "Chassis", DESCR: "12008/GRP chassis"
PID:           ,  VID: V01,  SN: 63915640

NAME: "slot 0", DESCR: "GRP"
PID:           ,  VID: V01,  SN: CAB021300R5

NAME: "slot 1", DESCR: "4 port ATM OC3 multimode"
PID: 4OC3/ATM-MM-SC ,  VID: V01,  SN: CAB04036GT1

NAME: "slot 3", DESCR: "4 port OC3 POS multimode"
PID: LC-4OC3/POS-MM ,  VID: V01,  SN: CAB014900GU

```

## Troubleshooting Tips

If any of the Cisco products do not have an assigned PID, the output may display incorrect PIDs and the VID and SN elements may be missing, as in the following example.

```

NAME: "Four Port High-Speed Serial", DESCR: "Four Port High-Speed Serial"
PID: Four Port High-Speed Serial, VID: 1.1, SN: 17202570

```

```
NAME: "Serial1/0", DESCR: "M4T"  
PID: M4T , VID: , SN:
```

In the sample output, the PID is exactly the same as the product description. The UDI is designed for use with new Cisco products that have a PID assigned. UDI information on older Cisco products is not always reliable.

## Configuration Examples for Unique Device Identifier Retrieval

There are no configuration examples for the UDI Retrieval feature. For sample display output from the **show inventory** command, see the [“Retrieving the Unique Device Identifier”](#) section on page 3.

## Additional References

This section provides references related to the UDI Retrieval feature.

## Related Documents

Related Topic	Document Title
Information about managing configuration files	<ul style="list-style-type: none"><li>• <a href="#">Cisco IOS XE Configuration Fundamentals Configuration Guide</a></li><li>• <a href="#">Cisco IOS XE Network Management Configuration Guide</a></li></ul>
Commands for showing interface statistics	<ul style="list-style-type: none"><li>• <a href="#">Cisco IOS Interface Command Reference</a></li><li>• <a href="#">Cisco IOS Interface and Hardware Component Command Reference</a></li></ul>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
CISCO-ENTITY-ASSET-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 2737	<i>Entity MIB (Version 2)</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>



# Feature Information for Unique Device Identifier Retrieval

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 Unique Device Identifier Retrieval**

Feature Name	Releases	Feature Information
Unique Device Identifier Retrieval	Cisco IOS XE Release 2.1	This feature was introduced.

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

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

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.

